МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Крымский федеральный университет имени В.И. Вернадского»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА БИЗНЕС-ИНФОРМАТИКИ И МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

IX Международная научно-практическая конференция

«Проблемы информационной безопасности социально-экономических систем»

2-4 марта 2023

Симферополь — Гурзуф

УДК 004.056:621.391
ББК 32.972.53
П781

П781 **Проблемы информационной безопасности социально-экономических систем** / Труды IX Международной научно-практической конференции, (Гурзуф, 2–4 марта 2023 г.) / под редакцией профессора Бойченко О. В. — Симферополь: Издательский дом КФУ, 2023. — 182 с.
ISBN 978-5-6049317-4-5

В сборнике размещены материалы анализа проблем информационной безопасности в решении задач планирования, разработки, внедрения, эксплуатации и развития информационных и телекоммуникационных систем, которые используются для поддержки текущей хозяйственной деятельности, стратегического планирования и процесса принятия решений в бизнесе и государственном управлении в условиях цифровой экономики.

Также в сборнике содержатся материалы по исследованию основных проблем информационной безопасности в функционировании экономических систем управления, изучению подходов формирования новой отрасли знаний, отражающей возможность управления рисками в контексте создания системы информационной безопасности применительно к проблемам крупных корпоративных информационных систем частного сектора экономики и электронного правительства.

УДК 004.056:621.391
ББК 32.972.53

ISBN 978-5-6049317-4-5

Апатова Наталия Владимировна
д.э.н., д.пед.н., профессор
Физико-технический институт
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНТЕНТА

Современный контент-маркетинг, распространённый в Интернет, оказывает влияние на клиента – потенциального потребителя товаров и услуг, посредством последовательности сообщений, представленных в различных форматах мультимедиа. Это могут быть явные рекламные сообщения с предложением о покупке, но чаще всего строится стратегия взаимодействия с постепенным вовлечением клиента в тему бренда, создание групп по интересам, привлечение на сайт с отвлеченной тематикой. Такие сложные ходы разрабатываются с целью убедить клиента в отвлеченности продавца от прямой продажи, создания видимости заботы о здоровье, благополучии, интересной и насыщенной событиями жизни потребителя.

Выделим три вида контента, подлежащего защите в бизнесе и обществе.

1. ***Сведения о потребителе***.

Поскольку потребитель становится главной ценность для производителя и продавца, сведения о нем необходимо тщательно защищать. Для защиты используют следующие методы и средства:

- хранить только необходимую информацию о потребителе, не противоречащую закону о защите персональных данных;
- иметь ответственного за сбор, хранение и защиту информации о потребителях;
- ограничить сбор данных, спрашивать у потребителей только информацию, необходимую для предоставления услуги или продукта компании; потребители часто возмущаются, когда их просят раскрыть информацию, которая кажется им не относящейся к делу, кроме того, если бизнес станет жертвой хакера, эта дополнительная раскрытая информация подвергает потребителей большему риску;
- защищать собранные данные, принимать надлежащие меры безопасности для защиты собранной информации (определение того, кто должен иметь доступ к данным, а также достаточную защиту баз данных, сетей и веб-сайтов компании; кроме того, предприятия должны использовать стандарты шифрования, соответствующие их бизнес-потребностям, при хранении или передаче любых конфиденциальных данных использовать брандмауэры, которые препятствуют доступу неавторизованных пользователей и защищенной информации);
- использовать надежный процесс аутентификации: создание сложных паролей, которые хакеры не смогут взломать с помощью инструментов подбора паролей;
- осознавать возможную угрозу, определять ценность информации для хакеров и о возможной ее краже, что может помочь определить, какие меры безопасности следует предпринять (когда предприятия пренебрегают оценкой потенциальных угроз, они становятся гораздо более уязвимыми для атак);
- предоставлять сведения о политике конфиденциальности потребителю, четко изложить деловые методы компании (поскольку многие потребители не тратят время на чтение политики конфиденциальности, необходимо напоминать им о том, как компания управляет информацией о потребителях в ключевые моменты, например, когда они предоставляют личные данные);
- инвестировать в новейшее программное обеспечение безопасности, операционные системы и веб-браузеры для защиты от злонамеренных взломов: устаревшие программы легче внедрить, поэтому регулярное обновление системы укрепляет ее защиту от вредоносных программ и вирусов, также ключевым моментом является внедрение современных процедур для обеспечения безопасности сети и программного обеспечения компании;
- необходимо соблюдать безопасность данных, хранящихся на бумажных и других физических носителях, вовремя уничтожать устаревшие данные и тщательно хранить актуальные;
- проверять безопасность поставщиков услуг, кто обрабатывает их данные о потребителях, и следить за тем, чтобы их действия соответствовали самым высоким стандартам безопасности;
- обучать сотрудников лучшим практикам, поскольку хакеры продолжают изобретать схемы и способы обмана ничего не подозревающих, поэтому предприятия должны убедиться, что их сотрудники знают о последних угрозах, чтобы они непреднамеренно не передавали информацию о потребителях; регулярное информирование сотрудников о передовом опыте может защитить конфиденциальность потребителей, а передовой опыт может пресекать схемы фишинга и атаки программ-вымогателей, а также другие угрозы [1].

2. *Общие сведения внешнего мира, с которыми постоянно сталкивается потребитель на работе и в быту*.

К таким сведениям и информационным продуктам относятся программы для мобильных телефонов, персональных компьютеров, различные приложения развлекательного и познавательного, коммерческого характера.

На рисунке 1 показаны наиболее важные для потребителя средства и информационные продукты, которые он связывает с необходимостью киберзащиты.

Рисунок 1 – Наиболее важные для потребителя средства и продукты, требующие киберзащиты [2].

Как следует из проведенного в [2] исследования, наиболее важны для потребителей является построение кибербезопасности в целом (13%) и мобильная защита – 54%, что суммарно дают 67%, на развлекательный контент потребители отводят 13% и 12% - на мобильную инфраструктуру, что в понимании концепции Apple, означает синхронность и связь в работе гаджетов одного пользователя.

Большое внимание родители уделяют безопасности своих детей, используя для этого различные мобильные приложения, позволяющие постоянно отслеживать не только местонахождение ребенка, но и чем он занят в Интернет. Родительский контроль имеет решающее значение для обеспечения безопасности детей в Интернете. Родители детей школьного возраста высоко ценят родительский контроль. На самом деле, 80% родителей детей в возрасте от 3 до 16 лет ответили, что родительский контроль важен, и они ожидают, что их оператор мобильной связи включит родительский контроль в договор на обслуживание [2]. На рисунке 2 показаны наиболее важные средства и результаты родительского контроля.

Рисунок 2 – Наиболее важные средства для родительского контроля в Интернет [2]

В целом потребители считают, что мобильные провайдеры способны защитить их информацию и связь, в том числе обеспечить:

- кибербезопасность потребительского спроса;
- у потребителей сами имеют некоторые приложения безопасности;

- потребители доверяют своим мобильным провайдерам и ожидают, что их провайдеры предложат безопасность;
- потребители готовы платить;
- потребители готовы сменить провайдера.

3. Контент сайта.

Сайт должен соответствовать ожиданиям безопасности потребителя [3]. Компоненты политики информационной безопасности сайта показаны на рисунке 3.

Рисунок 3 – Компоненты политики информационной безопасности сайта

Литература

1. 11 Tips to Protect Consumer Privacy for 2019 National Cybersecurity Awareness Month. URL: https://sopa.tulane.edu/blog/11-tips-protect-consumer-privacy-2019-national-cybersecurity-awareness-month
2. Consumers demand cybersecurity. Can you afford not to provide it? URL: https://cyberhub.allot.com/consumers-demand-cybersecurity-h1-2022-mobile-consumer-survey-results/
3. Does Your Website Meet Consumers' Security Expectations? URL: https://www.inc.com/peter-roesler/does-your-website-meet-consumers-security-expectations.html

УДК 004.056.56

Бойченко Олег Валериевич
д.т.н., профессор
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Симферополь, Россия

УПРАВЛЕНИЕ ДАННЫМИ КИБЕРБЕЗОПАСНОСТИ

Актуальность исследования. Одной из основных сложностей в обеспечении ИБ в России, как и во всем мире, отсутствие целостного взгляда на ИБ (архитектура) и неполный мониторинг и реагирование на инциденты (SecOps).

Кроме того, современные реалии всеобъемлющих санкций объединенного запада, рост числа кибератак со стороны проукраинских хакеров и сопричастных группировок, наряду с банальной кражей информации, выводом из строя оборудования, а также нарушением его функционирования, все больше усилий требует от органов управления всех уровней первоочередных мероприятий по созданию эффективной системы противодействия кибератакам. Указанные обстоятельства приобретают еще большую актуальность ввиду ряда объективных проблем национального характера.

Среди таковых наиболее ярко выраженными являются следующие:

- российский рынок средств защиты развит слабо и, преимущественно, ориентирован на регулятивные требования (наиболее развит рынок antimalware, СКЗИ/VPN, МСЭ/СОВ, DLP, SIEM);
- в большинстве продвинутых ниш рынка ИБ присутствует всего 1-2 игрока, что недостаточно для адекватного выбора и нормальной конкуренции;
- функциональность, качество и возможность массового производства средств защиты отечественного производства на данный момент сильно уступают зарубежным

аналогам.

Проведенный анализ системы мер кибербезопасности, применяемых в наиболее развитых странах мира, а также анализ практик, имеющих национальные корни, свидетельствует о немаловажной роли, в части мер противодействия киберрискам, управлению данными кибербезопасности.

Согласно определению ISO/IEC 27014 (управление информационной безопасностью), данные в кибербезопасности (Data Governance) – это набор практик, процессов, методологий, обеспечивающих управление информационными активами внутри организации, которые включают 10 доменов (рис. 1.):

1. Архитектура данных;
2. Метаданные;
3. Моделирование и проектирование данных;
4. Справочные и основные данные;
5. Безопасность данных;
6. Интеграция данных;
7. Управление документами и контентом;
8. Хранение и операции с данными;
9. Хранилища данных и бизнес-аналитика;
10. Качество данных.

Цель работы состоит в исследовании проблем, связанных с современными практиками управления данными кибербезопасности.

Методы исследования. Основным назначением данных в кибербезопасности является извлечение пользы из данных организации.

Так, например, с устройств Сбера и внешних систем собираются и обрабатываются более 730 млн событий [2]:

- телеметрии сетевых устройств и устройств защиты;
- события логов журналов;
- аудиты серверов и рабочих станций;
- данные из инфраструктуры и информационных систем;
- внешние источники информации об уязвимости;
- транзакционная активность клиентов.

Рисунок 1 – Структура данных кибербезопасности [1]

Практика свидетельствует, что без выстраивания процессов управления данными невозможно реагировать на угрозы и события кибербезопасности. Потому данные кибербезопасности используются для:

- построения аналитических витрин с последующей передачей во внутренние и внешние системы;
- внедрения в различные бизнес-процессы (в Сбере более 6 подразделений используют данные кибербезопасности в своих бизнес-процессах);
- расчета скорингов и обучения модели выявления мошенничества и киберугроз;
- создания собственных аналитических продуктов на платформе кибербезопасности;
- моделирования и исследования по данным кибербезопасности на основе полученного Data lake.

Исследуя основную проблему предметной области, следует обратить внимание на вопросы управления жизненным циклом автоматизированной информационной системы, поскольку экспоненциальный рост данных кибербезопасности привел к большой утилизации ресурсов и сделал процесс управления жизненным циклом данных одним из первостепенных элементов в управлении данными.

В настоящее время эксперты по кибербезопасности выделяют 9 этапов жизненного цикла данных [3]:

1. Определение данных;
2. Сбор данных;
3. Описание данных;

4 - 6. Обработка, транспорт и хранение данных;

7. Использование данных;
8. Формирование отчетности;
9. Определение политики хранения и уничтожения данных.

Рисунок 2 – Этапы жизненного цикла данных

Используя практику Сбера в части жизненного цикла данных, позволяющего формализовать процессы управления данными, следует отметить, что для реализации этапов жизненного цикла в финансовом секторе в частности используются [4]:

- системные логи и журналы аудита серверов и конечных устройств;
- телеметрии от сетевого оборудования и устройств безопасности по периметру;
- транзакционные данные от клиентов;
- данные об инфраструктуре;
- информационные сервисы;
- справочная информация из автоматизированных банковских систем (видео, фото, аудио от документов, которые требуется обрабатывать);
- информация из внешних источников.

Результаты исследования. Следуя положениям теории и практики решения проблемных задач поддержки и принятия решения в управлении информационными системами, эти данные можно поделить на три группы:

- структурированные;
- слабоструктурированные;
- неструктурированные.

Для каждого типа данных определяются свои инструменты сбора (файловые обработчики, стриминговые инструменты).

После этапа сбора и преобразования данные попадают в интеграционный слой, распределяющий данные – интеграционную шину Kafka. Из нее происходит обработка по лямбда-архитектуре:

- первый слой обрабатывает события в режиме реального времени;
- второй накапливает и хранит информацию. Долговременное хранение производится в Data Lake;
- аналитический слой для поиска или использования информации, как оповещения в режиме реального времени в первом слое.

Выводы. В заключении следует отметить, что работа с данными осуществляется как специалистами (руководители, аналитики, форензик-инженеры, Data Scientists), так и в

автоматизированных системах (антифрод-системы, IT и бизнес-системы платформы банка), а в качестве дополнительных компонентов и инструментов управления данными используются:

- система управления метаданных или каталог моделей данных;
- аналитический поиск;
- инструменты защиты данных и безопасности;
- инструменты мониторинга и качества данных.

Литература

1. Образовательная платформа Сбер Университета // [Электронный ресурс]. – Режим доступа: https://auth.sberuniversity.online/login (дата обращения 09.01.2023)

2. Бойченко О.В. Решение проблем сетевой информационной безопасности / О.В. Бойченко, // Актуальные проблемы и перспективы развития экономики: XVI Междунар. науч.-технич. конф., 20-22 апреля 2017 г.: тезисы докладов. – Симферополь, 2017. – С. 13-15.

3. Бойченко О.В. Современная проблематика киберпреступности в России / О.В. Бойченко, // Актуальные проблемы и перспективы развития экономики: Юбилейная XV Междунар. науч.-технич. конф., 19-21 апреля 2016 г.: тезисы докладов. – Симферополь, 2016. – С. 10-11.

4. Бойченко О.В. Управление рисками кибербезопасности / Бойченко О.В. // В сборнике: Актуальные проблемы и перспективы развития экономики. Труды XXI Международной научно-практической конференции. Симферополь, 2022. С. 6-8.

УДК 338.24

Борщ Людмила Михайловна
д.э.н., профессор
Институт экономики и управления
Герасимова Светлана Васильевна
д.э.н., профессор
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРИМЕНЕНИЕ СТРАТЕГИЧЕСКОГО МЕНЕДЖМЕНТА В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Предприятия являются основой развития экономики, которая составляет эффективный хозяйственный комплекс регионов, используя местные ресурсы, в том числе и интеллектуальные. Развитие предприятий вовлекает современного человека во все сферы социально-экономического развития, логически принимая участие в развитии государственного устройства. Предприятия вносят кардинальные перемены в мировоззрении общественного сознания, выступая основным фактором внедрения новых технологий, где человек становится генератором и участником инновационного развития.

На каждом отрезке времени предприятие должно отвечать на основные вопросы ведения хозяйственной деятельности, претерпевая происходящие изменения в конъюнктуре, которая сложилась на рынке, и выстраивая безопасное развитие. А разработка своей собственной финансовой политики и траектории развития должны основываться на оценке финансового состояния и экономического развития, применяя стратегическое планирование и прогнозирование. Анализ позволяет сделать вывод относительно рационального формирования и использования финансовых ресурсов в течение анализируемого периода, что позволяет рассчитывать запас прочности.

Исследование предприятия и внутреннего управления формируется сквозь призму государственного регулирования, поскольку государство, как общий цивилизованный институт, осуществляет свои функции через механизм нормотворчества, сопровождает процессы инновационного развития предприятий, за счет чего формируется институциональная среда.

На сегодняшний день предприятия находятся в состоянии проведения инновационной реконфигурации своего развития. Однако в тоже время в данном процессе присутствует очень высокий уровень неопределенности по выстраиванию отношений по взаимодействию со стейкхолдерами для эффективного устойчивого и безопасного развития.

Оценка финансового состояния субъектов хозяйствования относится к числу наиболее важных общеэкономических проблем, поскольку финансовое состояние отдельно взятых субъектов предпринимательства для экономики страны очень важно. В условиях инновационного развития огромное значение отводится: оптимальности формирования и эффективного использования имущества предприятий, которые состоят из различных видов внеоборотных и оборотных активов; рациональности сочетания собственных и заемных источников, образующих капитал субъекта хозяйствования; эффективности использования капитала субъекта хозяйствования; рациональности взаимоотношения с покупателями и

заказчиками, поставщиками и подрядчиками, кредитными учреждениями, акционерами, государством.

Контроль за показателями предприятия позволяет учитывать скорость динамических изменений внутренней и внешней среды, разрабатывать методологию комплексной оценки финансового и экономического потенциала предприятия, выявляя резервы и упущенные возможности. Развитие предприятий является частью государственной экономики, развивается в сложных условиях, преодолевает потрясения, адаптируясь в процессе развития к политическим и экономическим дестабилизирующим вызовам, что подталкивает предприятия к ускоренным темпам инновационного развития и повышению конкурентоспособности.

Эффективная работа предприятий разных форм собственности, как автономных элементов целостной системы экономического развития, заключается в комплексном применении методологии по оценке финансового и экономического потенциала.

Снижение уровня контроля за финансовым состоянием отдельных субъектов приведет к сбоям и проблемам в функционировании региональной экономической системы пространственного развития [9].

Значительное внимание изучению вопросов, связанных с финансовым состоянием предприятия, уделяли: Алексеева А.И. [1], Борщ Л.М. [4, 5, 10], Блажевич О.Г. [3], Васина А.А. [6], Воробьев Ю.Н. [7]. Воробьева Е.И. [8]. Новым реалиям построения цифровой системы управления предприятиями в современных условиях отражены в трудах Аренкова А.И. [2].

Оценка экономического потенциала предприятия включает анализ динамики и структуры источников формирования и направления использования финансовых ресурсов.

Источники формирования финансовых ресурсов предприятия «Уют» отражаются в пассиве бухгалтерского баланса. Проанализируем оценку их динамики и определим структуру. Совокупный капитал в течении анализируемого периода постоянно снижался, - за период 2020-2022 гг снижение произошло на 17139 или 26,803 % и составило на конец 2022 года 46806 тыс. руб. В наибольшей степени совокупный капитал предприятия уменьшился в 2022 году по сравнению с 2021 годом. Данное уменьшение практически произошло в 2,5 раза.

В составе совокупного капитала постоянно увеличивался собственный капитал, тогда как заемный капитал (краткосрочный и долгосрочный) уменьшался, т.е. именно за счет снижения заемного капитала и произошло уменьшение совокупного капитала.

Собственный капитал в течение анализируемого периода увеличился на 4239 тыс. руб. или 35,988 % и составил в 2022 году 16018 тыс. руб. В наибольшей степени собственный капитал увеличился в 2022 году по сравнению с 2021 годом, составив 67,044 % общего роста собственного капитала в течение анализируемого периода. Следовательно, собственный капитал в течение 2020-2022 годов увеличивался только за счет внутренних источников формирования собственного капитала, а именно за счет чистой прибыли предприятия в 2020 и 2022 годах. При этом следует отметить, что на предприятии сформирован непокрытый убыток, который в течение 2020-2022 годов уменьшился.

Заемный капитал в течение 2020-2022 годов уменьшился на 21378 тыс. руб. или 41,0 %, и составил в 2020 году 30788 тыс. руб. В наибольшей степени заемный капитал уменьшился в 2022 году по сравнению с 2021 годом. Данное уменьшение в 2,4 раза превышало аналогичное изменение заемного капитала. Следует отметить, что на уменьшение заемного капитала повлияло снижение как долгосрочного, так и краткосрочного заемного капитала.

Предприятия, как субъекты хозяйствования, являются частью государственной экономической системы, развиваются в сложных условиях, под влиянием внешней политики государства, преодолевают потрясения, адаптируются к политическим и экономическим дестабилизирующим вызовам, что подталкивает предприятия к ускоренным темпам инновационного развития в системе менеджмента.

Для оценки финансово-экономической безопасности предприятия в системе эффективного менеджмента вносятся кардинальные перемены в систему управления финансами и влияния внешних и внутренних факторов, что в мировоззрении общественного сознания выступает основным фактором внедрения новых управленческих технологий, где человек становится генератором и участником инновационного развития.

Литература

1. Алексеева А.И. Комплексный экономический анализ хозяйственной деятельности: Учебное пособие / А.И. Алексеева, Ю.В. Васильев, А.В. Малеева, Л.И. Ушвицкий. – М.: Финансы и статистика, 2006. – 586 с.

2. Аренков И.А., Смирнов С.А., Шарафуддинов Д.Р. Трансформация системы управления предприятием при переходе к цифровой экономике // Российское предпринимательство, 2018, № 5, С. 1711-1722. DOI: https://doi.org/10.18334/rp.19.5.39115

3. Блажевич О.Г. Комплексная финансовая диагностика предприятия // Научный вестник: финансы, банки, инвестиции, 2018, № 1 (42), С. 29-40.

4. Борщ Л.М., Герасимова С.В. Финансовое планирование развития предприятий как системы управления его эффективностью // Научный вестник: финансы, банки, инвестиции, 2020, № 2 (51), С. 29-39. DOI: https://10.37279/2312-5330-2020-2-29-39
5. Борщ Л.М., Герасимова С.В., Панаедова Г.И. Планирование пространственного развития регионов по принципу экосистемы // Региональная экономика. Юг России, 2021, Т. 9, № 1. С. 69-79. DOI: https://10.15688/re.volsu.2021.1.6
6. Васина А.А. Финансовая диагностика и оценка проектов / А.А. Васина. – СПб.: Питер, 2004. – 448 с.
7. Воробьев Ю.Н. Финансовый менеджмент: учебное пособие / Ю.Н. Воробьев. – Симферополь: Таврия, 2007. – 632 с.
8. Воробьева Е.И., Блажевич О.Г., Кирильчук Н.А., Сафнова Н.С. Методы финансового анализа для оценки состояния предприятий // Научный вестник: финансы, банки, инвестиции, 2016, № 2 (35), С. 5-13.
9. Джалал Мир Абдул Каюм, Борщ Л. М., Воробьева Е. И., Блажевич О. Г., Жарова А. Р. Построение финансовой модели в контуре экосистемы – креативного пространственного развития региона // МИР (Модернизация. Инновации. Развитие). 2022. Т. 13. № 3. С. 494–512. DOI: https://10.18184/2079-4665.2022.13.3.494-512
10. Финансовое прогнозирование и планирование (учеб. пособие-практикум) / Л.М. Борщ ; ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского». – Симферополь : ООО «Антиква», 2017. – 258 с.

УДК 338.23

Буркальцева Диана Дмитриевна
д.э.н, доцент,
директор Юго-Восточной академии (филиал),
профессор кафедры финансов и кредита
Институт экономики и управления
Киселев Рэм Олегович
заместитель председателя комитета по здравоохранению,
социальной политике и делам ветеранов
Государственного совета Республики Крым
Польская Светлана Игоревна
к.э.н., ассистент кафедры информатики
Физико-технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ НА ПРИМЕРЕ РЕСПУБЛИКИ КРЫМ

Цифровая трансформация является важным стратегическим направлением развития национальной и региональной экономик, что подтверждают соответствующие принятые программные документы. На особенности прохождения цифровой трансформации оказывают влияние: развитие рынка цифровых услуг и продуктов, географическое положение, приоритетные экономические отрасли региона, особенности менталитета местных жителей. Всё вышеперечисленное обуславливает актуальность исследуемого направления.

Цель данной публикации рассмотреть особенности и модель цифровой трансформации Республики Крым.

Цифровая трансформация региона перешла на новый этап после утверждения стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Республики Крым 20 августа 2021 года. Модель цифровой трансформации Республики Крым представлена рисунок 1.

Как видно цифровая трансформация затрагивает большинство экономических сфер, и в реализации этой модели задействовано значительное количество бенефициаров. В процесс реализации цифровой трансформации стоит отметь первоочередные задачи:

– развитие взаимодействия и цифровой культуры;
– развитие цифровых компетенций, повышение квалификации персонала;
– развитие цифровой инфраструктуры;
– скорость и оптимизация процессов;
– стратегический подход к управлению данными.

<table>
<tr><td colspan="8">Этапы</td></tr>
<tr><td colspan="8">Ручное управление → автоматизация → цифровизация → полная цифровая трансформация</td></tr>
<tr><td>Срок реализации:</td><td colspan="3">2022-2030 годы</td><td>Ресурсы:</td><td colspan="3">1) Федеральный бюджет 2) Региональный бюджет</td></tr>
<tr><td colspan="8">Отрасли:</td></tr>
<tr><td>Образование и наука</td><td colspan="2">Здравоохранение</td><td>Развитие городской среды</td><td>Транспорт и логистика</td><td colspan="2">Государственное управление</td><td>Социальная сфера</td></tr>
<tr><td>Промышленность</td><td colspan="2">Сельское хозяйство</td><td>Экология и природопользование</td><td>Строительство</td><td colspan="2">Финансовые услуги</td><td>Связь</td></tr>
<tr><td colspan="8">Технологии цифровой трансформации:</td></tr>
<tr><td>облачные технологии</td><td>новые производственные технологии</td><td>робототехника</td><td>интернет вещей</td><td>виртуальная (дополненная) реальность</td><td colspan="2">отечественное программное обеспечение (операционные системы, пакет офисных программ, среда виртуализации)</td><td>технологии искусственного интеллекта.</td></tr>
<tr><td colspan="8">Проекты «Цифровой экономики» Республики Крым</td></tr>
<tr><td>Создание информационной инфраструктуры</td><td colspan="2">Обеспечение информационной безопасности</td><td colspan="2">Поддержка цифровых технологий</td><td colspan="2">Обеспечение кадровыми ресурсами цифровой экономики</td><td>Цифровое государственное управление.</td></tr>
<tr><td colspan="8">Бенефициары:</td></tr>
<tr><td>Исполнительные органы государственной власти Республики Крым</td><td colspan="2">Органы местного самоуправления муниципальных образований в Республике Крым</td><td>Государственные компании и организации</td><td colspan="2">Государственные компании и организации</td><td>Крупный бизнес (публичные и частные компании)</td><td>Малый и средний бизнес</td><td>Индивидуальные предприниматели</td></tr>
<tr><td>Некоммерческие организации</td><td>Самозанятые граждане</td><td>Безработные (не работающие)</td><td colspan="3">Организации в сфере высшего, общего, дополнительного образования, дошкольного образования</td><td>Организации в сфере научных исследований и разработок</td><td>Организации в сфере здравоохранения</td><td>Организации в сфере лесного хозяйства</td></tr>
<tr><td>Организации в сфере сельского хозяйства и охоты</td><td colspan="2">Организации в сфере сбора и утилизации отходов, деятельности по ликвидации загрязнений</td><td>Организации в сфере транспорта</td><td colspan="2">Организации в сфере строительства</td><td>Промышленные предприятия</td><td>Занятые в сфере образования</td><td>Занятые в сфере здравоохранения</td></tr>
<tr><td>Занятые в сфере сельского хозяйства и охоты</td><td colspan="2">Студенты высших учебных заведений Республики Крым</td><td colspan="2">Студенты среднего профессионального образования Республики Крым</td><td>Учащиеся общеобразовательных учебных учреждений Республики Крым</td><td>Молодежь</td><td>Жители Республики Крым</td><td>Граждане Российской Федерации</td></tr>
</table>

Рисунок 1 – Модель цифровой трансформации Республики Крым

Так же стоит отметить и препятствия цифровой трансформации:
– нехватка компетенций и кадров;
– внутреннее сопротивление компаний;
– отсутствие/следование стратегии;
– недостаток финансирования;
– отсутствие необходимой инфраструктуры.

Внедрение цифровых технологий в Республике Крым позволит улучшить качество жизни проживающих на территории граждан за счет представления более широких цифровых возможностей, обеспечит стандартный цифровой сервис гражданам отдаленных территорий, улучшит инфраструктуру и повысит цифровую культуру населения.

Однако, не стоит возлагать слишком больших ожиданий на цифровую трансформацию, она не является панацеей от всех текущих проблем в регионе.

УДК 004.056.53

Гончарова Оксана Николаевна
д.п.н., профессор
Беляева Ирина Вячеславовна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РАЗВИТИЕ КВАНТОВОЙ КРИПТОГРАФИИ

Жизнь современного человека неразрывно связана с использованием телефонов, смартфонов, планшетов и компьютеров. С каждым годом мир технологий развивается, производители устройств стремятся к улучшению производительности и характеристик своих продуктов. Наряду с этими улучшениями производители внедряют технологии для защиты информации и повышают уровень безопасности. Существует множество различных способов - от паролей до биометрических систем и др. Помимо самых распространенных способов защиты, существует такой способ как квантовая криптография - это метод защиты коммуникаций, основанный на принципах квантовой физики.

В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов. Здесь используется квантовый принцип неопределенности Гейзенберга, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью. Используя эти явления, можно спроектировать и создать такую систему связи, которая всегда может

обнаруживать подслушивание. Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё изменения, разрушая исходные сигналы и по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика. Первая работающая схема представляла собой квантовый канал с передающим и принимающим аппаратами. Аппараты разместили на оптической скамье в кожухе. Управление происходило с помощью компьютера, в который были загружены программные представления легальных пользователей и злоумышленника. Злоумышленник не сможет незаметно скопировать поток квантов в силу теоремы о запрете клонирования. Легальные пользователи могут исправлять ошибки с помощью специальных кодов, обсуждая по открытому каналу результаты кодирования. Но всё-таки при этом часть информации попадает к криптоаналитику. Легальные пользователи, изучая количество выявленных и исправленных ошибок, а также интенсивность вспышек света, могут дать оценку количеству информации, попавшей к злоумышленнику.

Появление квантовой криптографии дало новый толчок в развитии методов защиты информации. Сейчас одним из важных достижений в этой области является то, что реализована возможность передачи данных по квантовому каналу со скоростью до единиц Мбит/с благодаря технологии разделения каналов связи по длинам волн и их единовременного использования в общей среде. В скором времени возможно достижение скорости передачи данных в 50 Мбит/с, создание квантового канала связи длиной более 100 км и организация десятков подканалов при разделении по длинам волн.

УДК 336.645.1

Zolotov B. A.
Candidate of Economic Science, Associate Professor
of the Vdadivostok Branch of the Russian Customs Academy
Zolotova V. I.
Doctor of Economic Science, Professor
at the Department of Economics and Company Management
at Far Eastern Federal University
Vladivostok, Russia

RISK ASSESSMENT OF INNOVATIVE TECHNOLOGIES

Many economists associate innovative ventures with the ability to promote innovations by means of risk business, and they refer small risk enterprises, which are able to implement commercially attractive innovations and hereon to make a profit, to the subjects of innovative ventures (1). In this regard an academic interest in risk assessment schedule and innovative technologies effectiveness is shown.

A risk assessment schedule of innovative technology [4], introduced in plenary report in Simferopol international conference, has been highly awarded.

Risk is estimated by sensibility analysis technique. Only one variable, risk's price, is changed in sensibility analysis. Two projects on rice production in Primorye and Krasnodar Territories are considered. Unfilled columns in tables 2 and 3 show received negative values of NPV. In Primorye Territory, capital investments according to the first alternative under consideration (640 kRUB in start year) are possible only at the 5% rate of return (discount rate). In Krasnodar Territory negative value of NPV appears only at 20% rate of return. NPV values are positive at 10% and 15%. The data of problem is listed in the table 1:

Table 1 – The data of problem

Indexes	Primorye Territory	Price +50%	Price -10%	Krasnodar Territory	Price +50%	Price - 10%
Capital input, (RUB/ha)	640000	640000	640000	480000	480000	480000
Amount of years for project, (years)	30	30	30	30	30	30
Depreciation, (RUB/ha)	21333,33	21333,33	21333,33	16000	16000	16000
Current charges, (RUB/ha)	13600	13600	13600	10200	10200	10200
Price of grain, (RUB/kg.)	28	42	25,2	23	34,5	20,7
Crop-producing, (t/ha)	3,2	3,2	3,2	6,2	6,2	6,2
Agricultural tax, (%)	10%	10%	10%	10%	10%	10%

Values of calculated risks are shown in the tables 2, 3:

Table 2 – Rice production projects risks in Primorye and Krasnodar Territories

	640 thous., RUB/ha				320 thous., RUB/ha				640/30 thous. RUB/per year			
Primorye Territory	5%	10%	15%	20%	5%	10%	15%	20%	5%	10%	15%	20%
Risk	28%	-	-	-	12%	31%	-	-	5%	5%	5%	5%
Krasnodar Territory	5%	10%	15%	20%	5%	10%	15%	20%	5%	10%	15%	20%
Risk	3%	10%	30%	-	2%	3%	7%	14%	1%	1%	1%	1%

Table 3 – Risk comparison and NPV

	640 thous.RUB/ha in the noughty				320 thous.RUB/ha in the noughty				By piecemeals			
Primorye Territory	5%	10%	15%	20%	5%	10%	15%	20%	5%	10%	15%	20%
Expected value of NPV, (RUB/ha)	191473	-	-	-	347501	89334			503528	308780	215070	163086
Risk	28%	-	-	-	12%	31%	-	-	5%	5%	5%	5%
Krasnodar Territory	5%	10%	15%	20%	5%	10%	15%	20%	5%	10%	15%	20%
Expected value of NPV, (RUB/ha)	899035	365672	109022		1016055	530256	296494	166820	1133076	694841	483967	366988
Risk	3%	10%	30%	-	2%	3%	7%	14%	1%	1%	1%	1%

According to the second alternative under consideration (320 thous. RUB/ha in start year), Primorye Territory has a positive value of NPV when discount rate is 5% and 10%, and it has a negative value when discount rate is 15% and 20%. Krasnodar Territory has a positive NPV in case of all rates under consideration. Risk level of employment of capital to rice production connected with change in price for rice in Krasnodar Territory is also much less than in Primorye Territory.

References

1. Mindeli L.E. Small and medium-sized innovative ventures: development conditions and international relations / L.E. Mindeli, L.K. Piniya. – M.: AMBA, 2008. – 332 p. (in Russian)
2. Vshivkova Ya.B., Zolotov B.A., Zolotova V.I. Methodological approach to quantitative risk assessment of innovative technology // First international research-to-practice conference Simferopol-Gurzuf, 2015, p. 8-13. (in Russian)

УДК 004.7.056

Кругликов Сергей Владимирович
ген. директор, д-р воен. наук, доцент
Дмитриев Владимир Александрович
зав. лаб., к.ф.-м.н.
Максимович Елена Павловна
вед. науч. сотр., к.ф.-м.н.
Объединенный институт проблем информатики НАН Беларуси
Республика Беларусь

ОБНАРУЖЕНИЕ АТАК В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ЦЕПЕЙ МАРКОВА

При решении задач, связанных с диагностикой и защитой сетевых ресурсов, центральным вопросом является оперативное обнаружение состояний телекоммуникационной сети (ТКС), приводящих к потере полной или частичной ее работоспособности, уничтожению, искажению или утечке информации, являющихся следствием отказов, сбоев случайного характера или результатом получения злоумышленником несанкционированного доступа к сетевым ресурсам, проникновения сетевых червей, вирусов и других угроз информационной безопасности. Раннее обнаружение таких состояний позволит своевременно устранить их причину, а также предотвратит возможные катастрофические последствия.

Для эффективного решения задач информационной безопасности нужен постоянный тщательный анализ актуальных атак и уязвимостей, с помощью эксплуатации которых эти атаки могут быть осуществлены. Подобный анализ необходим для своевременной реакции существующих систем защиты информации, которые зачастую функционируют именно в заданном пространстве атак. Как правило, при анализе возможных атак оценивают вероятности их появления (за некоторый период времени), а также ущерб, который они наносят информации.

В настоящее время наблюдается усложнение технологий проведения атак на ТКС, появляются новые ранее неизвестные виды атак, комплексные атаки, использующие совокупность различных методов атак и зачастую включающие целые группы взаимодействующих злоумышленников. Обнаружение таких комплексных атак затруднено вследствие необходимости анализа разнородных источников информации, поиска взаимосвязи между выявленными простыми атаками.

Одной из актуальных задач в области обнаружения атак является задача обнаружения нестандартной (аномальной) сетевой активности. Это требует реализации наблюдения работы программ/процессов, параметров сетевого трафика, работы пользователей, обеспечивающего слежение за возможными необычными и подозрительными событиями или тенденциями. Решение данной задачи осложняет тот факт, что почти каждый день появляются новые виды сетевых атак и инструментов воздействия на объекты ТКС, что приводит к ошибкам в работе систем обнаружения вторжений. Наличие аномалии может указывать на проводимую в настоящем времени атаку на информационные ресурсы ТКС. Поэтому на практике часто актуальна способность реагировать на возникающие в ТКС аномалии в режиме реального времени.

Одним из методов обнаружения атак в ТКС является метод обнаружения атак на основе цепей Маркова.

Рассмотрим марковскую цепь, с помощью которой исследуем свойства защищённой ТКС, которая подверглась воздействию n различным независимым атакам [1].

Допустим, что в некоторый момент времени t ТКС подверглась воздействию i-ой атаки. Считая, что ТКС имеет внутренние механизмы защиты, мы предположим, что в следующий момент времени $(t + 1)$ эта атака может быть либо отражена, либо, наоборот, успешно реализована с соответствующими негативными последствиями для ТКС. Это состояние ТКС называетсям отказом безопасности.

Для вычисления вероятностей пребывания ТКС в различных состояниях составим матрицу переходных вероятностей марковской цепи [2]:

$$U = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & q_n & 0 \\ r_1 & 0 & 0 & \dots & 0 & \overline{r_1} \\ r_2 & 0 & 0 & \dots & 0 & \overline{r_2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_n & 0 & 0 & \dots & 0 & \overline{r_n} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \quad (1)$$

где q_0 – вероятность отсутствия атаки;

$q_i (i = 1, \dots, n)$ – вероятность возникновения i - атаки;

r_i – вероятность успешного отражения i - ой атаки;

$\overline{r_i} = (1 - r_i)$ – вероятность отказа безопасности.

Вероятности состояний ТКС в произвольный момент времени t определяются следующим образом:

$$p_0(t) = \omega^{-1} \cdot \left[\left(\frac{q_0 + \omega}{2} \right)^{t+1} - \left(\frac{q_0 - \omega}{2} \right)^{t+1} \right], \quad (2)$$

$$p_i(t) = p_0(t-1) \cdot q_i, \quad (3)$$

$$p_{n+1}(t) = 1 - p_0(t) - p_0(t-1) \cdot \sum_{i=1}^{n} q_i, \quad (4)$$

$$\omega = \sqrt{q_0^2 + 4 \cdot \sum_{i=1}^{n} r_i \cdot q_i} > 0,$$

где $p_0(t)$ – вероятность состояния ТКС до воздействия атаки;

$p_i(t)$ – вероятность состояния ТКС после воздействия атаки;

$p_{n+1}(t)$ – вероятность состояния ТКС во время отказа безопасности.

k-е начальные моменты $\mu_k[T]$ времени отказа безопасности T определяются следующим образом [3]:

$$\mu_k[T] = \omega^{-1} \cdot \left[\frac{2}{q_0 + \omega} \cdot S_k \left(\frac{q_0 + \omega}{2} \right) \right] - \frac{2}{q_0 - \omega} \cdot S_k \left(\frac{q_0 - \omega}{2} \right) \cdot \sum_{i=1}^{n} (q_i \cdot \overline{r_i}), \quad (5)$$

$$S_k(x) = \left(x \cdot \frac{d}{dx}\right)^k \left(\frac{1}{1-x}\right).$$

В частности, среднее значение τ и дисперсия D времени отказа безопасности T определяются следующим образом:

$$\tau = \frac{1+\sum_{i=1}^{n} q_i}{\sum_{i=1}^{n}[q_i \cdot (1-r_i)]}, \quad (6)$$

$$D = \frac{1-\sum_{i=1}^{n} q_i + \sum_{i=1}^{n}\left[(q_i \cdot r_i)\cdot\left(3+\sum_{i=1}^{n} q_i\right)\right]}{\left\{\sum_{i=1}^{n}[q_i \cdot (1-r_i)]\right\}^2}. \quad (7)$$

Литература

1) Росенко А.П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе / А.П. Росенко // Известия Южного федерального университета. Технические науки. – 2008. – № 85 (8). – С. 71–81.

2) Тихонов В.И. Марковские процессы / В.И.Тихонов, М.А.Миронов. – Москва: Советское радио, 1977. – 488 с.

3) Касенов А.А. Марковская модель совместных киберугроз и ее применение для выбора оптимального набора средств защиты информации / А.А.Касенов, А.А.Магазев, В.Ф.Цырульник // Моделирование и анализ информационных систем. – 2020. – Т. 27, № 1. – С. 108–123.

УДК 330.46

Миронова Инна Алексеевна
к.э.н.
Тищенко Татьяна Ивановна
к.э.н.
Фролова Марина Петровна
к.э.н.
ФИЦ ИУ РАН
Москва, Россия

МЕТОДИКА ОТБОРА ИНФОРМАЦИОННЫХ ПРОДУКТОВ ДЛЯ РЕАЛИЗАЦИИ В РАМКАХ ПРОГРАММ ЦИФРОВИЗАЦИИ РЕГИОНА

Понятие «Информационный продукт» (ИП) в данной работе – региональная информационная система, созданная и/или эксплуатируемая за счет бюджетных средств в установленном нормативными документами порядке и находящаяся в ведении органа государственной власти региона и подведомственных ему государственных учреждений.

Поскольку количество бюджетных средств в каждый данный момент ограничено, обоснование выбора того или иного направления затрат должно быть дополнено ранжированием и отбором наиболее эффективных для общества информационных продуктов из множества предлагаемых.

Задача ранжирования и отбора информационных продуктов из перечня альтернатив для принятия некоторого управленческого решения является типичной задачей многокритериальной оценки в ситуации слабой структуризации проблемы, содержащей как качественные, так и количественные элементы. Многокритериальность связана с объективной невозможностью оценить проблему одним количественным показателем. Недостаток объективной информации для таких проблем является принципиально неустранимым на момент принятия решения.

Речь идет о решении следующей задачи. Дана группа альтернатив-вариантов решения проблемы (в данном случае – вариантов расходования средств, выделенных на цифровизацию региона в среднесрочном или краткосрочном периоде) и некоторое количество критериев (неограниченное в рамках разумного), предназначенных для оценки альтернатив. Каждая из альтернатив имеет оценку по каждому из критериев. Необходимо построить решающее правило, позволяющее выделить лучшую альтернативу; упорядочить альтернативы по качеству.

К решению подобной задачи логично применить метод аналитической иерархии (Analytic Hierarchy Process), который был предложен американским ученым Томасом Саати и развивался в трудах российского ученого Олега Ларичева [1-3].

Например, имеется четыре информационных продукта (все перечисленные продукты и их характеристики носят условный характер и предназначены исключительно для демонстрации предлагаемого алгоритма отбора проектов).

– ИП №1 «Региональная информационная система выдачи малоимущим гражданам электронного продовольственного сертификата».

– ИП №2 «Региональная информационная система учета избирателей».

– ИП №3 «Региональная информационная системы оперативного управления деятельностью скорой медицинской помощи»

– ИП №4 «Региональная информационная система по учету трудоустройства граждан».

Каждый проект характеризуется следующими показателями (критериями):

- совокупная стоимость владения системой (стоимость создания и стоимость эксплуатации системы) (X_1) [4-5];
- перспективы развития системы (1 – предусмотрена вторая очередь, 2 – предусмотрена вторая и последующие очереди, 3 – нет планов на развитие) (X_2);
- количество смежных ИП, с которыми осуществляется электронное взаимодействие или возможность интеграции с другими системами (1 – нет; 2 – есть ограниченное количество, 3 – есть неограниченное количество) (X_3);
- наличие средств минимизации информационных рисков (нарушения конфиденциальности, авторизации, секретности и т.д.) (1 – есть, 2 – нет, 3 – на данном этапе неизвестно) (X_4);
- наличие средств минимизации риска технических сбоев (1 –есть, 2- нет, 3 – на данном этапе неизвестно) (X_5);
- уровень новизны и уникальности ИП (1 – высокий, 2 – средний, 3 – низкий) (X_6).

На стадии подготовки региональных программ получить в первом приближении значения перечисленных выше характеристик проектов представляется весьма реальным.

Задача заключается в выборе нескольких (или одного) ИП из числа заданных исходя из лимита выделенных на реализацию программы цифровизации региона бюджетных средств. Рассмотрим ее, как задачу принятия решений в условиях многокритериальности и решим ее с помощью процедуры отбора проектов методом аналитической иерархии.

Шаг 1. Попарное сравнение критериев. вычисление коэффициентов важности критериев.

Для реализации этой процедуры предварительно аналитиком (экспертом) задается шкала относительной важности критериев и проектов:

Уровень важности	Количественное значение
Равная важность	1
Умеренное превосходство	3
Существенное или сильное превосходство	5
Значительное (большое) превосходство	7
Очень большое превосходство	9

Попарное сравнение критериев осуществляется аналитиком и фиксируется в виде матрицы сравнений:

	X_1	X_2	X_3	X_4	X_5	X_6	Корень 6–ой степени из произведений элементов строки	Коэффициент важности (вес) критерия
X_1	1	5	0,14	0,11	0,11	0,2	0,35	0,04
X_2	0,2	1	0,14	0,11	0,11	0,14	0,19	0,02
X_3	7	7	1	0,2	0,2	0,2	0,86	0,09
X_4	9	9	5	1	1	0,2	2,08	0,22
X_5	9	9	5	1	1	0,2	2,08	0,22
X_6	5	7	5	5	5	1	4,04	0,42

При сравнении критериев аналитик (эксперт) выражает свое мнение об их соотношении, используя одно из приведенных в шкале относительной важности критериев определений и соответствующее ему число.

Например, если аналитик считает, что величина совокупной стоимости владения ИП важней перспектив его развития, то на пересечении строки X_1 и столбца X_2 ставится цифра «5». Цифра «0,2» на пересечении строки X_3 и столбца X_4 получена делением «1» на «5» и означает, что, при прочих равных условиях, для аналитика значительно важнее наличие средств минимизации информационных рисков, нежели наличие смежных систем.

Шаг 2. Попарное сравнение ИП по каждому критерию; вычисление коэффициентов важности ИП.

Далее сравниваются проекты по каждому из критериев, и определяется вес (коэффициент важности) проекта для рассматриваемого случая.

Сравнение проектов по критерию X_1	ИП №1	ИП №2	ИП №3	ИП №4	Корень 4–ой степени из произведений элементов строки	Коэффициент важности (вес) ИП по критерию X_1
ИП №1	1	0,2	5	5	1,50	0,24
ИП №2	5	1	7	7	3,96	0,63
ИП №3	0,2	0,14	1	1	0,41	0,07
ИП №4	0,2	0,14	1	1	0,41	0,07

Сравнение проектов по критерию X_2	ИП №1	ИП №2	ИП №3	ИП №4	Корень 4–ой степени из произведений элементов строки	Коэффициент важности (вес) ИП по критерию X_2
ИП №1	1	0,20	3	7	1,43	0,22
ИП №2	5	1	7	9	4,21	0,63
ИП №3	0,33	0,14	1	9	0,80	0,12
ИП №4	0,14	0,11	0,11	1	0,20	0,03

Сравнение проектов по критерию X_3	ИП №1	ИП №2	ИП №3	ИП №4	Корень 4–ой степени из произведений элементов строки	Коэффициент важности (вес) ИП по критерию X_3
ИП №1	1	5	0,2	5	1,50	0,24
ИП №2	0,2	1	0,14	1	0,41	0,07
ИП №3	5	7	1	7	3,96	0,63
ИП №4	0,2	1	0,14	1	0,41	0,07

Сравнение проектов по критерию X_4	ИП №1	ИП №2	ИП №3	ИП №4	Корень 4–ой степени из произведений элементов строки	Коэффициент важности (вес) ИП по критерию X_4
ИП №1	1	0,2	0,14	0,14	0,25	0,04
ИП №2	5	1	0,2	0,2	0,67	0,12
ИП №3	7	5	1	1	2,43	0,42
ИП №4	7	5	1	1	2,43	0,42

Сравнение проектов по критерию X_5	ИП №1	ИП №2	ИП №3	ИП №4	Корень 4–ой степени из произведений элементов строки	Коэффициент важности (вес) ИП по критерию X_5
ИП №1	1	1	1	7	1,63	0,32
ИП №2	1	1	1	7	1,63	0,32
ИП №3	1	1	1	7	1,63	0,32
ИП №4	0,14	0,14	0,14	1	0,23	0,04

Сравнение проектов по критерию X_6	ИП №1	ИП №2	ИП №3	ИП №4	Корень 4–ой степени из произведений элементов строки	Коэффициент важности (вес) ИП по критерию X_6
ИП №1	1	1	9	1	1,73	0,32
ИП №2	1	1	9	1	1,73	0,32
ИП №3	0,11	0,11	1	0,11	0,19	0,04
ИП №4	1	1	9	1	1,73	0,32

Шаг 3. Определение наилучшего Информационного продукта.
Качество каждого из ИП оценивается числом, рассчитываемым по формуле:

$$Y_j = \sum_i W_i \times V_{ji}$$

где Y_j - показатель качества j - го ИП;
W_i - вес i - го критерия;
V_{ji} - вес j - го ИП при их сравнении по i - му критерию.
Расчет по приведенной формуле дал следующие результаты.

ИП	Оценка качества
ИП №1	0,248
ИП №2	0,271
ИП №3	0,236
ИП №4	0,245

Таким образом, ИП №2 оценивается как наилучший, далее идет ИП №1, затем ИП №4 и ИП №3. Отбор ИП можно осуществлять согласно вычисленным рангам до тех пор, пока не будет исчерпан лимит денежных средств, выделяемых на программу.

Одно из важнейших достоинств метода аналитической иерархии - это возможность ввода информации при осуществлении парных сравнений как в количественном, так и в качественном виде. Каждое заполнение матрицы сравнений сопровождается последующей автоматической проверкой согласованности суждений экспертов, вычислением индекса согласованности [6].

Литература

1. Ларичев О.И., Мошкович Е.М. Качественные методы принятия решений. – М.: Физматлит, 1996. – 208 с.
2. Ларичев О.И. Наука и искусство принятия решений. – М.: Наука, 1979. – 200 с.
3. Ларичев О.И. Теория и методы принятия решений, а также хроника событий в Волшебных странах. – М.: Лотос, 2003. – 392 с.
4. Липаев В.В. Технико-экономическое обоснование проектов сложных программных систем. – М.: СИНТЕГ, 2004. – 284 с.
5. Скрипкин К.Г. Экономическая эффективность информационных систем. – М.: ДМК Пресс, 2002. – 256 с.
6. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 278 с.

УДК 332.1

Назар Ариан Эмамович
аспирант
Морозова Наталья Ивановна
д.э.н, профессор
Казанский кооперативный институт (филиал)
Российского университета кооперации
Россия

ФОРМИРОВАНИЕ «КУЛЬТУРЫ ДОВЕРИЯ» В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ КАК СИСТЕМНЫЙ ЭЛЕМЕНТ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ И КОРРУПЦИИ В ЦИФРОВОЙ ЭКОНОМИКЕ

В настоящее время мировая экономика стоит на пороге кардинальных технологических трансформаций, которые порождают новые товары и услуги в финансовом, транспортном, торговом секторах, развивается шеринговая экономика, появляются цифровые торговые площадки, а офисы все больше приобретают черты гибридной формы, успешно сочетающей реальные и виртуальные рабочие места. Такого рода трансформация меняет не только технологический уклад, но и социальную структуру общества и экономические устои.

Новый технологический уклад, опирающийся на информационные технологии, призван рационализировать современные достижения в области компьютерной техники, новейших средств информационно-коммуникационных технологий, программного обеспечения и практического опыта, а также осуществлять поиск более эффективной организации информационного процесса для снижения затрачиваемых ресурсов во всех сферах жизнедеятельности современного мира. Как правило, использование информационных технологий ведет к экономии следующие видов ресурсов: затрат труда, времени, энергии и вещественных средств.

Компании, чтобы выиграть в конкурентной борьбе, погружены в атмосферу цифровой трансформации, происходит внедрение в бизнес искусственного интеллекта (далее - ИИ),

машинного обучения, больших данных (big data), интернета вещей (IoT) и облачных вычислений.

На уровне государства поддержка цифровой трансформации и скорость распространения информационных технологий (далее - ИТ) будут определять его позиции на международной арене и экономическое благополучие на десятилетия вперед. Следовательно, необходимо каждой стране, в том числе и России, необходимо действовать как можно быстрее.

Развитие отрасли ИТ для РФ выступает жизненно необходимым в условиях нарастающих санкций и изоляции. Технологический прорыв необходим для избавления от сырьевой зависимости отечественной экономики и перехода на модель опережающего развития, что позволит обеспечить высоко конкурентные позиции на мировом рынке.

Технология ИИ, как наиболее востребованная и широкого применяемая, создает систему, которая способна решать, как сейчас часто говорят, сложные интеллектуальные задачи в любой сфере деятельности человека. Она помогает машинам обучаться на опыте, приспосабливаться к новой информации и выполнять задачи присущие ранее только человеку. В основе работы ИИ лежат сложные нейросетевые модели, обучающие компьютеры обрабатывать данные таким же способом, как и человеческий мозг. Методы нейронных сетей - это принцип нейронных биологических сетей или для понимания, это некоторая математическая модель, в которой предпринята попытка моделирования работы мозга человека, состоящего из многих вычислительных узлов. Нейрон и связи между ними, каждый узел получает на входе много информации. Он считывает определённую функцию или передаёт её значение следующему слою. Другими словами, это тип процесса машинного обучения, называемый глубоким, который использует взаимосвязанные узлы или нейроны в слоистой структуре, напоминающей человеческий мозг. В результате создается адаптивная система и компьютеры учатся и постоянно совершенствуются.

Как уже было сказано, сфера применения ИИ очень велика. Так, в медицине с помощью ИИ можно поставить диагноз, иногда с точностью до 99%. В сельском хозяйстве можно повысить уровень урожайности, ведь ИИ четко рассчитает все внутренние характеристики, определяет место и дату посадки и сбора урожая. В сфере производства ИИ может осуществлять особой контроль по качеству выпускаемой продукции или предоставления услуг компании. В банковской и страховой сферах он способен выявить подозрительную операцию или мошеннические действия с активами клиентов, обнаружить и отразить кибератаки. С помощью ИИ можно синтезировать человеческую речь и мимику. Этот метод используют в процессах видеонаблюдения, поиска и идентификации объектов, а также в колл-центрах. Новая технология способствует развитию биометрии, а это еще одно средство защиты человека и его активов в виртуальном пространстве от мошенников.

23–24 ноября 2022 года состоялась международная онлайн-конференция «AI Journey 2022» на которой присутствовали руководители крупных компаний, научное сообщество, а также представители правительства РФ. Была озвучена проблема о недостаточном масштабировании информационных технологий (далее - ИТ), особенно внедрение ИИ в различные отрасли бизнеса. Так как многие индивидуальные предприниматели и малый бизнес еще недостаточно инвестируют в новые инструменты ИТ, с помощью которых можно повысить эффективность своей финансово-хозяйственной деятельности. На конференции спикерами было озвучено, что для этого будут проводить просветительские мероприятия о пользе ИТ и необходимый план уже имеется в разработке, но одной рекламы недостаточно, нужен еще практический опыт и реальные примеры.

Комплексное внедрение на всех уровнях экономики и всеми его субъектами новых технологий и обеспечивает цифровую трансформацию, способствующую переходу экономику на новую ступень развития - цифровую. Но, как и любая новая технология, она может таить в себе угрозу или становиться уникальной возможностью. Все зависит от того, как, в каких целях и кем она будет использоваться.

К примеру, уход компаний в виртуальное пространство таит в себе потенциальные угрозы. Прежде всего, это расходы на защиту коммерческой информации и клиентской базы от злоумышленников и конкурентов. Существенную угрозу таят в себе и владельцы цифровых платформ, которые представляют площадку для хранения ценной информации компании на своих облачных сервисах.

В сложившейся ситуации крайне важно институционализировать права и обязанности новых акторов в цифровой экономике, установив единые правила добросовестного поведения для всех контрагентов в вириальном пространстве. Иначе говоря, сформировать «культуру доверия» в виртуальном пространстве. А в случае оппортунистического поведения разработать механизмы принуждения и наказания для недобросовестных игроков. Без такого подхода успешное функционирование нарождающейся цифровой экономики станет просто невозможным.

Литература

1. Морозова Н.И. Инновационно-инвестиционная политика как ключевой элемент экономического роста и повышения качества жизни населения России //Бизнес. Образование. Право. 2013. № 1 (22). С. 186-190.
2. Ломакин С.И., Морозова Н.И. Формирование цивилизованного малого бизнеса как стратегическое направление обеспечения устойчивого развития государства и его субъектов //Современная экономика: проблемы и решения. 2015. № 1 (61). С. 141-148.
3. Тинякова В.И., Морозова Н.И. Вектор поиска новой образовательной модели в условиях экономики, основанной на знаниях // Учет и статистика. 2018. № 1 (49). С. 105-111.

УДК 330.336

Павлов Константин Викторович
д.э.н., профессор, профессор кафедры экономики
Полоцкий государственный университет
имени Евфросинии Полоцкой
г. Новополоцк, Республика Беларусь

ФОРМЫ И ОЦЕНКА УРОВНЯ РАЗВИТИЯ МЕЖРЕГИОНАЛЬНЫХ ХОЗЯЙСТВЕННЫХ ВЗАИМОСВЯЗЕЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

В настоящее время межрегиональное (особенно приграничное) сотрудничество стало важной составляющей международных связей российских и белорусских регионов. Действительно, на границе Российской Федерации и Республики Беларусь (то есть в ее приграничных районах) пересекается значительное количество жизненно важных проблем: внешнеполитических, экономических, научных, образовательных, культурных и др. Таким образом, можно отметить важность таких исторически сложившихся взаимодействий и в дальнейшем стоит укреплять и расширять уже сложившиеся контакты, используя современные механизмы и принципы взаимодействия.

В Европейском союзе развитие межрегионального и приграничного сотрудничества помогает достижению гармоничного территориального развития, которое оказывает влияние также на различные темпы экономического развития стран и территорий, различия в доходах и демографические особенности. Изучение процесса управления социально-экономическими проектами и программами межрегионального сотрудничества в условиях приграничного региона затруднено определенными ситуациями, которые нередко носят комплексный характер и поэтому требуют разработки специальных методик изучения.

При анализе приграничных связей важным вопросом является разработка методики оценки состояния реализуемых проектов и программ межрегионального развития. Здесь, в первую очередь, речь идет об оценке эффективности социально-экономических проектов и программ межрегионального сотрудничества. Это крайне важно для эффективного развития многих регионов России, таких, как Мурманская область, Республика Карелия, Приморский край и т.п.

Ш. Радвилавичюс и Н. Межевич отмечают, что при оценке приграничного сотрудничества важно помнить, что оценка может рассматривать различные направления сотрудничества:

- общая оценка влияния приграничного сотрудничества на социально-экономическое развитие приграничной территории;
- оценка программ двустороннего сотрудничества (например, программ ЕИСП);
- оценка конкретных проектов.

Стоит отметить, что в данном случае оценка – это систематизированное исследование ситуации реализации межрегиональных программ социально-экономического сотрудничества или ее результатов. Существует несколько видов оценки: базовая оценка, оценка процесса и оценка влияния. На наш взгляд, государственная система оценки должна включать все виды оценки. Все это крайне важно в настоящее время в условиях цифровизации, понимаемой в широком смысле как всеобъемлющую тенденцию.

Активная роль разрабатываемой методики оценки реализации межрегиональных программ социально-экономического сотрудничества связана с тем, что на каждом этапе развития разных систем (экологических, социальных, экономических) существуют не только положительные, но и отрицательные тенденции, факторы внешнего воздействия, которые только выявить и классифицировать, как правило, бывает недостаточно. В процессе проведения системы оценки реализации межрегиональных программ сотрудничества появляется возможность на основе обобщения информации выработать адекватное представление о состоянии, векторах и динамике развития объекта, его детерминантах и уже на этой основе разработать управленческие решения, реализация которых позволит ограничить или полностью

предотвратить отрицательное воздействие, а также помогут усилить действие благоприятных факторов и условий.

Методику оценки состояния реализации межрегиональных программ и проектов социально-экономического сотрудничества необходимо рассматривать как систему, функционирование которой включает ряд этапов. К ним следует отнести: процесс непрерывного наблюдения, исследование явлений и событий, формирование информационной базы управления, контроль за ходом и характером изменений объекта, оценку отклонений на основе системы критериев (эталонов).

Естественно, оценка состояния реализуемых проектов и программ межрегионального развития в условиях приграничного региона будет обусловлена дифференциацией социально-экономического состояния приграничных регионов, что предполагает при формировании предлагаемой системы показателей оценки введение как относительных, так и абсолютных показателей. Таким образом, вводимая методика оценки состояния реализуемых проектов и программ межрегионального развития в условиях приграничья должна учитывать следующие условия:

- доступность получения необходимой статистической информации;
- простота расчетов;
- возможность построения рейтинговых оценок;
- возможность сравнительных оценок.

Одним из сравнительно новых аспектов изучение территориальной тематики является проблематика, связанная с исследованием социально-экономических и экологических проблем взаимодействия приграничных регионов из разных государств. Анализу многочисленных вопросов развития и управления воспроизводственной системой приграничных регионов на постсоветском пространстве посвятили свои исследования следующие специалисты и ученые: А.А. Епифанов, В.М. Московкин, П.А. Черномаз и ряд других. Автор этих строк также занимался изучением данной проблематики.

Однако разновидностью приграничного социально-экономического взаимодействия является связь и зависимость приграничных водных регионов, т.е. районов из разных стран, граница между которыми имела океанический, морской, озерный, речной характер и т.п. Изучение особенностей взаимодействия приграничных водных, в т.ч. прибрежных районов в экономической сфере по сравнению с исследованием другого типа приграничных регионов является изученным в гораздо меньшей степени.

Выделение приграничной экономики (т.е. экономики приграничных регионов) как важного и перспективного направления регионолистики определяется актуальностью осуществления интенсивного изучения функционирования приграничных районов, при этом это актуально не только для России, но и для многих других стран.

Система показателей, характеризующих межрегиональные социально-экономические и экологические отношения и хозяйственные связи между приграничными территориями должна включать различные блоки, группы показателей: показатели межрегиональной торговли, миграции населения, межтерриториального перемещения капиталов и инвестиций, финансово-кредитных средств, информации. В особую группу следует выделить сводные показатели, дающие комплексную оценку динамики межрегиональных экономических отношений - сюда следует отнести показатели платежного баланса приграничных регионов, торгового баланса и пр. В каждой из этих групп показателей следует выделить те показатели, которые характеризуют природоохранную деятельность.

УДК 004.053.7

Сизерон Мари
Университет г. Ницца София-Антиполис
Франция

КИБЕРБЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ – ВОПРОСЫ КАДРОВОЙ ОБЕСПЕЧЕННОСТИ

Личная информация человека - опасный инструмент в руках мошенника, поэтому она представляет серьезную ценность. Принятие мер по защите персональных данных стало необходимостью из-за развития технических возможностей, например, распространения и копирования информации. Спрос на специалистов в этой области в последнее время очень вырос. От утечки информации пытаются защититься все: и крупные холдинги, и государственные организации и даже представители малого бизнеса [1].

В 2006 году на свет появился ФЗ №152 «О персональных данных» - первый существенно значимый документ по этому профилю. В нем были определены основы

защиты информации, конкретизированы требования к ее хранению и обработке. Тем не менее законодательная база тех лет существенно отличается от нынешней. Более подробно со сведениями, касающимися кибербезопасности, можно ознакомиться в нормативно-методических документах таких служб, как Роскомнадзор, ФСБ России и ФСТЭК, которые являются подзаконными актами Правительства РФ и Минсвязи.

С 2006 года терминология и основополагающие идеи и принципы ФЗ №152 «О персональных данных» сильно изменились. В 2015 появился ФСТЭК России - банк данных угроз безопасности, что помогло окончательно сформировать «костяк» в законодательстве. Поэтому, при поиске каких-либо законодательных актов лучше обращать внимание на дату их публикации. Среди нормативных актов, которые отвечают за правильность хранения, содержание и обработку личной информации, также стоит учесть ФЗ №179 «Трудовой кодекс РФ», ФЗ №129 «О государственной регистрации юридических лиц и индивидуальных предпринимателей» и прочие документы. Для каждой отрасли сформирован свой пакет обязательных документов». Однако на законодательном уровне защищаются только данные физических лиц. На компанию или организацию это никак не распространяется [2].

Для российского законодательства понятие защиты персональных данных напрямую связано с безопасностью человека, его неприкосновенностью и возможностью иметь свои личные или семейные тайны, пояснила эксперт. По российскому законодательству персональные данные - это любая информация, по которой можно установить личность человека.

К ней относят не только ФИО, но и семейное и имущественное положение, адрес проживания и регистрации, образование, а также другие сведения. Контролируют качество обработки личной информации органы государственной власти или местного самоуправления, а также юридические или физические лица в зависимости от взаимодействия с конкретной личностью.

На данный момент в России дефицит специалистов в области кибербезопасности. Эта профессия хорошо оплачиваемая, но весьма специфичная. Нужно иметь определенный багаж знаний, в том числе и статьи законов. Сотрудники сферы информационной безопасности, как правило, работают в офисе и только высококлассные специалисты - удаленно. По сути, их работа скрыта от посторонних глаз, но именно они отвечают за то, чтобы не произошла утечка информации, защищают конфиденциальные данные компании»

даже для того, чтобы стать младшим специалистом - junior, в профессии нужно проработать минимум 1-1,5 года. Но только пройдя несколько этапов и став профессионалом, ИТ-специалист сможет уличить злоумышленника, предугадать ход его мыслей, не допустить использования данных компании в корыстных целях [3].

Литература

1. Бойченко О. В. Пути решения проблем противодействия киберугрозам / О.В. Бойченко // В сборнике: Теория и практика экономики и предпринимательства: XVII Всероссийская с международным участием научно-практическая конференция. – Симферополь: Крымский федеральный университет имени В. И. Вернадского, 2020. - С. 29-31.

2. Корягина С. Кибербезопасность: кто стоит на страже персональных данных в России // [Электронный ресурс]. – Режим доступа: https://riafan.ru/22709623-iberbezopasnost_kto_stoit_na_strazhe_personal_nih_dannih_v_rossii (Дата обращения 02.02.2023).

3. Бойченко О.В. Управление рисками кибербезопасности / О.В. Бойченко // В сборнике: Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической конференции. - Симферополь, 2022. - С. 6-8.

Субетто Александр Иванович
д.э.н., д.ф.н., к.т.н,
профессор, заслуженный деятель науки РФ,
лауреат премии Правительства РФ
РГПУ им. А. И. Герцена
Санкт-Петербург, Россия

ЗАКОН О БИОМЕТРИИ В РОССИИ – ЭТО ПОТЕНЦИАЛЬНОЕ ОРУЖИЕ «ЗАПАДА» В ВОЙНЕ ПРОТИВ РОССИИ

Эта моя «статья-предупреждение» написана как отклик на статью «Это опасная ловушка для граждан», опубликованную в «Советской России» от 10 ноября 2022 года. В статье были опубликованы отзывы на этот закон Галины Быстровой из г. Владимира, Павла Петрушевского из г. Нальчика и Матвея Лыскова из Алтайского Края. В этом контексте данная статья отражает растущую тревогу граждан России по поводу того, что этот «биометрический закон», принятый в Государственной Думе в декабре 2022 г., де-факто превращает российское общество в

единстве с российским государством в тотально-цифрово-контролирующую каждого человека систему. И это происходит на фоне проводимой специальной военной операции, которая уже на наших глазах превращается в войну глобального империализма мировой финансовой капиталократии США, в том числе в форме НАТО, против России с целевой установкой её полного уничтожения, т.е. тогда, когда от России требуется: переход к мобилизационной экономике, мощной духоподъемной идеологии и превращение российского государства во власть народа, созидающего общество Правды, Справедливости, Любви, Дружбы, Взаимопомощи и Гармонии жизни с Природой.

Но есть еще один «подводный камень» в этом законе, утверждающем необходимость заведения на граждан России системы биометрических показателей, которые предстают как необходимый элемент тотальной цифровизации всех систем жизнеобеспечения в российском обществе.

Этот «подводный камень» состоит в моем прогнозе, что все эти биометрические данные на каждого из граждан России, организованные в определенные «банки данных» в российской информационной (компьютерной) системе окажутся в информационных банках данных в США, в Пентагоне, и будут использованы в готовящейся активно мировой финансовой капиталократией биологической войне против России, которую они собираются применить неожиданно, скрытно, достаточно избирательно против определенных групп населения и руководства страны с тем, чтобы потом так же внезапно нейтрализовать ядерную триаду страны.

Биометрическая информация коррелирует с генетической информацией. Требуется только «вскрыть» эти корреляционные связи. Вообще, по моим взглядам, не случайно интенсивная работа «генных инженеров» США по выработке все новых и новых видов биологического оружия, включая производство «боевых вирусов», совпадает:

- с интенсивным процессом разрушения в этой стране семьи,
- с ростом количества неплодородных пар к 25 годам и выше – более 25%,
- и ростом гомосексуализма.

Не понимают ученые-биологи мира, в том числе и ученые-генетики, считающие, что раскрыв нуклеотидную структуру ДНК они познали механизмы наследования тех или иных признаков от «родителей» («предков») к «детям» («потомкам»), что «ДНК-генетика», по моей гипотезе, контролируется «популяционной генетикой», отвечающей за поддержание разнообразия генома популяции и использующий для этого те «полевые субстанции» – «поля», которые открыты физикой (специально даже это понятие «поле» не конкретизирую). Думаю, что популяционная генетика как механизм и процесс находится под управляющим воздействием системогенетических механизмов Биосферы более высокого ранга.

Что за этим скрывается? – За этим «скрывается» то, что «генный инженер» в США, который создал новый боевой вирус, не подозревает, что его «лаборатория» находится под контролем гомеостатических механизмов Биосферы, например, её вирусно-микробного регулятора, и созданный в этой лаборатории «вирус» через управляемый мутагенез со стороны Биосферы, неожиданно превратится в «вирус» с параметрами, о котором этот «генный инженер» и не предполагал. Вся «генная инженерия» в мире, в том числе в США, как наука, которая не знает как действуют биосферные регуляторы Биосферы, использующие «полевую субстанцию» (для этого еще не создана соответствующая техника измерения), и вообще находящаяся только в начале «пути» познания мира, особенно «мира жизни», должна стать скромной, не подчиняться Капиталу (а вернее – Мировой Капиталократии), с его безумной установкой извлекать прибыль из всего, в том числе из войны и из уничтожения не только людей, но целых народов, этносов, цивилизаций. И похоже – собирается извлечь прибыль из экологической гибели всего человечества, в том числе и из уничтожения самого себя.

Иногда мне, после чтения мною лекций по этим проблемам, задавали слушатели вопросы: «Неужели у этих «хозяев денег» (термин В.Ю.Катасонова) нет ни капли здравого «ума, способности рационально мыслить?». Обычно, на этот вопрос я отвечал иносказательно словами Н.А.Бердяева, произнесенными им в 1918 году: «в корыстном интересе таится безумие». Через 100 лет этот приговор Н.А.Бердяева миру, развитием которого управляет прибыль, нажива, корысть, стяжание, и как их неотъемлемый элемент – решение противоречий с помощью насилия и войны, превратился в Приговор Природы Земли всей рыночно-капиталистической системе хозяйственного взаимодействия с ней в виде ускоряющихся процессов первой фазы Глобальной Экологической Катастрофы.

Мир Господства Капитала, в первую очередь олицетворяемый Западом – системой глобального империализма мировой финансовой капиталократии, вошел в эпоху своей агонии. Поэтому им и развязана война против России. Западу нужны её территория и ресурсы без русского народа.

В этой войне переход России на тотальную цифровизацию, в том числе и тотальное биометрическое сканирование населения, – это «подарок» нашему военному врагу, в первую очередь империализму США.

Пора думать – думать по-настоящему. А это дело трудное. Чтобы научиться «думать по-настоящему» – надо возродить высший приоритет развития науки, образования, воспитания, просвещения, как важнейших общественных благ. Образовательная политика России должна иметь целевую установку на переход общества в состояние научно-образовательного общества, в котором образование есть «базис» базиса духовного и материального воспроизводства, а наука выполняет миссию не только производительной силы, но и силы управления.

Закон о биометрии должен быть изъят с поля современной правовой рефлексии. Хватит увлекаться цифровизацией. Пора заняться в России возвышающем человека на великие дела духоподъемной идеологией. Такой идеологией может стать только идеология, соединяющая социализм с ноосферным развитием.

В.И. Вернадский, 160-летие со дня рождения которого мы, т.е. Россия, отметим 12 марта этого года, создал в период с 1929 по 1945 годы учение о переходе Биосферы в Ноосферу, как новое её состояние, связанное с растущей энергетикой воздействия деятельности человечества на Биосферу Земли, определив этот переход глобальным законом. Я, опираясь на эту обобщающую научную идею В.И.Вернадского и на научные школы в развитие этой идеи, Н.Н.Моисеева, В.П.Казначеева, А.Д.Урсула и других, разработал свою научно-мировоззренческую систему, назвав её Ноосферизмом. В ней я показал, что XXI век – это Эпоха Великого Эволюционного Перелома, предназначение которой – переход человечества к единственной форме его развития, спасающей от экологической гибели, – и которая есть научно управляемая социоприродная эволюция на базе общественного интеллекта, научно-образовательного общества и ноосферного экологического духовного социализма.

В заключении еще сделаю одно замечание по поводу «Закона о биометрии». «Биометрический портрет» человека, который станет достоянием информационной («цифровой») системы американского боевого спутника, будет облегчать мониторинг его передвижения в пространстве по поверхности Земли и избирательно его уничтожать, если это станет боевой задачей.

Если вести речь о русском интернете, то здесь необходима технологическая революция, с полным отказом от англоязычного тезауруса, с переходом на тотальную русскую терминологию и русские «интерфейсы». Именно по этому пути – пути создания интернета на китайском языке – пошли китайцы.

В конце 90-х годов знаменитый наш ученый и мыслитель Н.Н.Моисеев оставил нам замечательную книгу «Расставание с простотой». А весь «язык цифр» (я его полезность не отрицаю, но заостряю на этом внимание) – это «язык простоты» (и поэтому в соответствии с «теоремой о неполноте» Гёделя – неполон). Процессы первой фазы Глобальной Экологической Катастрофы уже 30 лет стремительно развиваются. За этим стоит проблема неадекватности человеческого знания, науки, культуры, я уж не говорю о сознании правящих элит, и о сознании всей мировой «цифро – интернетовской» системы, той Сложности Природы – Биосферы и планеты Земля как суперорганизмов, с которой столкнулись человек, общество и человечество в целом. В моем определении возник «Барьером Сложности». Задача науки, и вслед за наукой – культуры и образования, – преодолеть этот Барьер Сложности. Причем в быстром темпе.

Для этого необходимы целенаправленные программы «выращивания» ученых, специалистов, способных работать на междисциплинарном, полипрофессиональном поле. В России – эта необходимость все время оказывала свое «давление» на наши умы из-за сурового климата, большой её территории с разнообразием географических условий воспроизводства жизни, и поэтому – из-за высокой энергетической стоимости воспроизводства жизни общества, определившей базовым законом развития России – не закон конкуренции, а закон кооперации, т.е. то, что мы называем общинностью, коллективизмом, дружбой, взаимопомощью, любовью не только к «ближним», но и к «дальним».

Ещё в 1933 году В.И. Вернадский указал на необходимость смены узкой предметноспециализированной организации науки на проблемноориентированную организацию научного знания. Затем это положение, в результате анализа «уроков Чернобыльской катастрофы», воспроизвел В.А.Легасов. Он указал на такой один из «уроков» – необходимость подготовки «специалистов-проблемников», способных управлять ликвидацией аварийных состояний на объектах высокой технологической сложности. Я в 90-х годах, работая в Исследовательском центре проблем качества подготовки специалистов в Москве, поставил, как задачу, стоящую перед образовательной политикой страны, – переход высшей школы на подготовку своих студентов в новой парадигме профессионализма – проблемноориентированного, требующего более глубокого освоения не только необходимых разделов математики, процедур концептуализации, формализации, но и новых научных отраслей

– системологии (науки о системах), «метаклассификации» (науки о механизмах и закономерностях классифицирования в природе и в обществе), и других междисциплинарных методологических компасов, например – кибернетики в её современном виде, включая гомеостатику.

Дискуссия, которую породило обсуждение содержания «Закона о биометрии», – частично, и косвенно, отражают собой «диктатуру простоты» в «законодательно-правовых умах» России. А время требует умения работать со «сложностью». Наша Государственная Дума должна научиться адекватно отвечать на быстро меняющиеся ситуации и минимизировать возможность таких «ляпов», каковым, несомненно, явилось принятие к концу 2022 года «Закона о биометрии».

Государственная Дума через принятый закон де-факто уже превратила его в реальный процесс в системе внутренней политики страны, который может превратиться в оружие Запада в уже начатой им войне против нас, России. Одновременно, уже начавшаяся дискуссия вокруг «цифровизации» в обществе, в образовании, науке и вокруг «биометризации» (надо же до чего додумались «мозги» некоторых специалистов, и возможно даже считающих себя учеными), по моим взглядам, высвечивает более широкое поле проблем, которая связано с ответами на вопросы: «Что есть Россия?», «Что есть человек?», «Что есть естественный интеллект человека, как он работает, особенно когда взаимодействует с цифровым миром, не убиваем ли мы собственный интеллект, созданный эволюцией Вселенной на Земле?», «Что есть семья, не идет ли уже процесс гибели человечества, по крайней мере на так называемом Западе, когда гибнет семья?».

И список таких вопросов огромен. Нужно уважать автономность человека. В каждой такой автономности прячется гений, прячется огромный мир. В «Бессознательном» разума человека прячется «память» всей предшествующей эволюции Вселенной. Никогда компьютерный («цифровой») интеллект не достигнет уровня человеческого («естественного») интеллекта, созданного эволюцией Вселенной. Почему? – Именно потому, что он создается проектно этим самым человеческим интеллектом, причем самой незначительной его частью – рациональным умом.

XXI век – век Ноосферного Прорыва человечества из России, поднимающего Человека на Высоту Научного Управления самым сложным объектом – социоприродной эволюцией, и соответственно – на уровень Жизнесозидающего Ноосферного Труда и Творчества!

Или этот Прорыв произойдет, или нас на Земле не станет уже в 21 веке!

И тогда предупреждение английского историка, ученого с планетарным сознанием, Арнольда Джозефа Тойнби, высказанное им 50 лет назад, превратится в реальность. А он дал такой прогноз:

«Запад способен гальванизировать и разъединять… А мир нуждается в объединении. Альтернатива этому объединению – самоуничтожение».

Вот почему я настаиваю на положении: Будущее Человечества – это Социализм, но Социализм особого качества. А именно – Ноосферный Экологический Духовный Социализм, обеспечивающий научное управление социоприродной эволюцией, и соответственно – ноосферный союз цивилизаций на Земле. Поэтому СССР XX-го века – это только Предтеча будущей ноосферно-социалистической кооперации всех народов планеты Земля, и соответственно – Мира без Войн и Насилия. И в этом состоит призвание Человека!

УДК 004.054.5

Толкачев Сергей
Университет штата Миннесота
г. Миннеаполис, США

ВОПРОСЫ БЕЗОПАСНОСТИ НЕЙРОСЕТЕЙ

Вводы экспертной оценки специалистов компании Криптонит, которые провели масштабное исследование безопасности искусственных нейросетей, повсеместно применяемых в системах компьютерного зрения, распознавания речи и глубокого анализа данных, включая финансовые и медицинские, указываю на то, что искусственный интеллект может ошибаться даже при незаметных модификациях данных

Указанные результаты получены путем сравнения реализации различных атак, описанных в научных статьях по моделям машинного обучения (ML), построенных на основе искусственных нейронных сетей (ИНС) [1].

Так, в своём исследовании авторы использовали три общепринятых в информационной безопасности сценария:

1. Атака типа white-box предполагает наличие полного доступа к ресурсам сети и наборам данных: знание архитектуры сети, знание всего набора параметров сети, полного доступа к обучающим и тестовым данным;

2. Атака типа gray-box характеризуется наличием у атакующего информации об архитектуре сети. Дополнительно он может обладать ограниченным доступом к данным. Именно атаки по типу «серого ящика» чаще всего встречаются на практике;

3. Атака типа black-box характеризуется полным отсутствием информации об устройстве сети или наборе обучающих данных. При этом, как правило, неявно предполагается наличие неограниченного доступа к модели, то есть имеется доступ к неограниченному количеству пар «исследуемая модель» + «произвольный набор входных данных» [2].

В эксперименте протестированы различные библиотеки для создания вредоносных примеров по изначально отобранных AdvBox, ART, Foolbox, DeepRobust. Эксперименты проводились на различных типах моделей ML. В своем отчете «Криптонит» поделился самыми наглядными результатами, полученными с использованием одной фиксированной модели на основе свёрточной нейронной сети и пяти различных атак. Их реализации взяты из двух библиотек (NIST, которая содержит 60 000 образцов рукописных цифр (отобраны самые наглядные вредоносные примеры)).

Производительность AdvBox оказалась очень низкой, а DeepRobust на момент исследования была очень сырой, поэтому в сухом остатке оказались ART и Foolbox.

Исследование также показало, что проблема с безопасностью моделей ML, основанных на нейросетях, действительно есть. Нейросеть может «с уверенностью» выдать некорректный результат при совсем небольших изменениях в картинке или других входных данных — настолько незначительных, что человек их вряд ли заметит.

Однако нейросеть далеко не всегда удаётся обмануть так просто. В случае уверенного распознавания объекта придётся сгенерировать и проверить множество вредоносных примеров, прежде чем удастся найти рабочий. При этом он может быть практически бесполезным, так как вносит слишком сильные возмущения, заметные невооружённым глазом.

Для иллюстрации в «Криптонит» взяли наиболее легко распознаваемую цифру «9» из тестового набора и показали некоторые получившиеся вредоносные примеры. На иллюстрации видно, что в 8 случаях из 12 построить вредоносные примеры не удалось. В остальных четырёх случаях исследователи обманули нейросеть, но эти примеры получились слишком зашумлёнными. Такой результат связан с уверенностью модели в классификации исходного примера и со значениями параметров различных методов.

В целом эксперимент показал ожидаемые результаты: чем проще изменения, которые вносятся в изображение, тем меньше они влияют на работу ИНС. Следует подчеркнуть, что «простота» вносимых изменений относительна: это может быть и десяток пикселей, но вот догадаться, каких именно, и как их нужно изменить — сложная задача. Нет такого гвоздя, на котором полностью держится результат классификации CNN: в общем случае нельзя изменить один пиксель так, чтобы ИНС ошиблась.

Методы PGD, BIM, FGSM, CW, DeepFool оказались самыми эффективными для сценария «белый ящик». Вне зависимости от реализации, они позволяют провести удачную атаку с вероятностью 100%, однако их применение подразумевает наличие полной информации о модели ML.

Методы Square Attack, HopSkipJump, Few-Pixel, Spatial Transformation предполагают наличие информации об архитектуре модели. Были получены единичные удачные примеры атак, но практическое использование этих методов не представляется возможным. Возможно, ситуация изменится в будущем, если появятся достаточно эффективные реализации, стимулирующие интерес исследователей к этим методам [3].

Все рассмотренные методы «чёрного ящика» используют уровень достоверности, возвращаемый нейронной сетью. Если хотя бы немного понизить точность возвращаемого уровня достоверности, то (и без того невысокая) эффективность методов упадёт многократно.

Литература

1. Бойченко О.В. Интеллектуальные системы управления информационной безопасностью банков / Бойченко О.В. // В книге: Стратегическое управление развитием информационной безопасности социально-экономических систем на основе умных технологий. Борщ Л.М., Герасимова С.В., Жарова А.Р., Буркальцева Д.Д., Польская Л.В., Польская С.И., Кравченко Л.А., Гиндес Е.Г., Горячих М.В., Апатова Н.В., Королев О.Л., Бойченко О.В., Савченко Л.В., Мандрица И.В., Петренко В.И., Жук А.П., Минкина Т.В., Остапенко И.Н., Ремесник Е.С., Бакуменко М.А. и др. Монография. Симферополь, 2022. С. 259-276.

2. Бойченко О.В. Сетевая безопасность облачной инфраструктуры на основе искусственного интеллекта/ Бойченко О.В., Савченко Л.В. // В книге: Стратегическое управление развитием информационной безопасности социально-экономических систем на основе умных технологий. Борщ Л.М., Герасимова С.В., Жарова А.Р., Буркальцева Д.Д., Польская Л.В., Польская С.И., Кравченко Л.А.,

Гиндес Е.Г., Горячих М.В., Апатова Н.В., Королев О.Л., Бойченко О.В., Савченко Л.В., Мандрица И.В., Петренко В.И., Жук А.П., Минкина Т.В., Остапенко И.Н., Ремесник Е.С., Бакуменко М.А. и др. Монография. Симферополь, 2022. С. 233-258.

3. Нейросети // [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php (Дата обращения: 02.02.2023).

УДК 338.24.01

Турдубеков Улугбек Бегиджанович
к.э.н., доцент кафедры «Спортивный менеджмент и экономика»
Узбекского государственного университета физической культуры и спорта
Джураева Комила Гафуровна
к.э.н., доцент., Зам.декана факультета “Налоги и налогообложения”
Фискального института при Государственном налоговом комитете Республики Узбекистан
Султанов Акмал Обидович
к.э.н, заведующий кафедры “”Инженерные коммуникации”
Джизакского политехнического института Узбекистан

К МЕТОДОЛОГИИ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ БЕЗРАБОТИЦЫ В ЭКОНОМИКЕ: СИНЕРГЕТИЧЕСКИЙ ПОДХОД

Безработица в экономике – явление сложное, и в то же время трудно ее количественно оценить. Основным фундаментальным положением в ее исследовании является ни столько изучение и формирование механизмов ее снижения или предотвращения, сколько разработка теоретико-методологических основ анализа, осмысление природы существования, траектории появления, также влияния на эффективность экономической системы (мы абстрагируемся от ее социальной составляющей в контексте изменения экономической ситуации). Безработица и экономическая система, оценка их взаимодействия и вопросы оптимального сочетания этих оценок с целью дальнейшего развития достигнутого уровня и масштаба экономики представляют собой далеко не полный перечень вопросов, рассматриваемых в синергетике безработицы. При росте масштабов экономики в целом, такая оценка взаимодействия невозможно без формирования и развития соответствующих информационных систем, а также их информационной безопасности.

Уровень и структуру безработицы мы представляем конкретными цифрами, т.е., выражаем в количественном пространстве. Данное количественное пространство Q (i,j,k,s) представим в виде функции от параметров развития экономики Xi, демографического развития Yj, институциональных факторов регулирования экономики Zk и природно-экологических составляющих развития общества Ls:

Q = f (Xi, Yj, Zk, Ls), здесь:

i – индекс фактора развития экономики (X);

j – индекс демографического фактора развития (Y);

k – индекс институционального фактора регулирования экономики (Z);

s – индекс природно-экологических факторов развития общества (L).

Информационная система взаимодействия экономики и безработицы в рамках Q (i,j,k,s) функционирует безопасно в том случае, когда существует такое равновесное положение использования ресурсов экономики, при котором, их эффективность достигает максимальной точки во всем пространстве функционирования данной информационной системы.

На основе вышеизложенного методологию исследования безопасности информационной системы взаимодействия экономики и безработицы в рамках Q (i,j,k,s) представим как задачу синерегетической оценки его изменения в области допустимых значений. Сформулируем задачу: исследовать траекторию значения Q (i,j,k,s) и условия достижения Q (i,j,k,s) максимальных и минимальных уровней, а также количественно оценит эффективность экономической системы при экстремальных значениях Q (i,j,k,s).

Точки бифуркций «B» экономической системы в (Q (i,j,k,s),b) имеет значение равное:

Q (b)=f(Xb(I,jb,jb,kb,sb),Yb(ib,Y,jb,sb),Zb(ib,yb,Z,sb),Lb(ib,jb,zb,L)),

а аттрактор «A» экономической системы может быть выражен соотношением:

Q (a)=|f(Xi,Yj,Zk,Ls) – Q (b)|. Тогда максимальное и минимальное значения Q (i,j,k,s) определяются соотношениями:

Q max=Qb+|Qa+f(Xi,Yj,Zk,Ls)|, при i≠b, j≠b,k≠b и s≠b.

Qmin= Qb─|Qa+f(Xi,Yj,Zk,Ls)|, при i≠b, j≠b,k≠b и s≠b.

Эффективность E экономической системы при Q (i,j,k,s) = max и Q (i,j,k,s) = min определяются соотношениями:

Emax=Qmax*Ft(X,Y,Z,L),

Emin=Qmin*Ft(X,Y,Z,L), где Ft – функция условной интегральной цены единицы безработицы при фиксированных значениях i,j,k,s.

Оптимальные значения Q (i,j,k,s) также изменяются в зависимости от социально-психологических, мотивационных и профессиональных атрибутов людских ресурсов, выражаемых определенным состоянием склонности к потреблению. Количественные выражения склонности к потреблению выступают как ограничения пространства точек бифуркаций Q ((i,j,k,s), b).

Литература

1. Евстигнеева Л. П., Евстигнеев Р. Н. / Методологические основы экономической синергетики (научный доклад). — М.: ИЭ РАН, 2007. - 64 с.

2. Капица С. П., Курдюмов С. П., Малинецкий Г. Г. / Синергетика и прогнозы будущего. М., 2001. - 364 с.

3. Гринберг А.С. Защита информационных ресурсов государственного управления. / А.С. Гринберг, Н.Н. Горбачев, А.А. Тепляков. - М.: ЮНИТИ, 2003. - 327 с.

4. Турдубеков У.Б., Жолболдуева Д.Ш., Султанов А.О. Синергетическая интерпретация эффективности управления государственнқми финансами // Экономика и бизнес: теория и практика., 2017. №7. с 77-79.

УДК 33.01

Цхададзе Нелли Викторовна
д.э.н., профессор
Ярошецкий Михаил Александрович
ФГОБУ ВО «Финансовый университет при Правительстве РФ»
г. Москва, Россия

ИСТОРИЯ РАЗВИТИЯ БАНКОВСКОЙ СИСТЕМЫ РФ

Термин «банк» появился в средневековой Италии от названия – «banco», конторы, в которой оказывались посреднические услуги по обмену монет различного веса и с разным содержанием драгоценных металлов. Однако первыми банковскими операциями можно считать деятельность вавилонских купцов, которые принимали вклады от населения под проценты и выдавали ссуды под письменные обязательства или залог. Уже в VIII в. до н. э. тот же банк в Вавилоне принимал вклады, выдавал ссуды, выпускал банковские билеты или банкноты. [1] Самым крупным банком в Вавилоне был дом Игиби. Банк Игиби не только производил продажи и покупки от имени клиентов, за что получал право на часть урожая, но и выдавал денежные средства под расписку или залог, участвовал в торговых предприятиях, выступал посредником в различных сделках.

Российские банки.

Первые банки появились в Великом Новгороде в XII вв. Уже в то время банковские операции не только осуществлялись, но и пользовались спросом у населения.

Изначальной основой российской банковской системы были дворянские банки и банкирские фирмы. Банки кредитовали дворян под залог имений, а банковские фирмы в свою очередь занимались, в основном, кредитованием промышленных и торговых предприятий. Ситуация начала меняться в 1861 г. с отменой крепостного права. В это время создаются новые банки: Государственный банк, Крестьянский банк, появляются первые коммерческие банки, общества взаимного кредита, сберегательные кассы, ломбарды и другие организации, занимающиеся банковскими операциями схожими с ними. Складывается развитая банковская структура, экономика. [2]

Крупнейшими банковскими организациями в России XIX в. были Государственный банк и коммерческие банки. Кредитованием средней и мелкой торговли, в основном, занимались общества взаимного кредита и городские банки. Крестьянский и Дворянский поземельные банки - осуществлявшими ипотечное кредитование, одобряли долгосрочные кредиты и их основными клиентами были помещики и разбогатевшие крестьяне. Помимо банков в России существовали сберегательные кассы, которые вкладывали полученные от клиентов средства в государственные ценные бумаги, затем отдавали процент заработка своему клиенту. Широкой популярностью среди населения пользовались ломбарды, организации, чья деятельность позволяла гражданам взять нужную сумму денег в короткий срок под залог драгоценностей. Эта деятельность носила характер ростовщичества, и кредитование под залог ценных вещей, данный вид всегда имел большие проценты. К 1914г. в России действовало 115 фондовых бирж. Кредитная система в

России была четырехуровневой: центральный банк, коммерческие, а также земельные банки, страховые компании, специализированные банковские организации.

В 1860 году российский император Александр II подписал указ об образовании Государственного банка. Так началась история Банка России.

Первые годы Государственный банк занимался в основном краткосрочным коммерческим кредитованием. Но исторические события вносили свои коррективы. В 20-е годы XX века банк принял активное участие в возрождении финансовой системы страны, развитии товарно-денежных отношений. [2]В тяжелые годы Первой мировой и Великой Отечественной его деятельность была сосредоточена на покрытии военных расходов, снабжении войск и населения деньгами. В Советском Союзе Государственный банк был органом планового кредитования экономики, выпускал наличные деньги, проводил международные расчеты. В сложные для страны 1990-е годы банк сделал все возможное для поддержания стабильности экономики, создал систему валютного регулирования и контроля.

Следуя традициям и активно внедряя инновации, сегодня Банк России является высокотехнологичным мегарегулятором, который отвечает за стабильность всей финансовой системы страны.

Его первым управляющим стал известный банкир, предприниматель и благотворитель Александр Людвигович Штиглиц.

Баланс Государственного банка составлял 798,5 млн рублей. На кредитные операции приходилось 45,8 млн рублей, а золотой запас составлял 81,7 млн рублей. Денежной единицей в стране считался серебряный рубль, содержавший 18 г чистого серебра.

В 1911 году на работу в Государственный банк начинают принимать женщин, что до этого было запрещено. Однако разрешение получали только незамужние женщины и исключительно «по вольному найму».

На базе подконтрольного большевикам Государственного банка, его контор и отделений в апреле создан Народный банк Российской Советской Республики (в составе Наркомата финансов). Основной его функцией стала эмиссия бумажных денежных знаков и их доставка на места.

Советская банковская система.

Советская банковская система должна была поддерживать развитие промышленности, сельского хозяйства, кооперации и строительства. Население, для своих целей, как правило, чаще пользовалось услугами сберегательных касс, в будущем крупнейший банк России. Рассмотрим, эволюцию создания и развития банковской системы СССР.

Как уже отмечали, Российская империя до 1917 года имела свою банковскую систему, включавшую Центральный банк, коммерческие и земельные банки, которые к тому моменту уже имели как минимум полуторавековую историю. Кроме того, были страховые компании и другие специализированные финансовые учреждения. Система в целом повторяла то, что было на тот момент в других странах, всего насчитывалось 51 коммерческий и около 10 земельных банков.

С 1917 года банковское дело было объявлено государственной монополией, все коммерческие банки были национализированы и объединены с Государственным банком. Спустя год в стране запретили иностранные банки.

В годы Гражданской войны и политики военного коммунизма банки были нужны лишь для организации расчетов. Развитие банковской системы началось с началом Новой экономической политики (НЭП):

- В 1921 году создается Госбанк РСФСР, спустя 2 года его преобразуют в Государственный банк СССР. Его целью должно было быть оживление экономики после войны с помощью кредита и других банковских операций;
- В 1922 году совместно с шведским капиталом создан Российский коммерческий банк, но через 2 года СССР выкупает долю шведов и преобразует его во Внешторгбанк, который получил монопольное право на переводы за границу;
- В 1924 году создан Электробанк, который был призван финансировать работы по электрификации страны;

Тогда же продолжает свою деятельность Центральный банк коммунального хозяйства, Центральный сельхозбанк и Промбанк.

Каждый из этих банков работал по своему направлению, и все они выдавали долгосрочные кредиты под 1-4% годовых. Существовала и сеть частных банков, которые работали как сообщества взаимного кредитования.

Началось проведение денежной реформы, закончившейся в 1924 году. Один рубль образца 1922 года приравнивался к 10 000 рублей купюрами прежних выпусков, включая царские деньги.

В 1936 году по решению Правительства СССР Госбанку разрешено производить обмен иностранной валюты и оплату переводов из-за границы по курсу 1 рубль за 3 французских франка.

Курс иностранных валют в Государственном банке установлен исходя из соотношения 5 рублей 30 копеек за 1 доллар США.

Так же была создана служба инкассации.

С началом Великой Отечественной войны Госбанк СССР расширяет кредитование военной промышленности стараясь не сокращать кредитных вложений в другие отрасли народного хозяйства, выполнявшие военные заказы, оказывает финансовую помощь армии и эвакуированным в тыл предприятиям, обеспечивает расчеты в народном хозяйстве, соблюдая при этом режим экономии.

В Госбанке СССР создано управление полевых учреждений, которое отвечало за кассовое и расчетное обслуживание армии. В начальный период войны основной задачей было обеспечение войск наличными средствами.

В послевоенное время не менее 1,5 млрд рублей было выделено Госбанком СССР на восстановление народного хозяйства на освобожденных от немецкой оккупации территориях: на Северном Кавказе, в ряде областей Украины и Белоруссии.

К 1986 году система Государственного банка СССР состояла из 4459 учреждений (185 контор и 4274 отделения).

В 1987 году началась банковская реформа. Реорганизованы действующие и образованы новые специализированные банки. За Госбанком СССР закреплены функции централизованного планового управления денежно-кредитной системой страны. В СССР стали появляться первые акционерные коммерческие банки. [3]

В 1991 году от имени Государственного банка СССР стали выпускаться денежные билеты 1, 3 и 5 рублей (до этого официально именовавшиеся «государственными казначейскими билетами СССР»), разменные и курсовые монеты от 10 копеек до 10 рублей.

Для чеканки монет номиналом 10 копеек впервые использовали стальные заготовки, плакированные пластинами из томпака (сплава меди и цинка). Десятирублевая монета впервые стала «сборной», состоящей из двух частей: кольца из сплава меди, никеля и цинка (нейзильбер), а также латунного диска.

Центральный банк РСФСР признан единственным на территории республики органом государственного денежно-кредитного и валютного регулирования.

В 1998 году проведена деноминация российского рубля в соотношении 1000:1. Вышли в обращение разменные и курсовые монеты Банка России номиналами 1, 5, 10, 50 копеек, а также 1, 2 и 5 рублей. Основным элементом оформления разменных монет стало стилизованное изображение св. Георгия Победоносца. На курсовых монетах размещалась эмблема Банка России в виде двуглавого орла без короны, скипетра и державы.

10 июля 2002 года принят Федеральный закон «О Центральном банке Российской Федерации (Банке России)» — основной документ, регулирующий деятельность Банка России. Целями деятельности Банка России определены защита и обеспечение устойчивости рубля, развитие и укрепление банковской системы страны, обеспечение стабильности и развитие национальной платежной системы, развитие и обеспечение стабильности финансового рынка Российской Федерации.

Банковская система Российской Федерации

Из первых десяти коммерческих банков, созданных в РСФСР в августе — ноябре 1988 года, отпраздновать свое 25-летие смогут только четыре, остальные не дожили до юбилея и по разным причинам ушли с рынка.

Первый коммерческий банк под символическим названием «Союз» был зарегистрирован 24 августа 1988 года в городе Чимкенте. Через два дня был зарегистрирован ленинградский банк «Патент» (сейчас «Викинг»). Он стал первым кооперативным банком на территории РСФСР. Банк «Союз» не дожил до своего совершеннолетия.

До конца 1988 года на территории России было создано еще 24 банка. К концу 1991 года банковская система насчитывала 869 банков. На 1 января 1992 года общая численность коммерческих банков на территории СССР достигла 1616. К октябрю 1992 уже более 1600 банков. К концу 1992 года в стране было зарегистрировано уже более 2 тыс. кредитных учреждений. [4]

Первые иностранные банки были открыты через год после первого коммерческого российского банка.

Максимальное количество действующих кредитных организаций в России было в конце 1994 года — 2439. Затем началось их стремительное сокращение. Назовем три основных причины «смертности» банков. Во-первых, к началу 1995 года ЦБ РФ сумел создать относительно эффективную систему контроля над участниками рынка. Нарушители порядка

покидали рынок. Во-вторых, в 1995 году разразился очередной банковский кризис, что также не способствовало приходу новых игроков. В-третьих, с одной стороны, банковский бизнес к середине девяностых годов стал менее рентабельным, чем за пару лет до этого, а с другой, — резко возросла конкуренция. В 1995—1997 годах с рынка ушло около 1 тыс. кредитных организаций.

Хотя самый сокрушительный удар по банковской системе нанес кризис августа 1998 года. После него на рынке осталось около 1300 банков. Если сравнивать ситуацию с докризисным состоянием, то на пять действующих банков приходилось три с отозванными лицензиями. Большинство пострадавших — крупные и средние банки — кто мог позволить себе покупать в большом объеме ГКО. Например, из 14 банков, входивших в так называемый «Золотой клуб России» (2/3 активов и 90% вкладов физлиц), на рынке осталось только пять (Сбербанк, Внешторгбанк, Внешэкономбанк и банк «Возрождение», а также «спасенный» Агентством по реструктуризации кредитных организаций (АРКО) банк «Российский Кредит»). Остальные 9 в начале двухтысячных, после «тяжелой и продолжительной болезни» были вынуждены уйти с рынка. [5]

В общей сложности банки пережили 7 кризисов начиная с периода перестройки.

На руинах старой банковской системы стала строиться новая. В 2000 г. Центробанк начал переводить банки на международные стандарты отчетности, развивать методы управления банковскими рисками и контроля за ними, совершенствовать методику и практику надзора, обязал банки публиковать годовую отчетность. В 2001 г. был принят «антиотмывочный» закон.

После изменений старой банковской системы стала строиться новая. Середина нулевых стала золотым временем для российских банков. Быстрый рост экономики и открытие внешних рынков помогали им восстанавливать силы. Сектор рос быстрее других: активы банков с 30% ВВП в 1999 г. превысили 60% в 2007 г. Регулирование понемногу усиливалось, но было крайне мягким по сравнению с нынешним.

Основным фактором роста стала розница. Доля средств населения в пассивах банков превысила докризисную уже в 2002 г. и продолжала расти до 2006 г. Но если вклады всегда были важным источником средств для банков, то розничным кредитованием до 1999 г. они практически не занимались. В 2007 году открылись новые направления: ОСАГО и страхование вкладов.

Во время кризиса в 2014 году банки из-за санкций стали увеличивать резервы, однако в это же время хорошо зарабатывали на валютно-обменных операциях. Хотя ни в какое сравнение с переоценкой валютных вкладов и убытков банков это не идет.

После кризиса, борьба с рисками стала главным делом ЦБ. Центральный Банк создал специальную службу анализа рисков, как и западные регуляторы, заставляет крупнейшие банки проходить стресс-тесты. В 2018 г. он дважды увеличивал коэффициенты риска по ипотеке с низким первым взносом. Следовательно, сегодня Центральный Банк принимает максимальные меры при появлении первых намеков на возможное возникновение проблем.

Литература

1.Возникновение банков // Банко, всё о банках URL: https://banco.az/ru/news/vozniknovenie-bankov (Дата обращения: 05.10.2022).

2.Банки и кредит России во второй половине XIX – начале XX в. // Библиотека "Киберленинка", Журнал "Финансы и кредит" URL: https://cyberleninka.ru/article/n/banki-i-kredit-rossii-vo-vtoroy-polovine-xix-nachale-xx-v/viewer (Дата обращения: 04.10.2022).

3.История Банка России // Официальный сайт Банка России URL: https://www.cbr.ru/about_br/history/ (Дата обращения: 27.09.2022).

4.Как начинались коммерческие банки России // Сайт банки.ру URL: https://www.banki.ru/news/bankpress/?id=5162110 (Дата обращения: 05.10.2022).

5.Финансово-экономические кризисы последних десятилетий и их влияние на экономику России // Сайт ПРАЙМ - Агенство экономической информации URL: https://1prime.ru/sience/20190402/829858467.html (Дата обращения: 10.10.2022).

6.Цхададзе Н.В. Эффективность использования дистанционных технологий в предоставлении банковских услуг/ж. «Экономика вчера, сегодня завтра», №3, 2018.-С.358-367.

7.Цхададзе Н.В. Понятие и сущность банковских рисков//Экономика и менеджмент: от теории к практике, г.Ростов-на-Дону, 2017, 151 с.

8.Цхададзе Н.В. Механизмы оценки банковских рисков// О некоторых вопросах и проблемах экономики и менеджмента.- г. Красноярск, 2017, 110 с.

9.Nelli V. Tskhadadze Use of Remote Banking Technology / Series: Advances in Social Science, Education and Humanities Research" Atlantis Press, volume 289. (CSIS 2018), pp. 108-111. https://www.atlantis-press.com/proceedings/csis-18/articles?q=Tskhadadze (Дата обращения: 02.11.2022).

10. Nelli V. Tskhadadze, Nina V. Chernorizova International Financial Markets in the Conditions of Transformation of Financial System/ The Role of Financial Markets in the Global Economy. Springer Nature Switzerland AG 2019, E. G. Popkova (Ed.): ISC 2018, LNNS 57, pp. 757–764, 2019. https://doi.org/10.1007/978-3-030-00102-5_80 (Дата обращения: 02.11.2022).

11. Nelli V. Tskhadadze, Aza D. Ioseliani The Transformation of Human Social Life in the Era of Innovative Banking/ Human and Technological Progress Towards the Socio-Economic Paradigm of the Future. Part III. Edited by Elena G.Popkova and Marina L.Alpidovskaya/ 2020 Walter de Gruyter Gmbh, Berlin/Boston-pp.171-180. https://www.degruyter.com/document/doi/10.1515/9783110692075/html (Дата обращения 01.11.2022).

УДК 330

Черненко Владимир Анатольевич
профессор, д.э.н., профессор
Балтийский государственный технический университет ВОЕНМЕХ им. Д.Ф. Устинова
г. Санкт – Петербург, Россия
Резник Инна Александровна
доцент, к.э.н., доцент
Оренбургский государственный университет
г. Оренбург, Россия

КООРДИНИРОВАННОСТЬ ДЕНЕЖНО - КРЕДИТНОЙ ПОЛИТИКИ С ФИНАНСОВОЙ ПОЛИТИКОЙ В ЭКОНОМИКЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Денежно-кредитная политика (ДКП) предполагает комплексное решение мер по управлению финансовыми ресурсами в стране с целью обеспечения стабильности цен и низкой инфляции. Обеспечить стабильность цен и определенного уровня инфляции возможно при условии оптимального взаимодействия финансовых, материальных и трудовых ресурсов. При этом оптимальное взаимодействие финансовых ресурсов предусматривает использование стоимостного инструментария в интересах общества. То есть экономические агенты: государство, хозяйствующие субъекты, домашние хозяйства создают и обеспечивают устойчивость и развитие национальной экономики.

Развитие экономики РФ проходит в условиях развязанной тотальной гибридной войны США и западом против России. Недружественные страны ввели санкции против российских компаний и частных лиц, заморожены и активы страны в странах – сателлитах США, прекращены транзакции со многими российскими банками. Западные страны своими действиями убедили многие страны в несостоятельности и слабости финансовой системы, основанной на долларе и евро [1].

Политическая идеология и преступления против нашей экономики со стороны западной «цивилизации» требуют изменение подходов при реализации экономической политики, в том числе и ДКП при решении ключевых задач в экономике страны.

Комплексная «перезагрузка» национальной экономики в условиях формирования нового миропорядка предполагает использование ресурсного потенциала, инвестиционного инструментария, обеспечивающих процесс воспроизводства бизнес-среды и повышение уровня жизни населения [1].

Создание условий, обеспечивающих устойчивость и рост экономики РФ, происходят в качественно новой макроэкономической среде. ДКП, определявшая регулирование национальной экономики на основе «стабилизационной» программы МВФ, неприемлема в условиях современного развития экономики РФ. Ранее, «стабилизационная» программа МВФ предусматривала: открытие экономики для иностранных инвестиций, снижение курса национальной валюты, отмена импортного контроля; предоставление банками кредитов субъектам по относительно высокие процентные ставки, контроль за дефицитом государственного (федерального) бюджета и сокращение расходов, увеличение налогов и др. [2].

По сути, программа МВФ определяла вектор ДКП – сокращение денежной массы. Макроэкономический показатель – коэффициент монетизации не отвечал потребностям национальной экономики.

Задача зарубежных «партнеров» сводилась к ослаблению экономики страны. Те, кто отвечал за финансовую стабилизацию страны, и зарубежные «специалисты» не могли не знать, что финансовое регулирование по сценарию МВФ для России неприемлемо. Потребность российской экономики, что подтверждается и расширением кредитов ЦБ РФ, определяется большой территорией и особенностями регионального развития. Обеспечение устойчивости экономики находится за пределами монетарной политики, основу которой определил МВФ [2].

Российская экономика, обладающая огромным ресурсным потенциалом, включая человеческий капитал, постоянно находилась в турбулентном состоянии, что отрицательно сказывалось на макроэкономической ситуации. Политика Центрального банка РФ и Минфина РФ не обеспечивала роста национальной экономики. Из экономического оборота страны

изымалась значительная часть денежных средств (по отношению к ВВП) в форме обязательных платежей и регулятивных инструментов. Величина изъятия превышает аналогичный показатель Китая и США. Из-за высокой величины изъятия денежных средств из экономики страны относительно ВВП накапливались портфельные проблемы, которые «решались» по отработанному сценарию, в основе которого заложен «пусковой механизм» МВФ [2].

Например, в 2014 г. ДКП Центрального банка РФ и Министерства финансов привела к снижению курса национальной валюты, росту инфляции, ухудшению финансового положения большинства экономических субъектов, снижению реальных располагаемых доходов населения. Основная причина финансового регулирования экономики в 2014 г. – обеспечить поступление финансовых ресурсов в бюджетную систему за счет роста инфляции. Причина роста инфляции – снижение курса национальной валюты. Снижение курса национальной валюты привело к росту инфляции и дополнительному поступлению денежных средств в бюджете страны. Особенность макроэкономического регулирования Банком России в конце 2014 г. – изъятие денежной массы из обращения на основе изменения курса национальной валюты. Тем самым ДКП Банка России была направлена и на создание благоприятных условий нерезидентам, что соответствовало требованиям стабилизационной программы МВФ.

Эльвиры Набиуллиной на пленарном заседании Государственной Думы РФ в ноябре 2022 г. отметила, что финансовая система подверглась очень мощному санкционному давлению, но смогла продолжить бесперебойно работать, обеспечивать финансовыми ресурсами граждан и компании. Впереди у нас действительно очень большой фронт работ». Тем самым глава Банка России признала, что звенья финансовой системы выдержали экономические преступления США и западных стран, а финансовые ресурсы, в том числе денежно-кредитные обеспечили устойчивость финансовой системы.

Сценарный подход, предложенный главой Банка России, предусматривает регулирование экономики на основе традиционных инструментов. Банк России официально перешел к политике таргетирования инфляции в начале 2015 г., обозначив величину 4 %. Важнейшим условием для обеспечения ценовой стабильности является заякоривание инфляционных ожиданий населения, бизнеса и рынков на основе формирования доверия к ДКП Центрального банка [3].

Отметим, что в странах с формирующимися рынками, обеспечение заякоренности инфляционных ожиданий экономических субъектов вблизи цели требует гораздо больше времени и усилий со стороны регулятора по сравнению с развитыми странами. Обеспечение ценовой стабильности характерно для стран с более развитой экономикой. Сдерживающим фактором, отрицательно влияющим на развитие экономики в условиях тотальной гибридной войны, является возвращение к «Бюджетному правилу».

Конкретизация направлений развития экономики, обозначенные президентом РФ, предусматривает системный механизм инвестирования, создающий более высокий технологический уровень [1].

Следовательно, можно констатировать, что меняется содержание ДКП. Сквозной характер экономических отношений, в том числе финансовых отношений, охватывающий все звенья экономической системы, является определяющей формой развития национальной экономики. ДКП рассматривается как составная часть финансовой в контексте исследования производственно – финансовой системы страны.

Литература

1. Черненко, В.А., Резник И. А. Финансовая парадигма национальной экономики / В. А. Черненко, И. А. Резник // Актуальные проблемы и перспективы развития экономики: тр. XXI Междунар. науч.-практ. конф., Симферополь-Гурзуф, 20-22 окт. 2022 г. / Крым. федер. ун-т ; под ред. Н. В. Апатовой. - Симферополь : Изд. дом КФУ им. В. И. Вернадского, 2022. - С. 86-87.

2. Черненко В.А., Воронов А.А., Резник И.А Инвестирование национальной экономики: новый формат развития.- Экономический вектор.- 2022. -№ 2 (29).- С. 5-10.

3. Выступление Эльвиры Набиуллиной на совместном заседании профильных комитетов Госдумы по Основным направлениям единой государственной денежно-кредитной политики на 2023 — 2025 годы. - [Электронный ресурс]. – Режим доступа: https://za-dergavy.livejournal.com/294170.html -31.01.2023

УДК 32.019.51

Агеев Дмитрий Андреевич
магистрант
Сигал Анатолий Викторович
д.э.н., профессор
Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ МАЛОГО БИЗНЕСА И ПРЕДПРИНИМАТЕЛЬСТВА В УСЛОВИЯХ КРИЗИСА

Помощь малому предпринимательству считается неотъемлемой составляющей общегосударственной антикризисной политики и политики обеспечения экономической безопасности. После недавней пандемии, а также наложенных санкций со стороны западных стран, в России появился экономический кризис. Благодаря предпринятым чрезвычайным мерам федеральной и региональной поддержки малого и среднего бизнеса в условиях кризиса, обусловленного коронавирусной пандемией, российскому предпринимательству удалось относительно благополучно противостоять негативным явлениям [5]. Но санкционный кризис 2022 года крайне отрицательно сказался на российском малом и среднем предпринимательстве, ударил по нему. Появилась необходимость в дополнительной поддержке малого и среднего предпринимательства со стороны государства [1].

Главные народнохозяйственные функции малого и среднего бизнеса в современной России сводятся к противодействию росту безработицы, к обеспечению приемлемых доходов широким слоям населения. Поэтому необходимо продолжить оказание поддержки малого и среднего предпринимательства и самозанятых по всем возможным направлениям. Следует также усилить поддержку субъектов малого и среднего предпринимательства, самозанятых, специализирующихся на производстве товаров и услуг:

1. Для предприятий, выпускающих дефицитную продукцию;
2. Для предприятий, специализирующихся на продукции, производство которой наиболее рационально с точки зрения ниши некрупного предпринимательства в системе производственной специализации каждого региона [2].

В нынешних российских условиях целесообразен перевод всей экономики на мобилизационную модель в целях обеспечения национальной безопасности. Но речь должна идти только о рыночной мобилизационной экономике со свободными ценами на большинство товаров и услуг, свободным движением капиталов и рабочей силы. Тем более в качестве приоритета должна быть дана свобода развитию малого и среднего предпринимательства.

Ядром такой мобилизационной экономики должна являться поощряемая государством кооперация малого бизнеса и предпринимательства. Важнейшим элементом российской мобилизационной экономики станет качественное увеличение значимости и размера цифровизации хозяйственной деятельности (цифровые платформы, онлайн-сервисы, интернет-доставка, онлайн-торговля и т.п.) с участием, даже с ведущей ролью субъектов малого и среднего бизнеса и самозанятых.

Предпринимательство – малое, среднее, индивидуальное и самозанятые (неофициальная часть российского легального предпринимательства) – обычно считается инструментом сглаживания циклических и чрезвычайных кризисных явлений в экономике и социальной сфере. Уже многие десятилетия поддержка малого и среднего предпринимательства (МСП) в большинстве стран мира является обязательной частью государственной антикризисной политики. Кризисные явления в российской экономике, обусловленные коронавирусной пандемией и санкционными действиями западных стран (кризисы предложения важной продукции на внутреннем рынке из-за административных ограничений), не относятся к числу исключений.

В кризисных условиях у малого и среднего бизнеса в полной мере проявляются имманентные ему плюсы:

1. Малые хозяйственные организации не нуждаются в крупных капиталовложениях и основных фондах;
2. Малые предприятия могут перевооружать свои фонды с минимальными дополнительными затратами, компьютеризировать и автоматизировать бизнес-процесс;
3. Малые и средние предприятия своей деятельностью создают должную конкурентную среду;

4. Они просты в управлении и противостоят бюрократизации и заорганизованности; МСП демпфируют социальные катаклизмы, способствуют стабилизации экономической ситуации [3].

Но правомерно предположить, что невиданные ранее санкционные меры окажут более сильное негативное воздействие на экономику нашей страны, чем коронавирусный кризис со всеми его последствиями.

Несомненно, что эти негативные последствия в сочетании с несбалансированностью территориальной структуры малого и среднего предпринимательства (с концентрацией его развития в небольшом количестве российских регионов) и с его теневизацией порождают серьезные угрозы экономической безопасности нашей страны [4].

Литература

1. Горева, Е.А. Развитие малого бизнеса в условиях санкций / Е.А. Горева, Ю.Ю.Сидорак // Проблемы и перспективы социально-экономического развития регионов: Материалы Всероссийской научно-практической конференции: в 2 томах. Киров, 2015. – с. 14–17
2. Ионичев, В.Н. Проблемы привлечения малого и среднего предпринимательства к участию в закупках крупнейших российских государственных компаний в контексте рисков экономической безопасности / Ионичев В.Н. // Проблемы рыночной экономики, 2016. – № 2. – с. 31–37.
3. Груцынова, К.А. Малый бизнес как стратегический ресурс обеспечения экономической безопасности региона / К.А.Груцынова // Управление и экономическая безопасность: страна, регион, малый и средний бизнес: III Международная научно-практическая конференция. Ростов-на-Дону, 2020. – с. 28–32.
4. Назаренко, А.А. Развитие малого и среднего предпринимательства как фактор обеспечения экономической безопасности Российской Федерации / А.А. Назаренко, Н.В. Седова // Национальные интересы: приоритеты и безопасность, 2019. – с. 1424–1439.
5. Банк России совместно с Правительством запускает антикризисные программы льготного кредитования МСП, 05 03 2022 года. Cbr.ru. [Электронный ресурс]. URL: http://cbr.ru/press/pr/?file=05032022_173023PROTECTION05032022_163108.htm

Аджисалиев Шукри Шерянович
магистрант
Бакуменко Мария Александровна
к.э.н., доцент
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ РИСКОВ ОТЕЧЕСТВЕННЫХ ИННОВАЦИОННЫХ ПРОЕКТОВ

Для перехода России из перечня стран с нестационарной экономикой в список высокоразвитых стран со стационарной экономикой необходим существенный и устойчивый экономический рост. Помимо факторов экстенсивного экономического роста (количественное увеличение факторов производства), существуют факторы интенсивного экономического роста, одним из которых является использование инноваций. В настоящее время для высокоразвитых стран инновации являются важнейшим фактором дальнейшего роста экономики.

Инновации чаще всего реализуются в формате инновационного проекта. Одними из важнейших факторов, влияющих на решение о реализации какого-либо проекта, является совокупность и уровень рисков, присущих данному проекту. Как известно, инновационные проекты обычно связаны с высоким уровнем риска и неопределенности. Поэтому для России, как для любого другого государства, дальнейшее инновационное развитие во многом зависит от выбора и реализации эффективных инновационных проектов, уровень рисков которых должен быть определен с использованием современной научной методологии оценки эффективности инвестиционных инициатив.

Приведем определение «инновационного риска», авторами которого являются М. В. Грачева и С. Ю. Ляпина: «*инновационный риск* – экономическая категория, отражающая возможность возникновения неблагоприятной ситуации или неудачного исхода инновационной деятельности предприятия, что проявляется в недостижении (неполном достижении) целей и задач» [2, с. 49].

В работе А. К. Газизулиной приведены следующие факторы, оказывающие негативное влияние на процесс осуществления инновационных проектов: высокий уровень неопределенности, недостаточный уровень научно-технического развития и, самое важное, «отсутствие в Российской Федерации сложившейся и действующей в рамках определенных международных стандартов инновационно-венчурной экосистемы, а также отсутствие единых

показателей для классификации и ранжирования инновационных проектов по эффективности их инвестирования» [1, с. 2].

Также наблюдаются проблемы, препятствующие инновационному развитию, в юридической сфере. И проблема не только в том, что отсутствуют законы, регулирующие инновационную деятельность, а в том, что некоторые законы могут не соблюдаться достаточно влиятельными лицами, что сильно бьет по доверию и уверенности у потенциальных инвесторов. Это уже проблема общественных институтов, а точнее, присутствие ряда «деструктивных» институтов.

Одним из главных рисков отечественных инновационных проектов может оказаться недостаток или отсутствие финансирования. Из-за санкций и контрсанкций экономика лишилась до половины потенциальных инвесторов: иностранные предприниматели и государства не могут или не хотят вкладывать средства в российские проекты, а иностранные банки – выдавать кредиты. Поэтому остается надеяться на отечественные источники финансирования инновационных проектов, но при нынешней ситуации у них, скорее всего, другие приоритеты.

Также следует упомянуть заключение А. К. Газизулиной: «В США выстроена система финансирования инновационных проектов, направленная на стимулирование инновационной предпринимательской активности. В России отсутствие подобной системы, несмотря на усилия по ее созданию и развитию со стороны государства, затрудняет инновационным организациям путь к выстраиванию своей ниши на рынке внутри страны» [1, с. 4]. Из чего можно предположить, что основным источником финансирования инноваций являются собственные средства организаций.

Становление в России в 90-х гг. XX в. рыночных отношений определило инновационную деятельность как основной способ развития российских предприятий независимо от формы собственности и сферы их деятельности. Но, к сожалению, сегодня очень небольшое число российских предприятий готово пойти на риск, связав свою деятельность с инновациями. Большинство предприятий все же нацелены на краткосрочную выгоду, нежели на получение устойчивого дохода и формирование постоянного рынка сбыта. Из чего можно сделать вывод о неутешительном состоянии не только инновационного развития России, но и экономического развития страны в целом в современных условиях. Для решения проблемы существования множества рисков инновационной деятельности необходимы не точечные исправления, а масштабные изменения на уровне общественных институтов.

Литература

1. Газизулина А. К. Особенности финансирования инновационных проектов: опыт России и США / А. К. Газизулина // Политехнический молодежный журнал. – 2022. – № 2(67). – DOI: 10.18698/2541-8009-2022-2-772.
2. Грачева М. В. Управление рисками в инновационной деятельности: учеб. пособие для студентов вузов, обучающихся по экономическим специальностям / М. В. Грачева, С. Ю. Ляпина. – М.: ЮНИТИ-ДАНА, 2010. – 351 с.

УДК 330

Бакуменко Мария Александровна
к.э.н., доцент
Волосовец Даниил Владимирович
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ДАШБОРДЫ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ВИЗУАЛИЗАЦИИ ДАННЫХ И ПРИНЯТИЯ СВОЕВРЕМЕННЫХ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Эффективность функционирования коммерческого предприятия во многом определяется правильностью и своевременностью принятых управленческих решений. А, как известно, для принятия грамотного управленческого решения необходим анализ данных о параметрах и динамике изменений показателей внешнего окружения хозяйствующего субъекта и его внутренней среды.

Для принятия управленческих решений важна численная информация, которая лучше всего воспринимается лицом, принимающим решения (ЛПР), в графическом представлении. Речь в данном случае идет о значимости визуализации данных.

В научной литературе отмечают «… значимость не только самой визуализации информации для процесса принятия решений, но и особенностей и характера результатов визуального представления» [1, с. 1]. Основная цель визуализации данных – «… обеспечение

поддержки пользователя в процессе восприятия, понимания и осмысления информации и формирования новых знаний, а также обеспечение минимизации усилий по выполнению когнитивных задач в сравнении с текстовым представлением данных» [1, с. 2].

Выделяют следующие методы визуализации данных [2, с. 50]: графики, диаграммы, презентации, инфографика, схемы, карты, картограммы, дашборды и др.

Одним из эффективных методов визуализации данных в сфере предпринимательской деятельности является построение дашбордов. Выделяют следующие основные виды дашбордов: тактические, стратегические и оперативные [3, с. 119].

Дашборд – лаконичный отчет с визуально представленными данными, который размещают на одном экране, содержащий важные аналитические показатели. Дашборд представляет собой совокупность графиков, текста, чисел, элементов инфографики. Отчет должен предоставлять рекомендации для пользователя и прогнозные данные [4, с. 837].

Выделяют следующие требования к построению дашбордов [5]:

- предоставление сведений в режиме реального времени;
- удобство восприятия;
- подключение различных источников данных;
- соответствие структуры дашборда информационным потребностям пользователей;
- отражение наиболее важных показателей;
- не перегруженность информацией;
- понятность диаграмм и графиков;
- грамотный выбор цветовых решений;
- правильное построение конструкции дашборда (ключевая информация, аналитика, детализация).

Применение дашбордов на отечественных предприятиях будет способствовать экономии времени на сбор, обработку и анализ информации, а также будет способствовать повышению скорости и качества принятия управленческих решений.

Литература

1. Афанасьев А. А. Технология визуализации данных как инструмент совершенствования процесса поддержки принятия решений / А. А. Афанасьев // Инженерный вестник Дона. – 2014. – № 4. – URL: http://ivdon.ru/ru/magazine/archive/n4y2014/2619 (дата обращения: 10.02.2023).
2. Фешина Е. В. Методы визуализации данных при проведении экономического анализа / Е. В. Фешина, А. П. Овчаров, В. Р. Лабинцева // COLLOQUIUM-JOURNAL. – 2018. – № 11-7 (22). – С. 49-52.
3. Колосов Р. Е. Дашборды мгновенной отчетности предприятия: перспективы применения / Р. Е. Колосов // Молодой учёный. – 2021. – № 33 (375). – С. 118-119.
4. Слотина Н. В. Dashboard для принятия бизнес-решений / Н. В. Слотина, С. И. Ультан // Молодёжь третьего тысячелетия. Сборник научных статей. – Омск. – 2020: Издательство: Омский государственный университет им. Ф.М. Достоевского. – С. 837-841.
5. Буряков И. Т. Дашборд: приемы эффективной визуализации / И. Т. Буряков, Е. В. Зубкова // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы IX Международной научно-практической очно-заочной конференции (Екатеринбург, 2 декабря 2021 г.) / ответственные за выпуск: А. Ю. Коковихин, Н. М. Сурнина; ответственный редактор В. В. Городничев. – Екатеринбург: УрГЭУ, 2022. – С. 63-65.

УДК 004.052(075.32)

Гиндес Елена Григорьевна
д.н.гос.упр., доцент кафедры государственного
и муниципального управления
Скопутова Алина Максимовна
обучающаяся 1 курса направления подготовки 38.03.01 Экономика
Институт экономики и управления
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СРЕДЫ

Любая информационная среда – это совокупность взаимосвязанных элементов, объединенных в единую систему [1]. Информационная система – это совокупность взаимосвязанной информации, инструментов, методов, персонала, используемых для хранения, обработки и предоставления информации и принятия управленческих решений. [2] В последнее время, принимая во внимание такие угрозы, как сбои, ошибки, неисправности, следует обратить внимание на исследование надежности внедрения информационных технологий в этой области.

Высокая надежность информационной среды позволяет избежать вышеуказанных угроз и автоматизировать работу системы.

Не следует забывать о безопасности. Именно она обеспечивает защиту информации, хранящейся в одном экземпляре, в том числе и личной, чтобы поддерживать порядок обмена данными. Стоит отметить, что распоряжение информацией в коммерческой сфере способствует экономическому развитию, а, следовательно, если не обезопасить информацию от посторонних пользователей, то кража данных станет частым происшествием, что приведет к ухудшению финансового положения владельца информации [3]. Если рассматривать в общем виде, то безопасность – отсутствие неприемлемого риска. Она помогает исключить ошибки персонала, появление злоумышленников и непредвиденные ситуации.

Естественно, необходимо обеспечить качественную защиту информационной среды, чтобы предотвратить ее неконтролируемое распространение. Принимая во внимание детали характера проблемы информационной безопасности, наиболее подходящие превентивные меры включают:

- повышение общего уровня информационной культуры населения страны и организация более качественной подготовки специалистов;
- четкое определение правового статуса значимых информационных объектов, исключающего бесконтрольное их использование;
- проведение комплекса научно-исследовательских и опытно-конструкторских работ по созданию программных и технических средств, в том числе и отечественных, обеспечивающих достаточную защищенность баз данных. Это стоит делать из-за того, что использование иностранных инвестиций и материалов имеет некоторые последствия. Например, зависимость рынка информации от иностранных разработчиков и появление монополий на мировом рынке информационной безопасности;
- подготовка достаточного количества специалистов, которые непосредственно занимаются разработкой новых технологий и программ, обеспечивающих защиту информации;
- налаживание эффективного взаимодействия правоохранительной системы РФ с международными организациями и правоохранительными органами зарубежных стран, которые способны регулировать правовые отношения в информационной среде и вести борьбу с компьютерными преступлениями и на совей территории, и за рубежом.

Надежность информационной среды – важнейшая составляющая сложнейшей системы, которой пользуется человек. Отсутствие конфиденциальности информации приносит моральный или материальный ущерб. Недостаточная защищенность от неправомерного владения конфиденциальной информацией ведет к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современном мире безопасность информационных ресурсов обеспечивается за счет их комплексной системной защиты. Благодаря ей владельцам информации не нужно беспокоится о сохранении информации, в том числе и личных данных, утечка которых недопустима. Именно из-за всех вышеперечисленных факторов, в нашей стране необходимо делать более весомый акцент на разработку всевозможных фильтров, защитных систем, наблюдателей систем.

Литература

1. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. – Москва : Издательство Юрайт, 2023. – 104 с.
2. Информационные системы и технологии в экономике : учебное пособие для вузов / О. Ю. Нетесова. – 3-е изд., испр. и доп. – Москва : Издательство Юрайт, 2022. – 178 с.
3. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2023. – 342 с.

УДК 004.056.53

Иванюта Дмитрий Викторович
аспирант
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНАЛЬНОЙ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СИСТЕМЫ

С начала открытой фазы геополитического противостояния на Украине системы информационной безопасности России подверглись небывалому давлению. Если ранее такое давление осуществлялось скрыто, теперь к кибератакам структуры недружественных стран подключились официально.

Введенные беспрецедентные антироссийские санкции значительно обострили ситуацию с кибербезопасностью, где наметилась острая необходимость противостоять глобальным и локальным киберугрозам [1].

Работа в условиях экстренного импортозамещения вывела на новый уровень роль и значение информационной безопасности региональных социально-экономических систем, потребовала грамотного и внимательного подхода к отечественным разработкам практически по всем направлениям, связанным с защитой данных [2].

Таким образом, на современном этапе государственное регулирование обеспечения информационной безопасности региональной социально-экономической системы с учетом технических особенностей диктует необходимость реализации следующих этапов:

- формирование команды специалистов, для реализации межотраслевого сотрудничества с целью совершенствования политики информационной безопасности и организации стратегического планирования в сфере информационной безопасности с учетом специфики всех отраслей экономики;
- организация взаимодействия государства и субъектов экономики для сбора актуальных данных, связанных с утечкой информации, координация действий в области обеспечения информационной безопасности федеральных и региональных органов власти;
- определение приоритетных направлений, целей, задач, оценки рисков и обеспечение эффективного реагирования на их возникновение, путем описания основных методов и построения моделей информационной безопасности социально-экономической системы;
- осуществление профилактики преступлений в информационной сфере на основании проведенного анализа;
- обеспечение непрерывного совершенствования нормативно-правовой базы информационной безопасности с учетом возникновения новых угроз сохранности данных;
- стимулирование исследований, применение инновационных систем обеспечения информационной безопасности, разработка рекомендаций по совершенствованию моделей информационной безопасности социально-экономической системы;
- внедрение российскими компаниями перспективных решений противодействия компьютерным атакам и наращивание взаимодействия государственных органов, бизнеса и науки по устранению уязвимости критической информационной инфраструктуры;
- обеспечение работоспособности отечественных продуктов на российских операционных системах и базах данных, предотвращение использования информационных технологий в военно-политических, террористических, преступных целях;
- формирование высококвалифицированного кадрового потенциала, имеющего специальные профессиональные навыки для обеспечения информационной безопасности во всех отраслях экономики [3].

Если компания не будет применять меры по системной защите от киберугроз, то она имеет все риски потерять стабильность и оказаться незащищенной перед современными вызовами, которые привнес мировой политико-экономический кризис.

Поэтому в случае, когда предприятие по каким-либо причинам оказалось не готово к быстрому переходу на российские аналоги, в качестве временного решения проблемы, специалистам по информационной безопасности на данных предприятиях требуется уделить больше внимания настройке систем информационной безопасности и ограничению удаленного доступа к информационным ресурсам. Также необходимо ужесточить политику безопасности паролей, включить полную мультифакторную аутентификацию без исключений, рассмотреть возможность облегчения нагрузки на серверы [4].

Таким образом, государственное регулирование обеспечения информационной безопасности региональной социально-экономической системы с учетом цифровой трансформации направлено на внедрение и использование перспективных российских цифровых технологий с использованием продвинутой аналитики и более сложных алгоритмов, позволяющих оперативно реагировать на внутренние процессы экономики с целью формирования эффективных стратегических инициатив [5].

В данном направлении обеспечение информационной безопасности является одной из первостепенных задач обеспечения устойчивого и направленного характера социально-экономического процесса при условии разработки комплексных программ и моделей обеспечения информационной безопасности.

Литература

1. Бойченко О.В. Новые виды мошенничества в цифровом пространстве/ О.В. Бойченко // В сборнике «Актуальные проблемы и перспективы развития экономики », 18 Всероссийская с международным участием научно-практическая конференция. – Симферополь: КФУ им. В.И Вернадского, 2019. – С. 10-12.

2. Бойченко О.В. Кибербезопасность в цифровизации экономики/ О.В. Бойченко// В сборнике «Теория и практика экономики и предпринимательства», 16 Всероссийская с международным участием научно-практическая конференция. – Симферополь: КФУ им. В.И Вернадского, 2019. – С. 7-10.
3. Бойченко О.В., Иванюта Д.В. Развитие социально-экономической системы Российской Федерации: в книге «Стратегическое управление развитием цифровой экономики на основе умных технологий»: монография / О.В. Бойченко, Д.В. Иванюта. – С-Пб. : Политех-пресс, 2021. – С. 10-28.
4. Бойченко О.В. Решение проблем сетевой информационной безопасности / О.В. Бойченко, // Актуальные проблемы и перспективы развития экономики: XVI Междунар. науч.-технич. конф., 20-22 апреля 2017 г.: тезисы докладов. – Симферополь, 2017. – С. 13-15.
5. Бойченко О.В. Защита клиентской базы предприятия при использовании CRM-систем / О.В. Бойченко, Е.С. Тупота // Актуальные проблемы и перспективы развития экономики: XIV Междунар. науч.-технич. конф., 12-14 ноября 2015 г.: тезисы докладов. – Симферополь, 2015. – С. 240-241.

УДК 351.004

Кравченко Лариса Анатольевна
к.э.н., доцент кафедры экономической теории
Субоч Дмитрий Викторович
обучающийся направления подготовки
38.03.01 Экономика
Институт экономики и управления
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Интенсивное развитие информационных и цифровых технологий, их повсеместное внедрение, в первую очередь на производстве, повлекли за собой серьезные структурные изменения в экономической и социальной сферах жизни общества, развитие новых форм бизнеса, возникновение совершенно новых рынков и рисков. Как показывает опыт последних лет, адекватность реагирования на внешние и внутренние информационные вызовы является одним из непременных условий безопасного функционирования всех сфер жизнедеятельности государства. Вызовами и угрозами в сфере информационной безопасности являются рост масштабов компьютерной преступности, в том числе международной, отставание Российской Федерации в разработке и использовании отечественного программного обеспечения, недостаточный уровень кадрового обеспечения в области информационной безопасности. Система стратегического планирования научно-технологического развития пока не сбалансирована по вертикали и горизонтали управления, соответствующие приоритеты нестабильны и слабо увязаны с ключевыми проблемами обеспечения национальной безопасности, включая диверсификацию экономики в пользу высокотехнологичных производств[1].

Информация, являясь продуктом деятельности, выступает как собственность государства, предприятий, учреждений, организаций, граждан и как объект собственности требует защищенности. Основы защиты информации разрабатываются органами государственной власти исходя из условий обеспечения информационной безопасности. Законодательные средства защиты информации представлены законодательными актами государства, которые регулируют правила использования, обработки и передачи защищаемой информации. Законодательные акты также предусматривают меры ответственности за нарушение правил обращения с информацией.

Информационная безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и иного характера, адекватных угрозам жизненно важных интересов личности, общества и государства. Поскольку в процессе развития информационных технологий, информационные ресурсы формируются во всех сферах деятельности, и в первую очередь в политической, военной, экономической, научно-технической, информационную безопасность следует рассматривать как комплексный показатель национальной безопасности. Этим определяется ее важное место и одна из ведущих ролей в системе национальной безопасности России в целом [2].

Государственная политика в сфере информационных технологий должна выстраиваться в логике регулирования тех сущностей, над которыми возможен физический контроль. Это приводит к идее отказа от запретов и фокусировке на локализации центров обработки данных на территории РФ с возможностью предоставления их услуг внешним заказчикам. В России в результате реализации государством направления «Информационная безопасность» будут обеспечены устойчивость и безопасность информационной инфраструктуры, конкурентоспособность отечественных разработок и технологий информационной безопасности

и выстроена эффективная система защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности. В 2022 году в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика» прошел запуске двух сегментов национального киберполигона – индустриального и ИТ. Созданные сегменты имитируют корпоративные сети организаций банковской системы, энергосистемы, а также инфраструктуру нефтегазовых предприятий. Цель киберполигона – подготовить специалистов по информационной безопасности, обучить их современным методам моделирования и отражения компьютерных атак. Введен в эксплуатацию отраслевой центр Минцифры РФ по отражению компьютерных атак – ГОССОПКА. Специалисты центра анализируют технологическую защищенность субъектов критической информационной инфраструктуры и проверяют на уязвимости государственные информационные системы. Задача центра – усилить технологическую устойчивость, исключить вероятность взлома систем и утечек информации. В перспективе ГОССОПКА станет координатором отражений компьютерных атак на ИКТ-инфраструктуру. Как сообщает Минцифры России, кроме того, в опытную эксплуатацию введена информационная система мониторинга фишинговых сайтов. С помощью данной системы уже выявляются интернет-страницы, которые содержат недостоверную информацию по определенным темам. Сведения о таких сайтах направляются в Роскомнадзор для последующей блокировки. С развитием нормативной базы информационная система станет полноценной платформой межведомственного взаимодействия в электронной форме заинтересованных органов и организаций для оперативной блокировки фишинговых сайтов. Изменения также касаются обезличивания персональных данных – это обязательная процедура для формирования датасетов, которые могут использоваться государством и компаниями для развития технологий искусственного интеллекта [3].

Таким образом, информация для государства – это, прежде всего, стратегический ресурс, определяющий функционирование различных сфер деятельности. Комплексное решение задач по обеспечению защищенности национальных информационных интересов можно обеспечить лишь при проведении единой государственной информационной политики. Важной задачей современного этапа информационной безопасности России и регионов является построение такой системы ее институциональной организации, которая была способна сбалансированно соединять инструменты государственной политики с возможностями частных предприятий, обеспечивала бы качественный уровень предоставления защиты от терроризма, финансовых рисков, правовой конкуренции и т. д. Необоснованная медлительность при разрешении стратегически значимых проблем в области обеспечения информационной безопасности является негативным фактором, снижающим эффективность государственного управления в целом.

Литература

1. Земляков Д.Н. Национальная инновационная система: особенности формирования и реализации на макро-, мезо- и на микроэкономическом уровнях (о книге Ю.Б. Винслава «Инновационное развитие экономики: проблемы государственного и корпоративного управления») // Российский экономический журнал. – 2021. – № 6. – С. 118–130.
2. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.
3. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации Электронный ресурс. – Режим доступа: https://digital.gov.ru/ru/events/41423/ (дата обращения 22.01.2023)

УДК 004.056

Круликовский Анатолий Петрович
доцент
Арифова Алиме Мустафаевна
обучающаяся
ФТИ ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БИЗНЕС-ПРОЦЕССЫ И ОБЕСПЕЧЕНИЕ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность в любой организации имеет огромное значение. Защита информации, сохранение ее элементов обеспечивается качеством оборудования и надежностью бизнес-процессов, проходящих внутри предприятия, то есть понятия «информационная безопасность» и «бизнес-процессы» тесно связаны друг с другом.

На данный момент существует тенденция ухода информационной безопасности от защиты конкретных систем, сервисов, серверов, к встраиванию в структуру самих бизнес-процессов, так как уже по другому невозможно обеспечивать их надежность. Необходимо детально разбирать

каждый бизнес-процесс и выстраивать не «навесную» информационную безопасность, а встроенную в сам бизнес-процесс. В работе Долганова О.И. [1] показано, что функции информационной безопасности, обеспечение безопасности самих бизнес-процессов сильно размыты, вследствие этого они распределены по большому количеству подразделений: здесь и внутренняя безопасность, и экономическая, и операционные риски, и службы внутреннего контроля, и внутренний аудит.

Для обеспечения безопасности информации требуется не только четко налаженная функциональная составляющая бизнес-процессов, но и качественное внедрение новых технологий. В связи с современными тенденциями поддержка информационной безопасности организаций тесно связана с внедрением информационных технологий в бизнес-процессы предприятий.

Прежде всего, должна существовать структура, который проводит непрерывную оценку рисков. Комплексную диагностику состояния компании удобнее всего проводить с помощью SWOT анализа (Strengths, Weaknesses, Opportunities и Threats). По мнению Кришталюка А. Н. [2] это позволяет узнать сильные и слабые стороны организации и выявить возможности и угрозы.

Выделяют три группы рисков в бизнес-процессах:

- риски при проектировании;
- риски при реинжиниринге;
- риски в процессе использования бизнес-процессов

Риски при проектировании и реинжиниринге бизнес-процессов бывают связаны с незавершенностью поставленных задач, несоответствием этих задач реальным возможностям, иерархической или «наследственной» несовместимостью, то есть конфликтами между основными и последующими процессами.

Ефимов Е. Н. и Лапицкая Г.М [3] считают, что операционный риск или риск в процессе использования бизнес-процессов можно определить как неверное исполнение обязанностей, неэффективного внутреннего контроля, различных технических сбоев и конечно же несанкционированных действий персонала и внешних факторов влияния.

Для устранения рисков используются различные системы, которые идентифицируют, анализируют и предотвращают потери в производственных процессах.

Описание бизнес-процессов, их моделирование, последующий контроль и анализ выполнения - постоянная и последовательная деятельность по устранению операционных рисков. Следовательно, устраняются и потери , поэтому совершенствование бизнес-процессов неотъемлемо связана с обеспечением информационной безопасности.

Литература

1. Долганова, О.И. Моделирование бизнес-процессов: Учебник и практикум для академического бакалавриата / О.И. Долганова, Е.В. Виноградова, А.М. Лобанова. - Люберцы: Юрайт, 2016. - 289 с.
2. Кришталюк А.Н. Управление безопасностью бизнеса. Курс лекций / А.Н.Криштанюк. – Орел, 2014. – 90 с.
3. Организация информационной защиты бизнес-процессов [Электронный ресурс] // Cyberleninka, 2016. Режим доступа: https://cyberleninka.ru/article/n/organizatsiya-informatsionnoy-zaschity-biznes-protsessov (дата обращения: 25.01.2023).

УДК 004.056.5

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Бурячек Екатерина Игоревна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РОЛЬ HR В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Кибербезопасность занимает важное место в деятельности любой компании. Нарушения становятся все более распространенными из-за широкого использования цифровых хранилищ и облачных вычислений. Со времен увеличения удаленной работы из-за пандемии, киберпреступникам была предоставлена еще большая возможность атаковать уязвимые компании. Количество атак увеличилось на 14,8% по сравнению с данными 2021 года. При этом увеличилась доля массовых атак: их количество составляет 33% от общего числа. Чаще всего в результате атак организации сталкиваются с утечкой конфиденциальной информации (45%) и нарушением основной деятельности (30%) [1].

Огромное количество нарушений кибербезопасности происходят из-за человеческой ошибки. Как показано в работе Е.К. Барановой [2], специалисты в области управления персоналом обрабатывают множество конфиденциальных данных организации, которые включает в себя личную информацию сотрудника, сведения о зарплате, банковские реквизиты, даты рождения, контактные данные и т. д., В случае утечки они могут нанести огромный ущерб

Таким образом, специалисты по управлению персоналом имеют возможность предотвращения этих угроз. HR-отделы должны уделять большое внимание безопасности при найме и внедрении сотрудников и обеспечении соблюдения политики конфиденциальности данных.

HR относится к отделу, который управляет жизненным циклом каждого сотрудника. Процесс приема, найма, адаптации, обучения и увольнения сотрудников, а также администрирование льгот для сотрудников.

Повышая надежность адаптации, обучения, мониторинга и коммуникации в области кибербезопасности, HR-специалисты могут значительно снизить риск дорогостоящих утечек данных. В работе М.К. Бойдало [3] показано, что специалисты по персоналу компании должны убедиться, что сотрудники соблюдают политики безопасности, разработанные для защиты компании, ее клиентов и сотрудников.

Персонал компании подвергается большинству кибератак, отдел кадров вместе с ИТ-командой могут сыграть ключевую роль в борьбе с возможными угрозами кибербезопасности. Это причина, по которой ИТ и HR должны работать в команде. Поскольку данные, с которыми имеют дело сотрудники отдела кадров, очень подвержены атакам на безопасность.

Прежде чем разрабатывать превентивную стратегию, специалистам по персоналу необходимо определить потенциальные киберугрозы. Сегодня огромное количество предприятий имеют передовые программные решения для снижения рисков внешних кибератак, таких как вирусы или вредоносные программы. Фишинг является одним из таких примеров внешней киберугрозы, когда имитатор обманывает сотрудников, чтобы получить важную информацию, часто по электронной почте.

Один из наиболее эффективных приемов предотвращения киберугроз - обучить весь персонал отдела кадров протоколам кибербезопасности. Это необходимо для вновь принятых сотрудников. Обучение должно быть неотъемлемой частью процесса внедрения, в ходе которого вновь набранные сотрудники получают инструкции по вопросам, связанным с использованием конфиденциальных данных и доступом к ним, наряду с предоставлением им базовой подготовки по кибербезопасности. В работе К.Н. Дорофеева, Е.В Гараевой [4] обращено внимание что сотрудники отдела кадров должны убедиться, что вновь принятые на работу сотрудники не владеют какими-либо конфиденциальными данными бывшего работодателя.

Высококвалифицированные специалисты по безопасности пользуются большим спросом. Ни одна организация не застрахована от киберпреступности, а это означает, что ИТ-безопасность необходимо сделать одним из главных приоритетов. Первым шагом является поиск наиболее квалифицированных специалистов, которые будут руководить [5].

Специалисты по персоналу отвечают за обеспечение соблюдения сотрудниками политик безопасности, разработанных для защиты как самого предприятия, так и клиентов и сотрудников. Помимо информирования сотрудников о политике и процедурах компании, представители отдела кадров должны сотрудничать с руководством для расследования и устранения любых случаев, связанных с нарушениями этих правил.

Литература

1. Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (Дата обращения: 03.02.2023.)
2. Баранова, Е.К. Информационная безопасность и защита информации. Учебное пособие / Е.К. Баранова. - М.: Инфра-М, РИОР, 2019. - 368 с.
3. Бойдало, М.К. Метод и модель оценки профессионального соответствия персонала в вопросах обеспечения информационной безопасности / М.К. Бойдало, Г.П. Жигулин // Научно-технический вестник Поволжья. - 2019. - №3. - С. 66-71.
4. Дорофеев, К.Н. Кадровая безопасность в системе экономической оценки деятельности фирмы / К.Н. Дорофеев, Е.В Гараева // Журн. Молодой ученый. - 2018. - №6. - С. 327-331.
5. Снитко, Л.Т. Кадровая безопасность в системе экономической безопасности предприятия / Л.Т. Снитко // Вестник Белгородского университета кооперации, экономики и права. 2017. № 5 (61). С. 9-23.

УДК 338.2

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Гладышева Юлия Алексеевна
обучающаяся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

РАЗРАБОТКА ПРОЕКТА СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ С ИСПОЛЬЗОВАНИЕМ МЕТОДА СБАЛАНСИРОВАННЫХ ПОКАЗАТЕЛЕЙ

В мире цифровых бизнес-процессов защитить данные и информацию уже не так просто. Сегодня важная и конфиденциальная информация может быть разбросана по организации. Защита данных стала системной, вышедшей за пределы одного отдела предприятия, теперь она затрагивает каждого сотрудника и каждый процесс. Разрабатывая план стратегического управления важно учитывать информационную безопасность во всех частях организации.

Умение организации проводить самостоятельную стратегию во всех областях делает ее более защищенной, устойчивой, дает возможность адаптироваться к требованиям времени и обстоятельствам. В качестве инструмента для реализации и контроля внедрения стратегического управления Каплан и Нортон [2] в 1992 году предложили метод сбалансированных показателей. Таким образом, рассмотрение разработки проекта стратегического управления предприятием с использованием метода сбалансированных показателей является актуальным вопросом.

Под управленческой стратегией понимается основанная на анализе и прогнозе общая концепция того, как достигаются главные цели фирмы, решаются стоящие перед ней проблемы и распределяются необходимые для этого ограниченные ресурсы. Данная стратегия дополнена программой реальных действий, направленных на приобретение конкурентных преимуществ, достижения победы в конкурентной борьбе [1, С. 9]. Но это не только рассчитанная на перспективу концепция действий, но и способ мышления менеджеров и персонала.

Сбалансированная система показателей (ССП, BSC, Balanced Scorecard) — это система стратегического управления компанией на основе измерения и оценки ее эффективности по набору оптимально подобранных показателей, отражающих все аспекты деятельности организации: финансовые, производственные, маркетинговые, инновационные, инвестиционные, управленческие [2].

ССП обобщает реальные проблемы компании, нарушающие сбалансированную работу системы стратегического управления. Систематизация этих проблем позволяет разработать конкретные шаги по их устранению.

Для визуального отображения связи стратегических целей и перспектив используют стратегическую карту. Подобная оценка ситуации поможет принять взвешенные решения, исключив доминирование одной части организации в ущерб другим. Стратегические карты представляют собой диаграмму, отражающую направление развития компании и связывающую показатели эффективности и инициативы со стратегией компании. Для каждой точки зрения (проекции) существует набор целей. Меры в ССП соответствуют поставленным целям и задачам. План действий связан с целями и соответствующим им бюджетом.

Для построения проекта стратегического управления необходимо разбить стратегию организации на конкретные стратегические цели, детально отображающие различные стратегические аспекты. При интеграции индивидуальных целей могут быть установлены причинно следственные связи между ними таким образом, чтобы полный набор целей отображал стратегию компании. По мнению Беликовой И. П. [1, С. 29] - не следует определять слишком большое число стратегических целей для корпоративного уровня организации.

Сущность ССП заключается в формулировании стратегии в проекциях (или перспективах), постановке стратегических целей и измерении степени достижения данных целей при помощи показателей. Чаще всего выделяют следующие четыре проекции:

1) Проекция «Финансы» (или управление): рассматривает финансовые показатели организации и использование финансовых ресурсов (здесь важно уделить внимание защите финансовой информации, движению денежных средств, также информации о тратах клиента и т.д.).

2) Проекция «Клиент»: рассматривает эффективность организации с точки зрения клиента или ключевых заинтересованных сторон, для обслуживания которых предназначена организация (здесь рационально будет уделить внимание защите от утечки информации о статусе клиента, его возрасте, истории покупок, адресе, почте, телефоне и т.д.).

3) Проекция «Внутренние бизнес-процессы»: просмотр качества и эффективности работы организации, связанной с продуктом, услугами или другими ключевыми бизнес-

процессами (здесь важно уделить внимание защите информации, содержащей внутреннюю информацию, например, о разработке продукта или услуги, об управлении и т.д.).

4) Проекция «Обучение и развитие»: рассматривает человеческий капитал, инфраструктуру, технологии, культуру и другие возможности, которые являются ключевыми для прорывной производительности (здесь будет необходимо уделить внимание защите от утечки информации об уровне знаний сотрудников, специально разработанные учебные планы и т.д.) [3].

Также важно отметить, что при построении стратегического плана перспективы могут изменяться в зависимости от деятельности компании - расширяться, включая иные пункты.

Успех в бизнесе требует постоянной адаптации компании к окружающей среде, быстрой реакции на появляющиеся угрозы. Разработка проекта стратегического управления предприятием с использованием метода сбалансированных показателей позволит оперативно защищать информационные ресурсы во всех областях организации, развиваться в соответствии с имеющимися перспективами и поставленными долгосрочными целями.

Литература

1. Беликова, И. П. Основы стратегического управления : учебное пособие / И. П. Беликова, В. А. Ивашова. — Ставрополь : СтГАУ, 2020. — 128 с.

2. Каплан, Р. Организация, ориентированная на стратегию. Как в новой бизнес-среде преуспевают организации, применяющие сбалансированную систему показателей / Р.Каплан, Д. Нортон. – М. : Олимп-Бизнес, 2005. – 416 с.

3. Balanced Scorecard Basics [Электронный ресурср], — Режим доступа: https://balancedscorecard.org/bsc-basics-overview (дата обращения: 06.02.2023).

УДК 004.056

Ластовецкий Григорий Николаевич
обучающийся 1 курса
направления подготовки 38.03.01 Экономика
Прибыщук Глория Данииловна
обучающаяся 1 курса
направления подготовки 38.03.01 Экономика
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

РОЛЬ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВЕ

Кибербезопасность (информационная безопасность) - это такая совокупность действий и методов для борьбы с атаками злоумышленников, предназначенная для персональных компьютеров, мобильных устройств, серверов и в том числе для обеспечения информационной безопасности государственных структур.

Все киберугрозы делятся на три типа: первый тип- киберпреступление (выполняемое одним человеком или парой людей с целью извлечь материальную выгоду); второй тип- кибератака (совершаются в основном для сбора информации в политических или военных целях); третий тип - кибертерроризм (совершается для дестабилизации крупных систем с целью вызвать панику). Само понятие “Кибербезопасность” появилось в официальных документах только в начала XXI века, и в наши дни является неотъемлемой частью нормального существования любого государства [1, С.9]. Вместе с этим понятием появилось и киберпространство, которое признано многими странами новым полем боевых действий[3, С.2]. К такому выводу пришло большинство руководителей государств, так как кибератаки по мощности ничуть не уступают военной агрессии, ведь с их помощью можно полностью разрушить, например, целую систему управления развитой страны или коммуникации между государственными структурами, что создаст панику и внутренний дисбаланс.

В России термин “кибербезопасность” не был закреплен каким-либо нормативно правовым актом и наша страна только начала развиваться в этом направлении, несмотря на то, что отсутствие такого рода защиты может привести к ужасающим последствиям [4, С.11].

Подводя итоги, можно отметить, что роль кибербезопасности велика в любом государстве, ведь, в случае столкновения интересов некоторого государства, при недостаточном ее развитии, любая страна может попасть под сильнейшие кибератаки, после которых придется долгое время пройти процесс восстановления [2, С.13].

Литература
1. Алексеев Г., Смирнов И. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств, Зарубежное военное обозрение, №6, 2017 г., С.8-14.
2. Паршин С. Взгляды научного комитета МО США на классификацию угроз в киберпространстве. Зарубежное военное пространство, №5, 2017 г., С.12-17
3. Ромашкина Н.П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5(39)
4. Бородакий Ю.В., Бутусов И.В., Добродеев А.Ю. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2). Вопросы кибербезопасности, №1 (2), 2014 г., С.5-12.

УДК 004.056.

Мазурская Алина Владимировна
обучающаяся 1 курса направления
подготовки 38.03.01 «Экономика»
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
г. Симферополь, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИЯХ

В современном мире информация является значимым ресурсом, ее сохранность и правильное использование являются одними из первоочередных задач для развития организации и производства и снижения уровня разнообразных рисков. Важнейшим актуальным вопросом для предприятия является вопрос информационной безопасности.

Следование правилам информационной безопасности позволяет защитить информацию на предприятии и предотвратить сбои в работе существующей бизнес-системы. Прежде чем начать разработку стратегического плана безопасности, важно понять, какие цели должна преследовать система защиты и какие есть уязвимости деятельности предприятия. Стратегия безопасности – это комплексный подход, состоящий из организационных, технических и инженерных мер, которые в конечном счете поддерживают работу системы безопасности [1].

Каждая сетевая услуга, которую использует или предоставляет организация, создает риски для всей системы и сети, к которой она подключена. Создание комплексной системы защиты невозможно без политики безопасности. Политика безопасности – это набор правил, которые применяются ко всем функциям компьютеров и других коммуникационных ресурсов, принадлежащих организации. На практике правила создаются службой безопасности предприятия, администратором безопасности или компаниями, которые предоставляют услуги по защите данных. Все правила, указанные в политике безопасности, должны применяться к сотрудникам, компьютерам и другим вычислительно-коммуникационным ресурсам, которые принадлежат организации [2].

Правила информационной безопасности включают в себя:

– создавать персональные (уникальные) пароли к разным сервисам;

– использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы;

– доверять только проверенным менеджерам, сотрудникам и партнёрами;

– сотрудникам следует отключать доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет;

– сотрудникам предприятия нужно деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам, чтобы злоумышленник не проник через сеть к закрытой информации предприятия.

Схема защиты ресурсов должна гарантировать, что только авторизованные пользователи могут получить доступ к объектам системы. Возможность защиты всех типов системных ресурсов является основным показателем ее прочности. Служба безопасности должна определить разные категории пользователей, которые могут получить доступ к вашей системе. Кроме того, следует продумать, какую авторизацию доступа нужно предоставить этим группам сотрудников в рамках создания политики информационной безопасности предприятия [3].

Литература
1. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: доклад Генерального секретаря от 10 июля 2000 г. A/55/140. – Текст: электронный // Организация Объединенных Наций : официальный сайт. – 2021. – URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/535/04/PDF/N0053504

2. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности : записка Генерального секретаря от 30 июля 2010 г. A/65/201. – Текст : электронный // Организация Объединенных Наций : официальный сайт. – 2021. – URL : https://www.un.org/ga/search/view_doc
3. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. – Текст : электронный // Совет Безопасности Российской Федерации : официальный сайт. – 2021. - URL: http:// www.scrf.gov.ru/security/information/document5/

УДК 004.056

Макаров Даниил Дмитриевич
обучающийся 1 курса
направления подготовки 38.03.01 Экономика
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

ОЛИГОПОЛИЯ. СИТУАЦИЯ НА СОВРЕМЕННЫХ РОССИЙСКИХ РЫНКАХ

Олигополия – это одна из моделей рынка, при которой производство или продажа определенного продукта осуществляется немногочисленными крупными корпорациями.

Как правило, олигополии возникают естественным путем, на рынках, где продукция является либо узконаправленной, труднореализуемой с технической точки зрения или которая требует огромных финансовых вложений, а иногда и все вышеописанное.

Такие структуры характерны для рынков: судо-, авиа-, ракето-строительства, фармацевтики, брендовой одежды, индустрии развлечения, быстрого питания, табачной продукции и так далее.

Также, выделяют два основных вида олигополии – это однородная и дробная.

При однородной олигополии компании торгуют одним и тем же товаром со схожими параметрами, но ограниченным ассортиментом. Из примеров можно привести компании по продаже чая, кофе, сахара, драгоценностей, строительных материалов, сотовой связи.

При дробной же олигополии корпорации предлагают схожий по своей природе товар, но при этом в более детальном рассмотрении отличающийся от товара конкурентов. В пример можно привести компании по производству техники (начиная от смартфонов и гарнитуры, заканчивая условными холодильниками), автопром (по своей природе и там и там машина, но «начинка» является разной).

В настоящее время, в России, большинство российских олигополистических компаний являются «преемниками» крупных советских предприятий. Сохранив прежний курс деятельности, они кардинально изменили ее социально экономическое содержание.

Если раньше предприятия Советского союза ставили задачу на удовлетворение потребностей большинства путем выпуска необходимой продукции, то в нынешних реалиях олигополисты нацелены на извлечение максимальной прибыли от продукции.

Поскольку Россия в большинстве своем специализируется на добыче полезных ископаемых, то и количество олигополистических компаний сконцентрированы в этой сфере. К ним относятся: ЛУКОЙЛ, НК Роснефть, Газпромнефть, Сургутнефтегаз. Их доля добычи нефти и газа в 2013 году составила 77,6%.

Подводя итоги, можно отметить, что олигополия довольно частое явление на современных экономических рынках. Среднестатистический потребитель имеет вероятность столкнуться с повышенными ценами на товар при олигополии, но цена в любом случае будет ниже цены, которая была бы при монополии, поскольку все еще существует конкуренция между другими компаниями.

Литература

1. Бузгалин А.В. Трансформационный характер российской экономики: историческое место и закономерности развития // Философия хозяйства. 2005. №4/5(40 – 41)
2. Доклад о состоянии конкуренции в Российской Федерации [Электронный ресурс]. М., 2015. URL: http://fas.gov.ru
3. Сидоренко, Е. А. Особенности конкуренции на российском рынке услуг мобильной связи / Е. А. Сидоренко, Р. Д. Власенко — № 10 (114). — С. 870-873. — URL: https://moluch.ru/archive/114/30250/
4. Леонтьева, А. В. Трансакционные издержки в олигополиях / А. В. Леонтьева. // Молодой ученый. — 2014. — № 17 (76). — С. 293-295. — URL: https://moluch.ru/archive/76/12364/

УДК 330

Ремесник Елена Сергеевна
к.э.н., ст. преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Алтухова Юлия Петровна
начальник отдела правовой, кадровой и организационной работы
Марченко Людмила Евгеньевна
преподаватель
ГБУ ДПО РК «ЕЦ ПО в сфере закупок»
Республика Крым, Россия

РАЗВИТИЕ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В РОССИИ

Внедрение автоматизированных информационных систем в Российской Федерации (РФ) получило свое начало в 1994 году, когда Главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте России разработан первый российской стандарт электронной цифровой подписи — ГОСТ Р 34.10.-94, а в 1995г. принят Федеральный закон «Об информации, информатизации и защите информации» (на данный момент, утратившим силу) [1], что повлекло документирование информации в установленном порядке, при этом юридическую силу документов, включенных в информационные ресурсы, могла подтвердить электронная цифровая подпись (ЭЦП).

Первым и главным законом по использованию ЭЦП стал Федеральный закон «Об электронной цифровой подписи» [2], в котором давалось определение понятию ЭЦП. Правовое значение электронной подписи определено в ст. 160 Гражданского кодекса Российской Федерации, согласно которого, электронная подпись является аналогом собственноручной подписи.

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ФЗ-63), который отменил Федеральный закон «Об электронной цифровой подписи» [3], разделяет электронную подпись (ЭП) на три вида: простая ЭП, усиленная неквалифицированная и усиленная квалифицированная (рис.1). Каждая из видов подписи имеет свой уровень и возможности доступа.

Простая электронная подпись используется только физическими лицами и может являться паролем или логином для входа в личные электронные кабинеты, электронную почту, социальные сети.

Усиленная неквалифицированная ЭП будет являться более надежной, чем пароль в простой ЭП и применяется с помощью хранения ЭП на цифровом носителе (USB- флешка).

Усиленная квалифицированная подпись является самой защищенной, хранится на специально разработанных защищенных токенах и может быть выдана только специализированным удостоверяющим центром. Именно удостоверяющий центр будет выступать гарантом подлинности (достоверности) выданной электронной подписи.

В настоящее время широкое применение ЭП получила в электронном документообороте между организациями в том числе при обмене «первичными» бухгалтерскими, а также при сдаче электронной отчетности в ФНС, ФСС (отдельно следует отметить инициативность Федеральной налоговой службы), в сфере финансов (проникновение систем интернет-банкинга).

Национальная программа «Цифровая экономика Российской Федерации» [4] способствует цифровой трансформации всех социально-экономических сфер и ещё большему внедрению ЭП.

С 1 сентября 2023 года планируется перевести кадровый документооборот организаций в электронный документооборот, при котором работник подписывает документы своей ЭП как физлица [5].

ЭП всё больше применяется и в сфере образования, так Приказ Федеральной службы по надзору в сфере образования и науки РФ от 14 августа 2020 г. N 831 "Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления информаци [6], регламентирует к структуре официального сайта образовательной организации ряд требований, например, документы размещенные на сайте должны быть подписаны ЭП соответствующей условиям статьи 6 ФЗ-63 для их признания равнозначными документам на бумажном носителе, подписанным собственноручной подписью. Для борьбы с поддельными документами об образовании создана федеральная информационная система «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (ФИС ФРДО), в которую образовательным учреждением вносятся документы об образовании, квалификации. Для внесения информации в такой реестр, образовательной организации нужна усиленная квалифицированная ЭП.

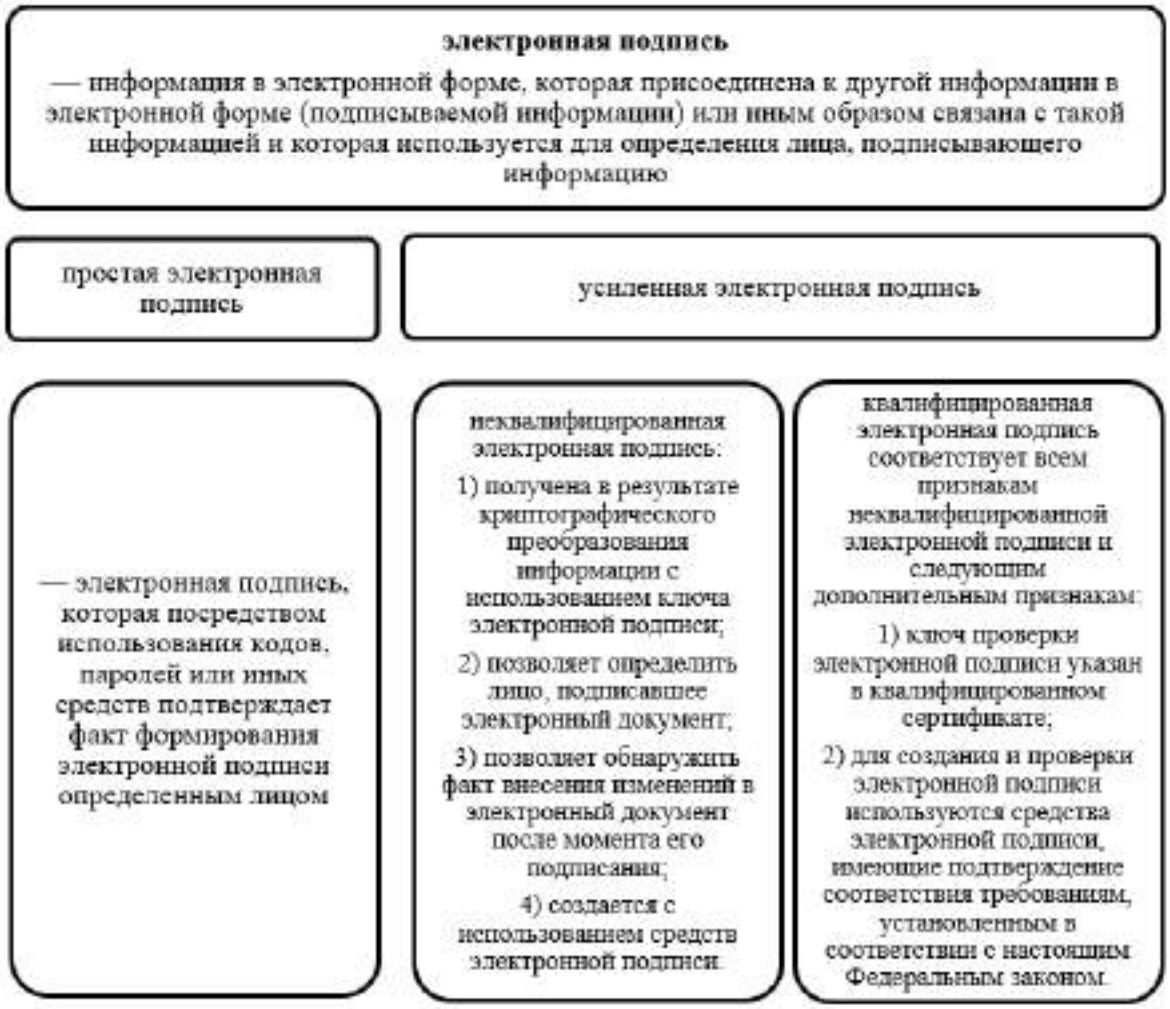

Рисунок 1 – Виды электронных подписей

Медицина тоже не отстает от цифровизации. Согласно приказа Министерства здравоохранения РФ с 1 февраля 2021г. [7] медицинские организации обязаны организовать электронную форму медицинских документов. Имеется национальный стандарт ГОСТ Р 52636-2006 «Электронная история болезни» [8], содержащий требования к электронному варианту медицинской карты пациента. Для подписания электронных медицинских документов чаще всего используется два вида квалифицированных ЭП: ЭП медицинского учреждения (для юридических лиц) и ЭП врача (для физических лиц).

При использовании ЭП также есть определенные риски. Одним из которых является риск, связанный с несанкционированным доступом, то есть применение без ведома владельца. Поэтому очень важно, чтобы каждая организация придерживалась комплекса правовых и организационно-технических мер обеспечения информационной безопасности, в том числе такие как:

- передавать ЭП, принадлежащую физическую лицу, другому лицу – нельзя;
- при увольнении работника у которого ест ЭП, организации надо отозвать сертификат ЭП;
- токен с подписью и компьютер, на котором он используется, должен быть защищен дополнительно паролем;
- защита от вирусов компьютера, на котором используется ЭП;
- сканы паспортов физических лиц, их реквизиты передавать или оставлять иным лицам – нельзя.

Литература

1. Федеральный закон "Об информации, информатизации и защите информации" от 20.02.1995 N 24-ФЗ [Электронный ресурс].
URL: http://www.consultant.ru/document/cons_doc_LAW_5887/ (дата обращения 07.02.23)
2. Федеральный закон "Об электронной цифровой подписи" от 10.01.2002 N 1-ФЗ [Электронный ресурс].

URL: http://www.consultant.ru/document/cons_doc_LAW_5887/ (дата обращения 07.02.23)
3. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения 07.02.23)
4. Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 07.02.2023)
5. Электронная подпись (ЭЦП) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Электронная_подпись_(ЭЦП) (дата обращения 05.02.23)
6. Приказ Рособрнадзора от 14.08.2020 N 831 (ред. от 12.01.2022) "Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления информации" (Зарегистрировано в Минюсте России 12.11.2020 N 60867) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_367746/ (дата обращения 07.02.23)
7. Приказ Министерства здравоохранения РФ от 7 сентября 2020 г. N 947н “Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов” [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/400083202/ (дата обращения 07.02.23)
8. Электронная история болезни. Общие положения. [Электронный ресурс]. URL: https://files.stroyinf.ru/Data2/1/4293844/4293844841.pdf (дата обращения 07.02.23)

УДК 004.056

Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Тышко Мирон Вадимович
Домашенко Анастасия Павловна
студенты 1 курса
направления подготовки «Экономика»
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В современных условиях функционирования частного сектора экономики, информационная безопасность является неотъемлемой частью его системы управления, от которой в конечном результате зависит комплексная экономическая безопасность предприятия. Потребность в защите информации обуславливается в первую очередь с развитием цифровых технологий и возможностей.

Информационная безопасность – это всесторонняя защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. [1]. Следовательно, обеспечение полноценной информационной безопасности предприятий подразумевает под собой непрерывный контроль в реальном времени всех важных событий и состояний, влияющих на безопасность данных.

Важно отметить, что для наибольшей эффективности система должна охватывать весь цикл информации (от ее поступления до уничтожения), при это защита данных должна осуществляться круглосуточно.

Обеспечение информационной безопасности на предприятии возможно только при комплексном подходе к защите. В данной системе должны учитываться все актуальные компьютерные угрозы и уязвимости.

Если компьютерная сеть предприятия будет взломана, злоумышленник получит доступ к информации и нанесёт этим вред. В качестве наиболее распространённой информационной безопасности предприятия являются DDoS-атаки. Киберпреступниками данные варианты сегодня применяются как в отношении крупных предприятий, так и небольших компаний в самых различных сегментах экономики.

Повреждение информации, атаки, кража, фальсификация данных – все это может негативно сказываться на различных факторах компании. Возможны финансовые потери из - за плохой репутации, затрат на возобновление работы системы, потери важных данных, которые могут быть ключевыми в гонке с конкурентами[2].

Безопасность системы на данный момент достигается на основе трех основных компонентов, основными из которых являются:

1. Целостность – это обеспечение состояния информации, при этом они останутся неизмененными и корректными. Обеспечение целостности информации предполагает предотвращение любого ее изменение либо изменение осуществляется только лица, которые имею на нее право.

2. Конфиденциальность информации – это гарантия того, что данные не будут прочитаны и интерпретированы теми людьми и процессами, которые не авторизованы это делать. В качестве примера можно привести: повреждение информации, утечка и ее незаконное разглашение другим лицам.

3. Доступность информации – означает, что сведения используется только сотрудниками, имеющими на это право[3].

Следует отметить, что невыполнение одного из вышеперечисленных компонентов может привести к нарушениям в работе информационной системы и к негативным последствиям в деятельности предприятия, такой как: утечка информации, что в конечном итоге может привести к финансовым потерям.

Процесс построения эффективной системы защиты информации обязательно включает самым тщательным образом проведенную идентификацию возможных источников угроз, а также факторов и причин, способствующих их появлению. Результатом такого анализа должен явиться полный перечень актуальных угроз информационной безопасности предприятия. Сформированное представление о потенциальных угрозах, имеющихся уязвимостях, которыми могут воспользоваться злоумышленники, обеспечит возможность выбора наиболее эффективных, но в тоже время экономически целесообразных средств защиты [4].

В России существует тенденция по переманиванию ведущих специалистов по кибербезопасности из компаний, специализирующихся на борьбе с киберугрозами, в крупные российские корпорации с целью выстраивания собственной модели ИБ, избегая рисков утечки данных, ожидаемых при работе с подрядчиками. О существовании таких рисков информационной безопасности банки предупреждает ЦБ РФ, издав специальный стандарт по правилам работы с аутсорсерами, будут они актуальны и для предприятия [5].

Для защиты информационной безопасности, государственная политика направлена на поддержку национального производителя и побуждает руководителем переходить на российское программное обеспечение. Наиболее актуально – это для небольших предприятий, так как оно достаточно надежное, при этом обладает высоким уровнем надежности.

Таким образом, одной и самых современных и актуальных проблем на предприятии – это защита данных, в настоящее время крайне важно учитывать все нюансы информационной безопасности с учетом постоянно усложняющихся рыночных отношений. Важно отметить, что правильный выбор системы защиты информации позволит минимизировать риски утечки конфиденциальных данных предприятия и положительно отразится на конечных показателях его финансово-хозяйственной деятельности.

Литература

1. Информационная безопасность в компании: [Электронный ресурс]. — Режим доступа: https://www.tadviser.ru/index. (Дата обращения: 27.01.2023).
2. Абдуллин, А. А. Информационная безопасность на предприятии / А. А. Абдуллин, С. А. Тимерханова // Современные научные исследования и разработки. – 2019. – № 1(30). – С. 55-56.
3. Ложкова, Ю. Н. К вопросу информационной безопасности современных предприятий / Ю. Н. Ложкова // Дневник науки. – 2019. – № 3(27). – С. 75.
4. Байгулов, Р. М. Основные угрозы информационной безопасности предприятия / Р. М. Байгулов, А. Г. Сковиков, Н. А. Сковиков // Вестник Московского гуманитарно-экономического института. – 2021. – № 3. – С. 26-35.
5. Примеры информационной безопасности предприятия: [Электронный ресурс]. — Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/primery-informatsionnoj-bezopasnosti-predpriyatiya/ (Дата обращения: 29.01.2023).

УДК: 351/354:004

Смерницкая Евгения Владимировна
к.э.н., доцент
Институт развития города
ФГАОУ ВО «Севастопольский государственный университет»
г. Севастополь, Россия

АКТУАЛЬНОСТЬ ЦИФРОВИЗАЦИИ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННОЙ ПОДДЕРЖКИ В РЕГИОНЕ

Инфраструктура государственной поддержки субъектов предпринимательства в Республике Крым представлена системой коммерческих и некоммерческих организаций. Данные субъекты осуществляют свою деятельность для обеспечения реализации государственных программ и проектов, обеспечивающих условия для создания субъектов малого и среднего предпринимательства, а также для оказания им, различного рода поддержки.

Государственная поддержка в Республике Крым является уже на протяжении девяти лет общепринятым инструментом в развитии предпринимательства в регионе. Начиная с 2014 года такая форма государственной поддержки как льготное налогообложение доходов юридических лиц была первой формой проявления. Консультационная помощь, в процессе перехода, юридических лиц в правовое предпринимательское поле и нормативно-правовое сопровождение также были одни из первых форм государственной поддержки. Создание свободной экономической зоны, выделение средств, на тот момент, через отраслевые министерства и ведомства, для того чтобы региональные товаропроизводители не покинули свой бизнес, а могли сосредоточится на его развитии.

На сегодняшний день инфраструктура государственной поддержки бизнеса в Республике Крым представлена совокупностью объектов, которые обеспечивают ее функционирование. Значительное количество государственных учреждений на разных уровнях управления оказывает государственную помощь в развитии малого и среднего предпринимательства в регионе. Более того, хочется отметить, что предоставление помощи происходит во всевозможных формах и с помощью многочисленных инструментов.

Инвестиционный портал Республики Крым предоставляет финансовую поддержку, а именно: микрозаймы размером до 5 миллионов рублей; предоставление поручительств; юридические и бухгалтерские консультации; лизинг; экспорт.

Фонд поддержки предпринимательства работает в различных направлениях развития предпринимательства в регионе, касаемо государственной поддержки. В большей мере оказывает консультационную, образовательную форму поддержки, что включает в себя: бесплатные консультации; обучающие программы, форумы, тренинги, семинары; разработка бизнес-плана предпринимательского проекта, социального проекта; поддержка участников кластеров; выстави и конкурсы и пр.

Центр кластерного развития Республики Крым в качестве государственной поддержки предоставляет такие услуги субъектам малого и среднего бизнеса, как: продвижение товаров и услуг; упаковка новых проектов; правовые консультации; сертификация; маркетинговые услуги; разработка технико-экономических обоснований пр.

Достаточно большое количество именно финансовой поддержки поступает через отраслевые министерства Республики.

Министерство имущественных и земельных отношений Республики Крым обеспечивает предоставление отсрочки по арендной плате по действующим договорам аренды имущества и земельных участков собственности Республики Крым.

Министерство сельского хозяйств оказывает государственную поддержку личных подсобных хозяйств, агротуризму, пищевой и перерабатывающей промышленности, на создание и модернизацию по переработке сельскохозяйственной продукции и пр.

Туристический бизнес в Республике Крым получил более 1,6 млрд. рублей на поддержание отрасли и сохранение кадрового обеспечения.

Министерство финансов в рамках проведения административных реформ связанных с цифровизацией финансовой системы, активно реализует образовательный контент по финансовой грамотности среди физических и юридических лиц.

Министерство экономического развития Республики Крым предоставляют субсидии для субъектов малого и среднего предпринимательства на возмещение процентной ставки по кредитам, оформленных в российских банках.

Микрофинансовая организация «Фонд микрофинансирования предпринимательства Крыма», предоставляет микрозаймы индивидуальным предпринимателям и юридическим лицам.

Отметим, что инфраструктура государственной поддержки в Республике Крым представлена достаточным множеством организаций, ведомственных и подведомственных структур, являющихся отраслевыми. Данное многообразие и дублирование некоторых функций

в части обеспечения консультационной помощи, образовательного контента, информационного обеспечения предоставления государственной поддержки обуславливает необходимость создания единой электронной платформы. Данная платформа будет представлять собой некий сводческий онлайн-центр, куда предприниматель любой отрасли экономики сможет отправить заявку на получение консультации о форме государственной поддержки, сроках подачи документов, алгоритма предоставления пакета документов, правильности заполнения документов и пр. Определив запрос пользователя, платформа сформирует тот набор необходимой информации, которая необходима клиенту, тем самым обеспечив компетентность и адресность, освободив его от ненужных поисков, траты времени и пр.

Данную онлайн-платформу можно проработать в рамках реализации Федерального проекта «Цифровое государственное управление», который нацелен на реализацию национальной цели «Цифровая трансформация», что определено Указом Президента Российской Федерации от 21 июля 2021 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

Ключевой целевой показатель, характеризующий достижение национальной цели – увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95% к 2030 году.

Федеральный проект включает мероприятия цифровой трансформации системы государственного управления, которые обеспечивают новый уровень предоставления услуг, необходимых для повышения качества жизни граждан и развития бизнеса.

Федеральным проектом предусмотрены мероприятия по трем основным направлениям, нас в данном случае будет интересовать такие направления как:

- цифровизация процессов предоставления государственных услуг и исполнения государственных функций государственными органами власти, так как министерства и ведомства Республики Крым предоставляют государственную поддержку;
- повышение скорости обслуживания граждан и создание комфортных условий для бизнеса, а также цифровая трансформация услуг и взаимоотношений в обществе;
-создание возможностей для перехода на цифровое взаимодействие граждан, бизнеса и государства.

Функционирование онлайн-платформы поможет систематизировать необходимую информацию о государственной поддержке предпринимателей Республики Крым, будет выступать в роли информационного и консультационного центра, разводящего свод общих вопросов на частности и конкретику, при этом обеспечиваю адресность обращений и предоставлений действенной помощи.

УДК 004.738

Троян Ирина Анатольевна
доцент кафедры экономической теории, к.э.н., доцент
Щеглова Анастасия Евгеньевна
студентка направления подготовки 38.03.01 Экономика
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И.Вернадского»
Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОТРЕБИТЕЛЯ

В сегодняшнем все более оцифрованном мире объем данных, к которым осуществляется доступ и которые совместно используются в сложных сетях, продолжает неуклонно возрастать. Информационная безопасность становится все более актуальным вопросом, поскольку потребители все чаще совершают покупки в Интернете и все больше беспокоятся о том, что это означает для их личных данных.

В связи с быстрым распространением устройств, подключенных к Интернету, как потребительских, так и промышленных, ландшафт киберугроз растет быстрее, чем люди могут успевать следить за ними. Умение потребителей замечать угрозы, а тем более защищаться от них, отстает. Поскольку потребители безразличны к защите своих точек взаимодействия в Интернете, возникают риски при осуществлении коммерческих операций в сети. Интернет называют информационной супермагистралью. Но когда мошенники, хакеры и другие злоумышленники пытаются украсть личную информацию потребителя в Интернете, полезно знать, как заблокировать устройства, сеть и защитить информацию.

Потребители все больше обеспокоены тем, что организации имеют доступ к их личной информации или хранят ее. В связи с ростом риска киберпреступности компаниям необходимо сосредоточить свое внимание на обеспечении защиты потребительских данных и формировании

доверия своих клиентов – как потребителей, так и предприятий [1]. Организации теперь должны быть прозрачными не только в том, как они используют личную информацию потребителей, но и в том, как они сообщают о потенциальных преимуществах и рисках обмена своими данными. Доверие потребителей к организации имеет решающее значение для ее репутации, финансов и возможностей для роста. Если потребитель не доверяет предприятию в управлении своими данными, безопасности и конфиденциальности своих личных данных, честности и прозрачности в отношении ценностей компании и кибербезопасности, существует больший риск потери бизнеса и репутации.

Угрозы безопасности или конфиденциальности все чаще связаны не с кибератаками на ведущих поставщиков онлайн-услуг, а с использованием уязвимостей в широко используемых потребительских продуктах. Основные направления, которые потребитель самостоятельно может реализовать, связаны с защитой персональных устройств и домашних сетей. Так, важно регулярно обновлять свое программное обеспечение безопасности, интернет-браузер и операционную систему. Это помогает убедиться, что существует критические исправления и средства защиты от угроз безопасности.

Необходимо использовать меры для защиты своих учетных записей, особенно тех, которые содержат личную информацию: банковские учетные аккаунты, электронная почта и учетные записи в социальных сетях. Для этого необходимо создавай и использовать надежные пароли.Это означает не менее 12 символов. Как правило, сделать пароль длиннее — это самый простой способ повысить его надежность.

Рекомендуется также использовать многофакторную аутентификацию. Некоторые учетные записи обеспечивают дополнительную безопасность, требуя два или более учетных данных для входа в учетную запись потребителя. Это называется многофакторной аутентификацией. Кроме того, следует выбирать контрольные вопросы, ответы на которые знает только потребитель. Многие контрольные вопросы требуют ответов на информацию, доступную в общедоступных записях или в Интернете. Поэтому по возможности важно избегать таких вопросов, как почтовый индекс, девичья фамилия матери и место рождения.

Также одним из направлений обеспечения информационной безопасности является создание резервной копии данных. Резервное копирование данных означает создание дополнительной копии всех файлов: либо через сохранение в облаке, либо на внешнем запоминающем устройстве (например, флэш-накопитель USB, самый доступный вариант, предлагающий умеренный объем памяти).

Важно понимать, что программы однорангового обмена файлами, которые популярны среди потребителей, например для доступа к бесплатной музыке и видео, сопряжены со значительными киберриском. Такие программы могут без ведома потребителя поделиться важными файлами и папками, также есть риски неосознанно загрузить вредоносное ПО, пиратские материалы или материалы, защищенные авторским правом.

Одним из важных способов защиты потребительской информации является защита домашней сети. Важно с помощью обеспечить защиту программ маршрутизаторов, отслеживающих точки соединения между устройствами потребителя и Интернетом. Если вредоносное ПО попадет на любое из подключенных устройств, оно может распространиться на другие устройства, подключенные к домашней сети. Однако, если потребитель может сам контролировать, насколько защищена его домашняя сеть, то в случае с общедоступными сетями Wi-Fi, риски киберпреступности возрастают. Следует осуществлять и сохранять онлайн-покупки, банковские операции и другие личные транзакции только в домашней сети или через мобильные данные, так как эти данные обычно зашифрованы.

На сегодняшний день крайне важна роль национальных органов по вопросам конкуренции и защиты прав потребителей в создании последовательной модели кибербезопасности. В наш век цифровых преобразований крайне важно, чтобы мир кибербезопасности быстро развивался, чтобы противостоять росту киберугроз и кибератак, чтобы поддерживать доверие потребителей. В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы информационное общество определено как общество, в котором информация и уровень её доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан [2]. На уровне государственной кибербезопасности особенно важно определить минимальные меры безопасности и согласовать общие процедуры (планы) реагирования на наиболее серьезные инциденты. С другой стороны, с точки зрения индивидуальных предпринимателей не менее важно обеспечить защиту обрабатываемой ими информации, например, коммерческую тайну и данные о клиентах, особенно от угрозы несанкционированного доступа или раскрытия. В этой связи организациям нужна правильная система безопасности. Однако и сами потребители должны иметь возможности для эффективной собственной защиты, которые часто не только не имеют достаточных знаний в области ИТ-безопасности, но и в значительной степени зависят от механизмов безопасности,

предоставляемых им поставщиками продуктов и услуг, которые они используют. Таким образом, информационная безопасность потребителя в современных условиях цифровизации и повседневного использования сети Интернет для совершения потребительских операций, носит многоуровневой системный характер.

Литература

1. Петренко, А. А. Управление киберрисками 5G / А. А. Петренко, С. А. Петренко, А. Д. Костюков // Защита информации. Инсайд. – 2020. – № 5(95). – С. 8-15. – EDN YUTDAS.
2. Указ Президента Российской Федерации от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»

УДК 33.01

Цхададзе Нелли Викторовна
д.э.н., профессор
Подлужная Ирина Дмитриевна
ФГОБУ ВО «Финансовый университет при Правительстве РФ»
г. Москва, Россия

БЕДНОСТЬ НАСЕЛЕНИЯ КАК ИНДИКАТОР НАЦИОНАЛЬНОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Актуальность темы данной статьи заключается в том, что проблема бедности населения оказывает отрицательное влияние на систему национальной экономической безопасности, а государство, в свою очередь, рассматривает бедность как один из индикаторов экономической безопасности страны в целом.

В экономической и статистической литературе используются различные подходы для измерения бедности. Подавляющее большинство исследователей считает, что к бедным относятся те, чьи доходы ниже границы бедности. При этом граница бедности представляет собой объективно определенную величину дохода, рассчитанную исходя из национальных или субнациональных минимальных норм потребления материальных благ и услуг.

Такой подход к оценке бедности предполагает использование перечня товаров (с указанием их количества), которые составляют минимальную потребительскую корзину, а также источников информации о ценах на них.

Этот метод оценки бедности используется в Российской Федерации. В качестве границы бедности рассчитывается прожиточный минимум, представляющий собой уровень дохода, обеспечивающий приобретение научно обоснованного минимального набора материальных благ и услуг для поддержания жизнедеятельности человека. Прожиточный минимум в Российской Федерации регулируется Федеральным законом №134-ФЗ «О прожиточном минимуме в Российской Федерации» и Федеральным законом №227-ФЗ «О потребительской корзине в целом по Российской Федерации. Данные законы использует следующие понятия:

- минимальная потребительская корзина (минимальный набор продуктов питания, непродовольственных товаров и услуг, необходимых для сохранения здоровья человека и обеспечения его жизнедеятельности);
- прожиточный минимум (стоимостная оценка потребительской корзины плюс обязательные платежи и сборы);
- семья (лица связанные родством или свойством, совместно проживающие и ведущие совместное хозяйство);
- основные социально-демографические группы населения (трудоспособное население, пенсионеры, дети).

В соответствии с законом №134-ФЗ прожиточный минимум используется в качестве критерия оценки уровня жизни населения при разработке и реализации социальной политики, федеральных и региональных социальных программ; для обоснования устанавливаемых на федеральном уровне минимального размера оплаты труда, минимального размера пенсии по старости, размеров стипендий, пособий, других социальных выплат, включая оказание необходимой государственной помощи малоимущим гражданам; а также при формировании федерального бюджета и бюджетов субъектов Российской Федерации.

Итак, бедность – это экономическое положение части населения и семей, стоящих на относительно низком уровне обеспеченности денежными, имущественными и другими ресурсами, а следовательно, и на низком уровне удовлетворения своих материальных и духовных потребностей. Количество бедного населения и уровень его жизни зависят от стадии развития общественного производства и определяются комплексом общественно-политических и социально-экономических условий: более высокая стадия общественного производства

обеспечивает потенциальные возможности более высокого порога бедности. Границы бедности могут быть оценены на основе фактической и нормативной обеспеченности населения ресурсами для личного потребления и соответственно уровней удовлетворения материальных и духовных потребностей людей.

Уровень бедности – размер дохода, обеспечивающий прожиточный минимум. Обычно рассчитывается либо в виде соотношения со средним доходом в стране, либо методом прямого расчета [1].

Бедность имеет множество причин в своих истоках, начиная от количество пресной воды, пригодной к употреблению, и количества земли, опять же, пригодной для сельскохозяйственной деятельности, до направления политики, проводимой местным правительством, и наличия вооруженных конфликтов. Но это не единственные возможные причины.

В теоретическом аспекте все причина наличия бедности можно разделить на группы:

1. Экономические (безработица, низкая з/п, низкая производительность труда, неконкурентоспособность отрасли);
2. Политические (военные конфликты, вынужденная миграция);
3. Образовательно-квалификационные (низкий уровень образования, недостаточная профессиональная подготовка);
4. Религиозно-философские;
5. Психологические;
6. Демографические (неполные семьи, большое количество иждивенцев в семье);
7. Социально-демографические (инвалидность, старость, высокий уровень заболеваемости);
8. Религиозно-географические (неравномерное развитие регионов).

Кроме того, стихийные бедствия, такие как пандемия COVID или землетрясения 2020 года в Пуэрто-Рико, могут еще больше истощить и без того скудные ресурсы бедного региона.

Общий показать бедности определяется формулой, предложенной Джеймсом Фостером, Джоэлом Гриером и Эриком Торбеке:

$$P_a=\frac{1}{H}\sum_{h=1}^{q}\left(\frac{Zh-Yh}{Zh}\right)^a$$

P – общий показатель бедности.

a – параметр, показывающий о каком именно показатели бедности идет речь.

Z_h – черта бедности отдельного домохозяйства h, которая зависит от его состава.

Y_h – уровень дохода отдельного домохозяйства h

q – количество бедных домохозяйств

H – общее количество домохозяйств.

На основании данной формулы определяются основные показатели бедности:

1)коэффициент бедности и уровень бедности (a=0);

2)индекс глубины бедности (a=1);

3)индекс остроты бедности (a=2);

Коэффициент бедности (доля бедных домохозяйств в общем количестве домохозяйств) характеризует степень распространенности бедности, но не позволяет оценить, насколько доходы бедных домохозяйств ниже границы бедности.

$$P_0=\frac{1}{H}\sum_{h=1}^{q}\left(\frac{Zh-Yh}{Zh}\right)^0$$

Индекс глубины бедности позволяет оценить насколько ниже относительно черты бедности расположены доходы бедных домохозяйств.

$$P_1=\frac{1}{H}\sum_{h=1}^{q}\left(\frac{Zh-Yh}{Zh}\right)^1$$

Индекс остроты бедности в отличие от индекса глубины бедности при расчете бедности придается больший удельный вес домохозяйствам с более значительным дефицитом доходов, расходов или потребления.

$$P_2=\frac{1}{H}\sum_{h=1}^{q}\left(\frac{Zh-Yh}{Zh}\right)^2$$

Давайте посмотрим на общую официальную статистику бедности в России. Данная статистика производится ежегодно и ежегодно, в основном, можно наблюдать повышение коэффициента бедности.

Таблица 1 – Уровень бедности в России с 1992 по 2021 г.

Год	Уровень бедности, %	Год	Уровень бедности, %
1992	33,5%	2007	13,3%
1993	31,3%	2008	13,4%
1994	22,4%	2009	13,0%
1995	24,8%	2010	12,5%
1996	22,1%	2011	12,7%
1997	20,8%	2012	10,7%
1998	23,4%	2013	10,8%
1999	28,4%	2014	11,3%
2000	29,0%	2015	13,4%
2001	27,5%	2016	13,2%
2002	24,6%	2017	12,9%
2003	20,3%	2018	12,6%
2004	17,6%	2019	12,3%
2005	17,8%	2020	12,1%
2006	15,2%	2021	11,0%

Источник: [https://rosstat.gov.ru/].

Как можно заметить по таблице, по данным 2021 года, предоставленным Росстатом, количество россиян, доходы которых ниже величины прожиточного минимума, составляет более 16 100 000 человек, или 11 % населения РФ.

Далее представлена информация более наглядно, в виде графика.

Рисунок 1 – Инфографика уровня бедности в России по годам
Источник: [https://rosstat.gov.ru/].

Так же стоит упомянуть о величине границы бедности, о которой было достаточно сказано до этого.

Таблица 2 – Границы бедности в целом по РФ, рублей в месяц

	Все население	В том числе			ИПЦ к IV кварталу 2020 г., %
		трудоспособное население	пенсионеры	дети	
2020 год					
Базовая граница бедности IV квартал	11329	12273	9348	11140	100
2021 год					
I квартал	11581	12545	9556	11387	102,22
II квартал	11813	12797	9747	11616	104,27
I полугодие	11697	12672	9652	11502	103,25
III квартал	11970	12968	9877	11771	105,66
Январь-сентябрь	11788	12770	9727	11591	104,05
IV квартал	12269	13292	10124	12065	108,30
Год	11908	12900	9826	11709	105,11

Источник: [https://www.fedstat.ru/].

Чтобы перед нами предстала полная картина уровня бедности, стоит рассмотреть уровень бедности не только России, но и в остальном мире.

Руководствуясь некоторыми критериями, разработанными Всемирным Банком, к категории бедных стран можно отнести тех, у кого уровень ВВП на душу населения ниже 1025$ в год. В самых богатых странах мира этот показатель превышает 12475$.

Итак, континентом с самым высоким уровнем бедности является Африка, беднейшие страны на планете - Демократическая Республика Конго (уровень крайней бедности - 77,1%) и Мадагаскар (77,6%). В качестве характеристики данных стран можно привести некоторые термины: преобладание авторитарного режима, наличие военных конфликтов, слаборазвитая экономика в целом, коррупция, преступность, плохое состояние экологии и другие.

Стоит привести сам список стран с самым высоким уровнем бедности в мире. Так по данным Всемирного банка, страны с самым высоким уровнем бедности в мире являются:

1. Южный Судан (80,2%);
2. Экваториальная Гвинея (76,80%);
3. Мадагаскар (70,70%);
4. Гвинея-Бисау (69,30%);
5. Эритрея (69,0%);
6. Сан-Томе и Принсипи (66,70%);
7. Бурунди (64,90%);
8. Демократическая Республика Конго (63,90%);
9. Центральноафриканская Республика (62,0%);
10. Гватемала (59,30%).

Так же стоит упомянуть об уровне бедности в странах ОСЭР за 2021 год для примера. Из всех стран ОЭСР в Коста-Рике по состоянию на 2021 год был самый высокий уровень бедности - более 20%. Страной со вторым по величине уровнем бедности стала Венгрия - 17,6 %. На другом конце шкалы самый низкий уровень бедности в Чехии - 5,6 %, за ней следуют Финляндия и Дания.

Таблица 3 – Уровень бедности в странах ОСЭР за 2021 год, %

Страна	Уровень бедности за 2021 год	Страна	Уровень бедности за 2021 год
Коста-Рика	20,3%	Германия	10,9%
Болгария	17,6%	Португалия	10,6%
Израиль	17,3%	Люксембург	10,5%
Румыния	17,0%	Австрия	10,0%
Латвия	16,9%	Швейцария	9,9%
Мексика	16,6%	Польша	9,8%
Япония	15,7%	Венгрия	9,2%
Литва	15,4%	Швеция	8,8%
Юж.Корея	15,3%	Канада	8,6%
США	15,1%	Норвегия	8,4%
Турция	15,0%	Франция	8,4%
Эстония	14,9%	Нидерланды	8,3%
Испания	14,7%	Бельгия	8,1%
Италия	14,2%	Словакия	7,8%
Австралия	12,6%	Ирландия	7,4%
Новая Зеландия	12,4%	Дания	6,5%
Греция	11,5%	Финляндия	5,7%
Великобритания	11,2%	Чехия	5,6%

Источник: [https://www.vsemirnyjbank.org/ru/].

В результате сравнения уровня бедности в России с другими странами Россия относиться к странам, в которых бедность является достаточно серьезной проблемой. Как можно отметить из выше приведенной таблицы уровень бедности на 2021 год в России (11%) меньше, чем у США (15,1%) и Великобритании (11,2%), но это не отменяет того, что даже 11% являются проблемой.

Как было сказано выше, уровень бедности – одна из самых важных социальных проблем России. Данной проблеме уделяется много внимания, она освещается в СМИ, ее рассматривают политики и ученые. Но несмотря на это ситуация улучшается крайне медленно. Это имеет ряд своих причин. Так вопреки положительной тенденции в решении представленной проблемы, в целом происходит ухудшение по всей стране, что является следствие таких факторов как: низкий уровень заработной платы, связь финансовой бедности с социальной, низкая величина МРОТ и других социальных гарантий. Это приводит к увеличению уровня бедности (по данным Росстата уровень бедности в России вырос с 11% в 2021 году до 14,5% в 2022 году).

Стоит заменить, что высокий уровень бедности является угрозой экономической безопасности страны, требующей безотлагательного решения. Для решения этой угрозы правительство страны проводит ряд социальных мероприятий на законодательном уровне.

В качестве наиболее наглядной демонстрации стоит упомянуть такие мероприятия, как:

1. Повышение уровня заработной платы;
2. Содействие в трудоустройстве;
3. Социальная поддержка семей и несовершеннолетних детей;
4. Увеличение размера МРОТ;
5. Активизация промышленности;
6. Развитие малого и среднего бизнеса (предоставление льгот и субсидий) и т. д.

Делая краткий вывод из перечисленных мероприятий можно сказать, что для того чтобы справиться с бедностью в России, необходимо активизировать промышленность, обеспечить стабильность экономики в стране и в мире, а также обеспечить повышение общего уровня заработной платы. Уровень бедности снизиться, если значение жизни станет выше, а этого можно добиться, разработав и внедрив определенные социальные программы. Но в то же время нельзя гарантировать, что реализация все перечисленного даст желаемый результат. Это будет являться лишь первой ступенью благодаря которой станет возможно определить какой шаг должен быть сделан дальше, для улучшения и закрепления ситуации.

Подводя итоги, нужно признать, проведение анализа бедности в России и в мире должно осуществляться при помощи комплекса связанных между собой факторов. И как следствие, борьба с бедностью – это задача, что не имеет универсального решения, но при последовательном осуществлении комплекса мер, разработанных посредством анализа текущего состояния и динамики положения в обществе, на основе которых разрабатываются именно такие пути решения, которые будут эффективны в реалиях данного государства.

Литература

1. Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б..Современный экономический словарь. — 2-е изд., испр. М.: ИНФРА-М. 479 с..1999.
2. Цхададзе, Н.В. Анализ социально-экономической дифференциации и уровня благосостояния населения России / Н.В. Цхададзе, К.В. Хаустова // Инновации и инвестиции. – 2019. – № 1. – С. 269-273.
3. Цхададзе Н.В. Социально-экономическое неравенство населения России / Н.В. Цхададзе // Вестник Московского университета МВД России. – 2020. – № 6. – С. 300-306.
4. Цхададзе, Н.В. Эффективность и безопасность рыночной формы хозяйствования // Рыночное хозяйство в условиях риска и неопределенности. Монография. Под редакцией В.А. Сидорова, Я.С. Ядгарова, Е.Л. Кузнецовой, В.В. Чапли. – Лондон, 2020. – С. 384-434.
5. Tskhadadze, N.V. Socio-economic differentiation of the population of Russia in the conditions of scientific and technical progress / K. V. Khaustova, N. V. Tskhadadze, M. A. Ekaterinovskaya // Инновации и Инвестиции. – 2020. – № 5. – С. 58-61.
6. Человеческий капитал в модели устойчивого экономического роста России: Монография. Под научной редакцией О.В.Карамовой, Г.А.Терской, Н.В.Цхададзе. – М.: Прометей, 2023.- 514 с.
7. Официальный сайт ЕМИИС Государственная статистика. - URL: https://www.fedstat.ru/indicator/59577# [Электронный ресурс] (дата обращения: 16.11.2022)
8. Официальный сайт Федеральной службы государственной статистики. - URL: https://rosstat.gov.ru/ [Электронный ресурс] (дата обращения: 16.11.2022)
9. http://global-finances.ru/uroven-bednosti-v-rossii-po-godam/ [Электронный ресурс] (дата обращения: 26.11.2022)
10. Официальный сайт Всемирного Банка. - URL: https://www.vsemirnyjbank.org/ru/home [Электронный ресурс] (дата обращения: 23.01.2023)

УДК 33.01

Цхададзе Нелли Викторовна
д.э.н., профессор
Тюрина Ирина Андреевна
Галиева Камилла Тимеряновна
студенты
ФГОБУ ВО «Финансовый университет при Правительстве РФ»
г. Москва, Россия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В РОССИИ

На сегодняшний день в России наблюдаются проблемы, связанные с защитой внутренних данных как небольших фирм, так и огромных корпораций. Нам бы хотелось обсудить текущее состояние отрасли, сделать выводы и отследить векторы развития информационной безопасности в России.

Подавляющее большинство различных компаний не может противостоять хакерам и в 96% случаях позволяет проникнуть во внутреннюю сеть; в 90% случаях при атаке хакеры получают доступ к информации, которая является коммерческой тайной. Такая тенденция обусловлена скорее всего тем, что много средств компании тратят именно на сетевую безопасность и другие средства защиты, то есть без доработки под их конкретный бизнес. Даже большие корпорации чаще всего просто покупают «пакеты», обеспечивающие безопасность системы, но не тратят средства на специалистов, которые могли бы эффективно взаимодействовать с средствами защиты и которые смогли бы оперативно реагировать на угрозы.

В таблице ниже представлена информация о крупнейших компаниях по обеспечению информационной безопасности в России.

№ 2021	№ 2020	Название компании	Выручка ИБ в 2021 г., тыс. ₽, с НДС	Выручка ИБ в 2020 г., тыс. ₽, с НДС	Рост выручки ИБ 2021/2020, в %
1	1	Лаборатория Касперского	55 820 960	50 638 566	10,2%
2	3	Softline	22 311 000	20 320 000	9,8%
3	2	Цитадель	18 973 588	20 478 792	-7,4%
4	6	Ростелеком-Солар	12 270 000	8 354 000	46,9%
5	5	Bi.Zone	10 447 886	8 971 000	16,5%
6	9	Инфосистемы Джет	8 838 000	6 970 000	26,8%
7	7	ИнфоТеКС	8 469 939	7 290 485	16,1%

Источник: CNews Security.

Опираясь на таблицу, представленную выше, мы видим наиболее крупные компании, которые обеспечивают информационную безопасность отдельных фирм и предприятий. Все они распространяют свое ПО, которое помогает компаниям обезопасить себя и свою конфиденциальную информацию. Как мы видим почти у всех из них возросла выручка, что свидетельствует о их востребованности на рынке. Но также большое влияние на обеспечение информационной безопасности оказывает государство.

Согласно законодательству, в России действуют органы информационной безопасности, каждый из которых несет ответственность в определенных сферах отрасли и обладает соответствующими полномочиями. Органы информационной безопасности призваны организовывать и вести деятельность в направлении защиты информации. Профессиональная работа по кибербезопасности в России ведется следующими государственными органами: Министерство обороны, МВД, Роскомнадзор, Центробанк РФ, Совет Безопасности РФ, ФСТЭК, ФСО, СВР, Комитет Госдумы по безопасности.

В рамках каждой частной, коммерческой организации также должны действовать службы, занимающиеся организацией информационной безопасности на уровне одной компании: службы экономической безопасности, HR-отдел, режимный отдел, служба информационной безопасности.

В области технической защиты информационных данных основными органами информационной безопасности в России являются ФСТЭК и ФСБ. ФСБ ведет полноценную работу по технической защите информации, выполняя многочисленные функции. Во-первых определение процедур осуществления в границах имеющихся полномочий контроля над организацией и работой инженерно-технической, крипто безопасности информационных систем, телекоммуникационных систем, систем зашифрованной, секретной и другой спецсвязи; осуществление и организация, согласно действующим законам, сертификации средств защиты данных, телекоммуникационных комплексов и систем, технических средств, которые необходимы для обнаружения электронной аппаратуры, используемой для незаконного получения информации. Также занимается контролем над соблюдением режима секретности при эксплуатации зашифрованных данных в специализированных департаментах госорганов и коммерческих организациях в РФ; обеспечением информационной защиты объектов критически важной инфраструктуры, расположенных в ней технических средств от утечки данных по техническим каналам и осуществлением и организацией получения лицензий заинтересованными лицами на отдельные виды деятельности.

Исходя из вышесказанного, мы видим, что информационная безопасность тесно связывает несколько субъектов рынка и частных лиц. Обеспечение защиты данных является неотъемлемой частью системы, которая влияет на успех реализации компании на рынке. В будущем, мы считаем, государство и компании, обеспечивающие информационную безопасность должны

взаимодействовать друг с другом, и это поможет сократить риски возникновения угроз и повысить осведомленность экономических участников процесса.

Грамотный подход к обеспечению информационной безопасности оказывает сильное влияние, в том числе и на экономику страны. Экономическая нестабильность напрямую влияет на уровень экономической безопасности и защищенности граждан.

Экономические ограничения негативно повлияли на состояние ряда отраслей российской экономики. Санкции, например, в банковской сфере, а именно ограничения в возможности получения кредитных ресурсов, вызвали снижение инвестиционной активности, спровоцировали инвестиционный спад в стране и ослабление курса рубля.

Одной из главных угроз для экономической безопасности российского общества является также проблема сырьевой направленности экономики. Для минимизации последствий указанной угрозы в настоящее время проводится политика импортозамещения, которая может вести за собой ряд как позитивных, так и негативных последствий. Правительству необходимо реализовывать политику развития в области научно-технического прогресса, начинать сотрудничество с иностранными компаниями по созданию высокотехнологичной продукции и принимать меры по изменению ориентации.

Проблема занятости в условиях экономической нестабильности также во многом определяет экономическую безопасность страны. Качество и количество человеческого капитала являются основными факторами развития отечественной экономики в условиях глобальных изменений. Наличие проблем по занятости в стране в первую очередь отражается на населении, которое зачастую выражает свое недовольство в различных акциях протеста, массовых митингах, а также совершенных преступлениях. Увеличение имущественной дифференциации населения и повышение уровня бедности ведет к нарушению социального мира и общественного согласия. То есть негативное влияние любых внешних факторов на человека подрывает стабильное состояние его жизни, ее качество, что толкает на совершение экономических преступлений

Россия сегодня имеет недостаточно высокий уровень экономической безопасности. Определено, что в России существует множество угроз, негативно влияющих на российскую экономику. Разработки экономического и политического курса страны с учетом важности обеспечения надежности экономической системы и ее устойчивости к существующим угрозам экономической безопасности объективно необходимы для нашей страны. В настоящее время ряд специалистов указывают на положительную динамику в сфере обеспечения экономической безопасности, однако некоторые аспекты все же вызывают обеспокоенность. В частности, необходимо согласиться с тем, что и по сей день, экономика нашей страны зависит от сырьевого экспорта и уровень зависимости от высоко технологичных продуктов остается также высоким.

Литература

1. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: Высшая школа, 2021. - 536 с.
2. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2022. - 368 с.
3. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: ИНФРА-М, 2022. - 368 с.
4. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2022. - 304 с.
5. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - М.: Академический проект, 2023. - 544 с.

УДК 004.056

Ирих Эльмира Мамутовна
Кысса Андрей Андреевич
обучающиеся 1 курса направления
подготовки 38.03.01 Экономика
Институт экономики и управления
Научный руководитель:
Усенко Роман Станиславович
старший преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМЕ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Подобные атаки ориентированы на получение доступа к секретной информации, ее изменение и уничтожение, на вымогательство у пользователей денежных средств либо на нарушение нормальной работы фирм [1].

В России, в сфере кибербезопасности можно наблюдать следующие устойчивые угрозы:

• низкая правовая компетентность населения и участников бизнеса по вопросам кибербезопасности;

• в связи с санкциями, к сожалению, на данный момент большинство вендеров технологий, связанных с кибербезопасностью, покинули рынок России;

• так же по итогу 2022 года можно выделить угрозу со стороны хактивизма, который проявляется в форме негативного выражения позиции (по социальным вопросам), используя кибератаки;

• технологические перебои и непреднамеренные ошибки персонала, ведущие к неблагоприятному влиянию на элементы ИК-инфраструктуры.

По оценкам специалистов отечественной DevSecOps компании Swordfish Security, из-за слабого уровня защищенности российского бизнеса и госструктур, в 2023 году количество успешных кибератак может увеличиться на 30-40 %. На рисунке 1 представлен график изменения количества совершенных киберпреступлений за период с 2018 по 2022 год.

Рисунок 1 – Динамика киберпреступлений за 2018-2022 гг. [2]

Начальными мерами по развитию кибербезопасности должны соответственно стать:

• постоянно организованный на международном уровне обмен информацией между госорганами, социальными организациями и бизнес-сообществом о киберинцидентах и новых технологиях защиты.

• регулярное освещение в СМИ успехов в борьбе с киберпреступниками;

• постоянное совершенствование возможностей в сфере кибербезопасности.

Законодательный уровень представляется основополагающим для обеспечения информационной безопасности. На законодательном уровне имеется две группы мер:

• меры ограниченной направленности – меры, обращенные на создание и поддержание в обществе неблагоприятного (в том числе с применением наказаний) взаимоотношения к нарушениям и нарушителям информационной безопасности;

• меры созидательной направленности – устремляющие и координирующие средства, содействующие развитию сообщества в области информационной безопасности, способствующие в разработке и распространении средств предоставления информационной безопасности.

Эксперты ITU расценивают компьютерную безопасность всех государств мира по пяти параметрам: юридическая, техническая, организационная подготовленность, стремление к сотрудничеству, формирование образовательного и экспериментального потенциала стран. На

рисунке 2 представлена группа стран, структурированная по возрастанию индекса кибербезопасности.

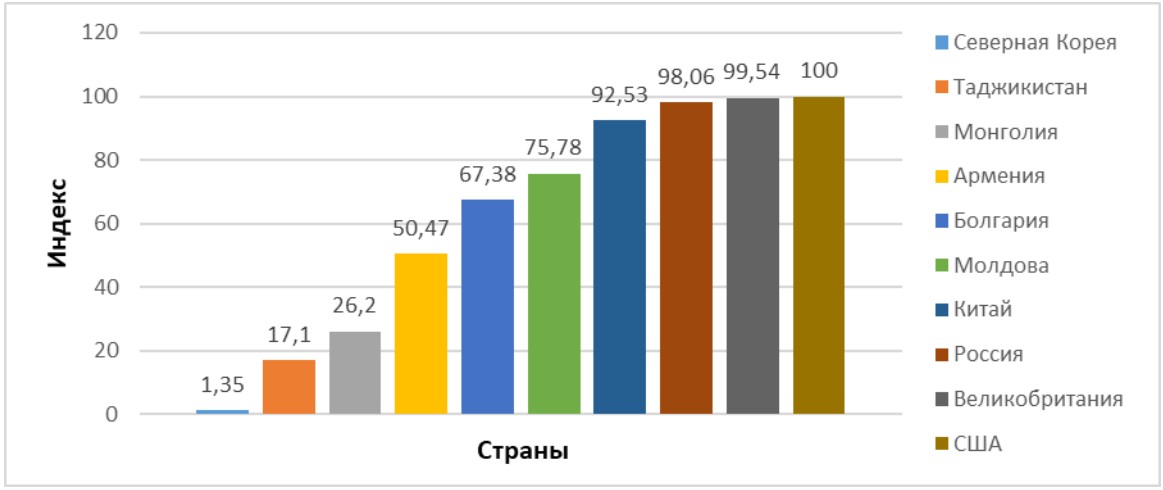

Рисунок 2 – Рейтинг стран по уровню кибербезопасности за 2021 [2]

Киберпреступность становится всё масштабнее и разнообразнее. Жертвами злоумышленников, которые орудуют в виртуальном пространстве, сегодня могут стать не только обычные люди, но и целые страны [3]. Поэтому кибербезопасности необходимо уделять достаточно большое внимание.

Литература

1. Смирнова, Е. А. Введение в цифровую культуру : учебное пособие / Е. А. Смирнова, М. А. Смирнов. — Череповец : ЧГУ, 2021. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180959 (дата обращения: 16.01.2023). — Режим доступа: для авториз. пользователей. — С. 173.
2. Рейтинг стран по уровню кибербезопасности [Электронный ресурс] – Режим доступа: https://nonews.co/directory/countries/cybrsecurity-index (дата обращения: 16.01.2023).
3. Плотникова, П. В. Киберпреступность как угроза обществу / П. В. Плотникова, Р. С. Усенко // Проблемы информационной безопасности : Труды VI Всероссийской с международным участием научно-практической конференции, Симферополь-Гурзуф, 13–15 февраля 2020 года. – Симферополь-Гурзуф: ИП Зуева Т.В., 2020. – С. 105-107.

УДК 339.16

Круликовский Анатолий Петрович
доцент
Волосовец Даниил Владимирович
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СОВРЕМЕННАЯ МОДЕЛЬ ЭЛЕКТРОННОЙ КОММЕРЦИИ – NEXT COMMERCE

Электронная коммерция была на подъеме еще до того, как появился COVID. Но пандемия вызвала значительное ускорение роста электронной коммерции. Фактически, во время пандемии, всего за три месяца электронная коммерция пережила 10-летний рост.

В 2021 году объем мировых продаж электронной коммерции составил 5,2 трлн долларов, и ожидается, что в течение следующих четырех лет эта цифра вырастет на 56% и достигнет 8,1 трлн долларов к 2026 году (см. рис. 1). Прогнозируется, что к 2023 году на электронную коммерцию будет приходиться более 22% от всей розничной торговли.

Продажи электронной коммерции удвоились за последние пять лет [2] и ожидается, что рынки снова почти удвоятся к 2026.Многие компании делают значительные инвестиции в развитие возможностей электронной коммерции.

Вступление в следующий этап роста требует выхода за рамки традиционной электронной коммерции и онлайн-продаж. Это вызвало необходимость в создании персонализированного, адаптированного взаимодействия с клиентами по всем возможным каналам - и все это при поддержке сквозных цифровых технологий и операционной модели, которая ставит электронную коммерцию, основанную на цифровых технологиях, в центр бизнеса. В отчете

McKinsey & Company [3] такая модель электронной коммерции получила название NeXT Commerce.

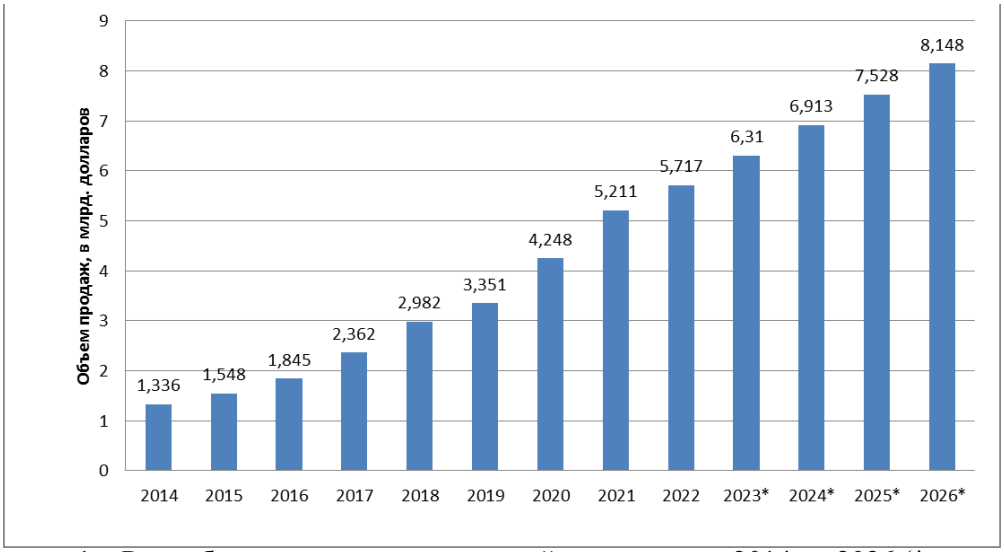

Рисунок 1 – Рост объемов продаж электронной коммерции с 2014 по 2026 (* - прогноз)
Источник: [1].

NeXT Commerce повышает скорость, точность и гибкость, необходимые для более быстрого достижения прибыльного и устойчивого роста, обеспечивая омниканальную, социальную, живую метавселенную NeXT Commerce.

Этот подход к электронной коммерции нуждается в существенном обновлении, основанном на стремлении стать незаменимым для клиента благодаря более глубокому уровню взаимодействия с клиентами в онлайн и офлайн. Реализация такого подхода требует, чтобы компании могли организовать взаимодействие, отвечающее постоянно растущим ожиданиям клиентов.

В исследовании [4] были выделены следующие глобальные факторы, которые оказывают огромное давление на устаревшие бизнес-модели электронной коммерции.

1. Ускорение роста электронной коммерции. Все признаки указывают на предстоящий сильный рост в секторах B2C и B2B, при этом электронная коммерция будет расти более чем на 12 процентов каждый год, по меньшей мере до 2026 года. В работе [5] показано, что в Соединенных Штатах и Европе насчитывается по меньшей мере 25 миллионов высокопотенциальных цифровых клиентов, которые начали использовать электронную коммерцию во время COVID, но не полностью приняли ее.
2. Быстро меняющееся поведение клиентов. Темпы внедрения цифровых технологий в течение COVID удвоились по всему земному шару [5], и ожидает, что эта тенденция сохранится.
3. Растущие ожидания клиентов. Каждая успешная цифровая инновация повышает планку ожиданий клиентов для всех остальных - Tik Ток для видео, Amazon для удобства, Alibaba для актуальности, и это лишь некоторые из них. Если компании не смогут оправдать растущие ожидания, клиенты уйдут. Около 74 процентов клиентов B2B хотят, чтобы доступность продукта отображалась онлайн, в то время как 72 процента хотят иметь возможность совершать покупки через любой канал, который они могут использовать [6].
4. Нынешний подход к электронной коммерции является неустойчивым для многих компаний, особенно в сфере потребительского бизнеса. Примерно у трех четвертей розничных продавцов наблюдался отрицательный рост рентабельности, даже несмотря на то, что электронная коммерция стала составлять большую долю выручки [7].
5. NeXT Commerce компании эволюционировали, для того что бы значительно увеличить масштаб работы и скорость выполнения операций. 5G сделал потребление данных дешевле и лучше для потребителей, а облачные технологии предоставили компаниям огромную вычислительную мощность, что способствует снижению затрат. Развитие мобильной сети 5G может радикально изменить бизнес-операции. Ожидается, что рынок 5G будет расти в среднем на 65,8% до 2030 года и достигнет оценки в 797,8 млрд. долларов. Эта технология имеет решающее значение для предприятий, которые стремятся предлагать новые услуги и отслеживать информацию, чтобы оставаться впереди конкурентов. Например, развитие мобильной сети 5G способствует улучшению сбора и анализа данных для предприятий.

Сеть 5G также имеет решающее значение для поставщиков медицинских услуг, которые инвестировали в телемедицину. Высокая скорость сети 5G позволяет осуществлять видео- и дистанционное наблюдение за пациентами практически в режиме реального времени.

6. Конкурентное давление. B2B и Компании B2C сталкиваются с сокрушительными конкурентными силами с двух сторон. С одной стороны, крупные компании, ориентированные на цифровые технологии, используют свои преимущества для выхода на новые рынки, потенциально угрожая каждому устоявшемуся сектору. С другой стороны, все больше стартапов запускают инновационные бизнес-модели, которые могут быстро масштабироваться. Финансирование стартапов в сфере электронной коммерции достигло рекордных 54 миллиардов долларов в 2021 году по сравнению с 19 миллиардами долларов в 2020 году.

NeXT commerce требует огромных координированных изменений в структуре обслуживания клиентов.

Бренды NeXT commerce придерживаются стратегии, при которой ни один канал обслуживания клиентов не предпочтительнее другого, где бы они ни находились, онлайн и вне сети. Они создали полностью интегрированные системы управления клиентами, запасами и заказами, которые управляют потоками данных по каналам и местам хранения на основе предпочтений клиентов, а не на основе того, как настроены системы.

В Китае проблемы с доверием означают, что потребители, как правило, посещают восемь точек соприкосновения, прежде чем принять решение [5], это потребовало особого внимания согласованности во всех каналах работы с клиентами.

Компании всегда стремились к соседству, но NeXT commerce открывает более широкую сеть рыночных возможностей: технологические компании могут предлагать платежные услуги; розничные торговцы могут предлагать банковские услуги; торговые площадки могут предлагать средства массовой информации.

NeXT commerce извлекают значительную выгоду от использования технологий искусственного интеллекта для систематической оптимизации всего спектра операций: от ценообразования и ассортимента до производительности за счет объединения заказов, конфигурации доставки.

Успешные компании становятся незаменимыми для своих клиентов. Используя цифровые технологии для перехода от элементарных транзакций к предоставлению всевозможного обслуживания клиентов. За последние пять лет затраты на привлечение клиентов выросли в среднем на 60 процентов. Компаниям необходимо выработать радикально более глубокое и широкое понимание того, чего на самом деле хотят их клиенты и как это обеспечить. Данные преобразования невозможны без применения разнообразных информационных технологий, что требует разработки новых моделей обеспечения информационной безопасности.

Литература

1. Chevalier S. Retail e-commerce sales worldwide from 2014 to 2026 [Электронный ресурс] / S. Chevalier. — Режим доступа: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/#:~:text=In%202021%2C%20retail%20e-commerce,8.1%20trillion%20dollars%20by%202026 (дата обращения 08.10.2022).
2. Suzy Davidkhanian S. US e-commerce forecast 2022 [Электронный ресурс] / S. Davidkhanian Insider Intelligence, July 26, 2022. — Режим доступа: https://www.insiderintelligence.com/content/us-ecommerce-forecast-2022 (дата обращения 10.08.2022)/
3. NeXT Commerce [Электронный ресурс]. — Режим доступа: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/how-we-help-clients/next-commerce (дата обращения 20.08.2022).
4. Becoming indispensable: Moving past e-commerce to NeXT commerce [Электронный ресурс]. — Режим доступа: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/becoming-indispensable-moving-past-e-commerce-to-next-commerce (дата обращения 20.12.2022).
5. Hajro N. Digital resilience: Consumer survey finds ample scope for growth [Электронный ресурс] / N. Hajro, K. Smaje, B. Vieira, R. Zemmel.— Режим доступа: https://www.thembsgroup.co.uk/internal/digital-resilience-consumer-survey-finds-ample-scope-for-growth/ (дата обращения 05.11.2022).
6. B2B sales: Omnichannel everywhere, every time [Электронный ресурс]. — Режим доступа: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/b2b-sales-omnichannel-everywhere-every-time (дата обращения 25.02.2022).
7. Solving the paradox of growth and profitability in e-commerce [Электронный ресурс]. — Режим доступа: https://www.3csoftware.com/mckinsey-company-solving-the-paradox-of-growth-and-profitability-in-e-commerce/ (дата обращения 25.02.2022).

УДК 004.056.35/4

Бойченко Олег Валериевич
д.т.н., профессор
Овсепян Эдгар Артемович
обучающийся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

УПРАВЛЕНИЕ КИБЕРРИСКАМИ В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Актуальность исследования. В современном обществе практически все инфраструктуры, обеспечивающие жизнедеятельность, используют информационные технологии, которые, в свою очередь, играют решающую роль практически в любой инфраструктуре компании. Очевидно, что в этих условиях значение кибербезопасности современного общества (инфраструктур госуправления, финансовой, банковской, транспортной отраслей, а также энергетического, ресурсного, коммунального и продуктового обеспечения) чрезвычайно возрастает. На сегодняшний день кибербезопасность перестала быть проблемой, которая беспокоит лишь специалистов по IT и ИБ. Инциденты в сфере кибербезопасности сказываются на деятельности высшего руководства и на решениях, принимаемых топ-менеджерами. Потребителям услуг также хорошо известно об инцидентах и угрозах в сфере информационной безопасности, что вызывает у них серьезную озабоченность. На сегодняшний день управление киберрисками, угрожающими конфиденциальной информации и системам, является первоочередной задачей для большинства компаний.

Цель работы состоит в исследовании проблем, связанных с обеспечением эффективного управления киберрисками компании с целью создания эффективной производственной среды и благоприятного социально-экономического развития региона.

Методы исследования. Сообщения в СМИ о различных инцидентах в сфере ИБ стали таким же обычным делом, как прогноз погоды. За последний год практически все отрасли во всем мире пострадали от киберугроз того или иного рода. Так, в прессе было много сообщений о том, что автомобильные компьютерные системы, зачастую подключенные друг к другу и в ряде случаев обеспечивающие беспроводную связь с внешним миром, могут быть взломаны с целью захвата контроля над тормозной системой, рулевым управлением и даже двигателем [1].

Управление киберрисками – это скоординированное управление процессом сбора, обработки и анализа оперативной информации, а также технологическими и финансово-хозяйственными операциями с целью обеспечить эффективное управление информационными активами организации для предотвращения нежелательных последствий. Звучит, на первый взгляд, сложно. Но на самом деле это весь бизнес-процесс, посредством которого бизнес защищает свои жизненно важные активы и репутацию от внешних и внутренних угроз со стороны физических лиц или организаций. При этом процесс не ограничивается техническими мероприятиями. Любой компании необходимо рассматривать управление киберрисками в качестве неотъемлемой части управления своим собственным бизнесом и контроля рисков.

Конечная же цель управления киберрисками заключается в повышении устойчивости организации к рискам кибербезопасности до того уровня, когда ее системы и производственные процессы смогут обеспечивать возможность выявления киберугроз и реагирования на кибератаки, чтобы свести к минимуму перебои в производственной деятельности, а также свои финансовые потери.

При управлении киберрисками очень важно обеспечить сбалансированное использование трех ключевых компонентов (люди, процессы и технологии). В данном случае следует обратить внимание на концепцию кибербезопасности, разработанную NIST. Этот документ ориентирован на организации, занимающиеся эксплуатацией объектов жизненно важной инфраструктуры в США [2]. В нем представлена эффективная модель обеспечения безопасности на основе оценки рисков, которую могут взять на вооружение предприятия разной отраслевой направленности и географической принадлежности. Принятие такой концепции, помимо прочего, может принести дополнительные выгоды, среди которых можно отметить укрепление сотрудничества и повышение уровня информированности руководителей компаний и представителей отраслевых организаций о мерах по обеспечению безопасности. Согласно рекомендациям NIST, компаниям, в первую очередь, следует идентифицировать и классифицировать свои самые ценные информационные активы, а также определить, где в рамках экосистемы сосредоточены имеющие наибольшее значение данные, и кто имеет к ним доступ.

Результаты исследования. Таким образом, можно сделать вывод о том, что управление киберрисками подразумевает под собой разработку четко продуманной программы. Руководству компаний стоит задуматься над ее созданием в новом году. Программа эффективного управления киберрисками станет одним из многих компонентов контрольной среды компании,

являющейся неотъемлемой частью системы управления рисками. Хотя такая программа не устраняет киберриски, она позволяет управлять этими рисками с помощью процесса принятия компетентных решений с учетом всей имеющейся информации. Команде руководителей высшего звена необходимо осознать свою ведущую роль в процессе обеспечения устойчивости организации к киберрискам и стремиться задавать нужный тон на всех уровнях управления компанией. Руководителям важно понимать значение минимизации киберрисков как одной из основных задач в работе по обеспечению непрерывного движения организации к успеху [3].

Выводы. Вот несколько основных шагов, которые могут быть рекомендованы руководителям высшего звена в этом направлении:

- создание системы управления киберрисками;
- понимание границ киберпространства своей организации;
- определение своих жизненно важных бизнес-процессов и активов;
- выявление существующих киберугроз;
- усовершенствование собственных методов киберразведки;
- эффективное использование различных вариантов страхования от киберрисков;
- модернизация технологий в области обеспечения кибербезопасности;
- оптимизация процесса сбора, анализа и представления информации;
- планирование работы и ответные действия.

Однако по мере того, как число инцидентов по всему миру продолжает стремительно расти, становится ясно, что киберриски никогда не будут полностью ликвидированы.

Литература

1. Старостина Е. Управление киберрисками в новом году: первые шаги в этом направлении // Информационная безопасность // [Электронный ресурс]. – Режим доступа: www.pwc.com/gsiss2015 (дата обращения: 2301.2023).

2. Бойченко О.В. Управление рисками кибербезопасности / Бойченко О.В. // В сборнике: Актуальные проблемы и перспективы развития экономики. Труды XXI Международной научно-практической конференции. Симферополь, 2022. С. 6-8.

3. Бойченко О.В. Модель многоступенчатой кибератаки CYBER KILL CHAIN / Бойченко О.В. // В сборнике: Дистанционные образовательные технологии. Материалы VII международной научно-практической конференции. Симферополь, 2022. С. 246-250.

УДК 004.056.33.5/2

Бойченко Олег Валериевич
д.т.н., профессор
Посыпкин Илья Игоревич
обучающийся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КИБЕРБЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ

Актуальность исследования. Проблема обеспечения отказобезопасности в системах управления неразрывно связана с вопросами обеспечения их информационной защищенности в первую очередь от кибератак. Термин «кибер» определяется как «имеющий отношение к информационным технологиям». Информационные технологии реализуются в так называемом киберпространстве, под которым понимается «среда, созданная при помощи физических и не физических компонентов, характеризуемая использованием компьютеров и электромагнитного диапазона для хранения, изменения данных и обмена данными при помощи компьютерных сетей». Использование кибернетических возможностей с целью достижения задач в киберпространстве или с помощью киберпространства определяется как кибероперация. Теперь мы можем дать определение понятия «кибератака»: кибератака — это кибероперация, как наступательная, так и оборонительная, которая может привести к нанесению ущерба здоровью людей или человеческим жертвам, или к нанесению материального ущерба или к разрушению объектов [1].

Цель работы состоит в исследовании проблем, связанных с обеспечением кибербезопасности цифровых технологий в Российской Федерации для создания условий эффективного функционирования информационных систем управления экономикой в условиях широкомасштабного кибервлияния злоумышленников.

Методы исследования. Кибер-защищенность как способность информационной системы управления успешно выполнять предусмотренные задачи в условиях деструктивных воздействий, вызванных кибератаками, а также технологическими нарушениями и/или отказами

составных технических средств. Основные угрозы нарушения киберзащищенности в информационных системах представлены на рис. 1.

Говоря о информационных атаках, следует отметить, что результатом успешной кибератаки может стать нарушение целостности или доступности информации, для чего злоумышленники часто используют специализированное ПО, позволяющее автоматизировать действия, выполняемые на различных стадиях атаки.

В общем случае в любой кибератаке можно выделить четыре стадии:

1) рекогносцировка. На этой стадии нарушитель старается получить как можно больше информации об объекте атаки, чтобы на ее основе спланировать дальнейшие этапы вторжения. Этим целям может служить, например, информация о типе и версии операционной системы; список пользователей, зарегистрированных в системе; сведения об используемом прикладном ПО и т.д.;

2) вторжение. На этом этапе нарушитель получает несанкционированный доступ к тем ресурсам, на которые совершается атака;

3) атакующее воздействие. На данной стадии реализуются те цели, ради которых и предпринималась атака: например, нарушение работоспособности системы, удаление или модификация данных и т.д. При этом атакующий часто выполняет операции, направленные на удаление следов его присутствия в системе. Всякая атака основана на наличии в системе управления уязвимостей, и «правильное» использование хотя бы одной из них открывает злоумышленнику вход в систему;

4) развитие атаки. После атакующего воздействия нарушитель стремится перевести атаку в фазу дальнейшего развития. Для этого в систему обычно внедряется вредоносная программа, с помощью которой можно организовать атаку на другие средства системы [2].

Рисунок 1 – Концепция обеспечения гарантированного уровня

Отметим, что полное устранение опасных отказов в управлении теоретически возможно, но практически не осуществимо, поскольку потребует экономических затрат, заведомо больших, чем ожидаемый ущерб от воздействия опасных отказов. Реальный путь — это определение допустимого уровня риска от кибератак и создание эффективной защиты от опасных отказов [3].

Результаты исследования. Абсолютной киберзащищенности невозможно достичь, поскольку устранение одних уязвимостей в системе не исключает возможности появления новых. Проблема обеспечения киберзащищенности — это проблема совершенствования «щита» от нападения «меча».

Выводы. Одновременно с повышением уровня защиты совершенствуются средства нападения, и не факт, что эффективность средств защиты в определенные отрезки времени сколь угодно выше эффективности средств нападения.

Литература
1. ИСО/МЭК 27032:2012 (ISO/IEC 27032:2012). Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности.
2. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435 (дата обращения: 23.01.2023).
3. Казарин, О. В. Методология защиты программного обеспечения / О. В. Казарин. — М.: МЦНМО, 2009.

УДК 338

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Кравчук Анастасия Эдуардовна
обучающаяся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СОВРЕМЕННЫЕ СПОСОБЫ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ

Благодаря развитию информационных технологий для современного бизнеса начинается новый этап повышения производительности, сокращения времени на выполнение бизнес-процессов и минимизации затрат на человеческие ресурсы за счет внедрения автоматизированных систем [1]. Для начала мы обратимся к определению автоматизации.

Автоматизации бизнес-процессов – это использование технологий для автоматизации задач, которые повторяются и выполняются вручную, в рамках всей организации с целью достижения максимальной эффективности и ценности. Начало первой настоящей формы автоматизации было положено в 1913 году, когда Генри Фордом была изобретена первая движущаяся сборочная линия для массового производства своих автомобилей Model T [2], поэтому понятие автоматизации не является новым, однако период её активной трансформации и возникновения различных способов автоматизировать бизнес-процесс связаны с появлением цифровых технологий.

Несмотря на довольно длительное существования такого явления как «автоматизация», по сей день её актуальность очень велика и с каждым годом только возрастает. Это связано со сложностью бизнес-процессов в целом и постоянной необходимости сделать их наиболее эффективными. В первую очередь это относится к бизнес-процессам, включающим в себя ручную и бумажную документацию, сейчас все большее количество информации подлежит оцифровке для удобства её дальнейшего использования и увеличения производительности сотрудников. Также это касается и более трудоемких процессов, например, в промышленных областях, где машина может выполнять ручные процессы намного быстрее и качественнее, чем человек [3].

Далее мы рассмотрим основные виды автоматизации бизнес-процессов, выделим их отличия и особенности:

1. Роботизированная автоматизация процессов (RPA). В целом данный вид автоматизации представляет некоторое программное обеспечение, действие которого направлено на замену деятельности человека в выполнении конкретного бизнес-процесса. RPA ориентирована в основном на автоматизацию простых и повторяющихся задач, которые не требуют принятия решений и имеют четкий последовательный алгоритм, то есть работает со структурированной информацией. К таким задачам мы можем отнести, например, извлечение или ввод данных, создание отчетов и многие другие. Определив «робота» для выполнения простых алгоритмов бизнес-процесса, можно минимизировать затраты предприятия на рабочую силу и значительно ускорить процесс завершения работы.

Преимуществом RPA, помимо сокращения затрат на персонал, является её адаптивность к изменениям, поэтому корректировка системы не будет слишком трудоемкой [4]. Пример использования роботизированной автоматизации процесса: проверка программным роботом надежности контрагента путем проверки документов и официальных реестров на предмет нахождения его в черном списке.

2. Интеллектуальная автоматизация процессов. Это автоматизация человеческих задач на основе предопределенных правил рабочего процесса, которая сочетает в себе искусственный интеллект и роботизированную автоматизацию процессов. Она имеет довольно много общего с RPA, например, ускорение выполнения рабочих процессов, минимизация погрешностей и

оптимизация повторяющихся задач. Однако, интеллектуальная автоматизация не ограничена простыми алгоритмированными задачами, чего нельзя сказать про RPA, а напротив, находит применение для нестандартных и сложных задач. Еще одно отличие интеллектуальной автоматизации от RPA заключается в том, что она одинаково хорошо справляется как со структурированными данными, так и с неструктурированными.

Довольно простой и известный нам пример данного вида автоматизации – чат-бот с искусственным интеллектом, который может взаимодействовать с клиентами. Особенное распространение сейчас он имеет в мессенджерах и на сайтах предоставления различных видов услуг для получения первичной консультации и ответов на часто задаваемые вопросы.

Следует отметить, что оба способа автоматизации хороши, и каждое предприятие имеет свое бизнес-решение. Автоматизация позволяет упростить трудовую деятельность каждого, от уборщика до банковского работника. Разработка новых решений автоматизации и использование цифровых технологий могут послужить предпосылками для перехода на новый этап автоматизации бизнес-процессов.

Литература

1. Клокотов, И. Ю. Актуальность внедрения автоматизации технологических процессов и производств на современном этапе развития нашего общества / И. Ю. Клокотов // Международный журнал прикладных наук и технологий «Integral», 2019. – №1. – С. 143–147.

2. Ford / Википедия – свободная энциклопедия. – Официальный сайт свободной энциклопедии Википедия. - Режим доступа: http://www.ru.wikipedia.org, свободный (дата обращения: 02.02.2023).

3. A future that works: automation, employment, and productivity: Report / McKinsey & Company. 2017. URL: https://www.gita.org.in/Attachments/Reports/MGI-Afuture-that-works-Full-report.pdf (дата обращения: 02.02.2023).

4. Лавров, В. С. Роботизированная автоматизация процессов / В. С. Лавров, С. И. Петюк. // Научные записи молодых исследователей, 2017. – №6. – С. 43–45.

Остапенко Ирина Николаевна
к.э.н., доцент
ФТИ ФГАОУ ВО "КФУ имени В.И. Вернадского"
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИТРИКС-24

В условиях цифровизации всех сфер жизнедеятельности человека особую важность представляет задача автоматизации предприятий для повышения эффективности обработки информации, анализа деятельности, оптимизации менеджмента, принятия эффективных решений. Автоматизированные системы обработки экономической информации (АСОЭИ) представляют собой совокупность различных средств, предназначенных для сбора, подготовки, хранения, обработки и предоставления информации, удовлетворяющей информационные потребности пользователей. На рисунке 1 представлены возможности корпоративного портала Битрикс 24, предназначенного для решения комплекса задач [1].

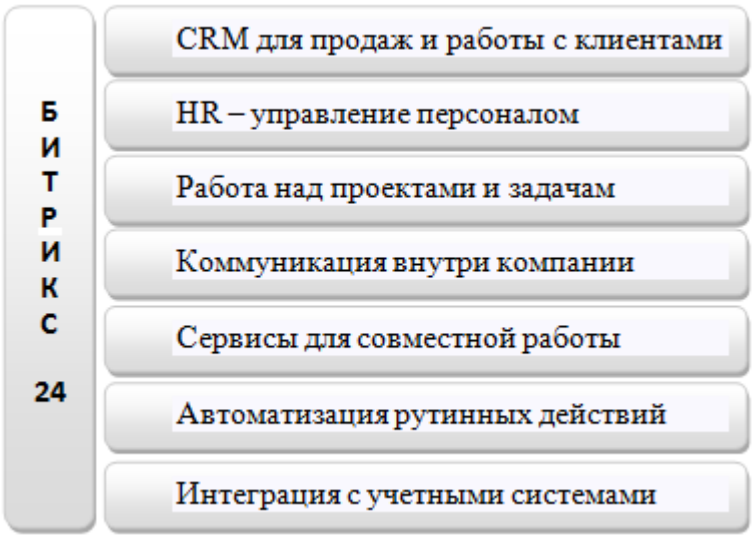

Рисунок 1 – Возможности корпоративного портала Битрикс 24

Каждую возможность можно рассматривать как источник рисков информационной безопасности предприятия. Серверы Битрикс24 определяют большой многофункциональный кластерный комплекс, развернутый и работающий на виртуальных серверах. По данным центра отраслевой разработки «Битрикс24» - это безопасный облачный сервис совместной работы, поскольку данные, загруженные в «Битрикс24» надёжно хранятся, и только пользователь с правами получает к ним доступ в соответствии с системой прав пользователей. Проактивный фильтр (Web Application Firewall) - основа системы ИБ, представляет комплекс специализированных инструментов, выполняющих фильтрацию трафика, обеспечивает защиту от большинства известных атак на веб - приложения. Фильтр распознает большинство опасных угроз и блокирует вторжения на сайт [2]. Политика информационной безопасности (ИБ) портала представляет собой систему правил, ограничивающих возможность авторизации пользователей в целях обеспечения определенного уровня ИБ. Политика ИБ настраивается для группы пользователей. Для пользователей, которые принадлежат к нескольким группам, действует самое строгое правило безопасности по каждому из пунктов, т.е. самая строгая политика ИБ [3].

Литература

1. Корпоративный портал Битрикс24 - платформа для совместной работы сотрудников. – URL: https://bit-24.ru/korporativniy-portal-bitrix24/

2. Битрикс 24 безопасно хранит ваши данные в облачном сервисе для совместной работы. – URL: https://otr-soft.ru/uslugi/1c-bitrix/bitriks24/bezopasnost

3. 1С-Битрикс24: Безопасность и защита от внешних угроз. – URL: https://www.bitrix24.ru/features/box/safe.php

УДК 004.056.5

Титаренко Дмитрий Викторович
к. э. н., доцент
Хименко Владимир Вячеславович
обучающийся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В современных организациях, защита информации является ключевым аспектом, так как вся информация, как большая или маленькая, должна быть защищена и недоступна для несанкционированного доступа. Угрозы безопасности вычислительной системы, такие как вредоносные воздействия, могут негативно повлиять на целостность системы. Для обеспечения безопасности информационных систем, обычно создают специализированные системы защиты, которые обеспечивают безопасность от несанкционированного доступа и вредоносных действий. Администраторы сети используют эту систему защиты для контроля и обеспечения безопасности информационных систем, выполняя функции, такие как диагностика, ремонт

Для усиления безопасности информационных систем разрабатываются различные методы и технологии, такие как шифрование, аутентификация пользователей, контроль доступа, мониторинг и защита от вредоносного ПО. Однако, необходимо понимать, что даже при использовании самых современных методов защиты информации, невозможно полностью исключить риск возникновения угроз безопасности.

Если для примера взять гибридную компанию на 50 сотрудников, в которой часть специалистов трудится в офисе, а часть работает удалённо. Процессы могут быть организованы следующим образом:

Вся конфиденциальная информация – базы данных, архивы и т. д. – хранится на собственных серверах, расположенных в офисе. Доступ к серверной имеют только системные администраторы и руководство компании.

Рабочие компьютеры объединены в доменную сеть (все настройки пользователей хранятся на главном сервере, контроллере домена, все параметры рабочих станций регламентированы).

Удалённые сотрудники получают доступ к сети по VPN.

Весь трафик контролируется межсетевым экраном с грамотно настроенными политиками.

Файлы проверяет антивирус.

Активность сотрудников отслеживают DLP-платформа и Kickidler.

Для упрощения мониторинга можно использовать SIEM-систему.

После внедрения всего перечисленного останется позаботиться о человеческом факторе. Также обязательно нужно подготовить сотрудникам чёткие инструкции по работе с конфиденциальными данными, грамотно настроить все права и не забывать держать руку на пульсе происходящего. Тогда и только тогда конфиденциальные данные будут под защитой.

Литература

1. Иремадзе Э. О. Основы информационной безопасности / А. Заремба // Журнал Скиф. Вопросы студенческой науки – 2022.– №5– С. 261-266.
https://cyberleninka.ru/article/n/osnovy-informatsionnoy-bezopasnosti
2. Сандракова И.В.Контроллинг маркетинга и информационная безопасность торгового предприятия / Н.Ю.Мандрик, И.И.Берсенев, Г.В.Черкасов // Журнал Практический Маркетинг. – 2014.– С. 24-29.
https://cyberleninka.ru/article/n/kontrolling-marketinga-i-informatsionnaya-bezopasnost-torgovogo-predpriyatiya/viewer
3. Лопатин Ю.Н.Информационная безопасность в России. Проблемы, поиски решений // Журнал Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. – 2008. – №2 –С. 51-57.
https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-rossii-problemy-poiski-resheniy/viewer

УДК 338.246

Байракова Ирина Викторовна
к.э.н., доцент кафедры экономической теории
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Полетаева Анна Романовна
обучающаяся 1 курса
направления подготовки 38.03.01 Экономика
ФГАОУ ВО «КФУ им В.И. Вернадского»
г. Симферополь, Российская Федерация

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Безопасность является основным критерием, обеспечивающим гарантии личных, естественных и неотъемлемых прав и свобод человека, а также национальных интересов государства и общества в экономической, политической, экологической, социально-демографической и других сферах. Таким образом, доминирующим элементом в системе безопасности каждого государства являются национальная безопасность.

Экономическая безопасность государства может трактоваться как: состояние устойчивости к негативным факторам; как состояние защищенности национальных интересов; как способность экономики к удовлетворению потребностей государства и общества; как состояние развития экономики страны; как состояние устойчивого Следовательно, в обобщенном виде, экономическая безопасность – такое состояние защищенности национальной экономики страны от внешних и внутренних угроз, которое позволяет ей обеспечить экономическую независимость и суверенитет, социально-экономическую и военно-политическую стабильность общества и государства и их дальнейшее развитие, создать достойные условия жизни для своих граждан.

Составляющими экономической безопасности для основных секторов национальной экономики выступают:

- для реального сектора – производственная безопасность, экологическая безопасность, внешнеторговая безопасность, инвестиционная безопасность, инновационная безопасность, сбытовая безопасность, ресурсно-сырьевая безопасность, технологическая безопасность;
- для социального сектора – безопасность культуры, безопасность правопорядка, демографическая безопасность, политико-правовая безопасность, социальная безопасность, продовольственная безопасность, информационная безопасность;
- для финансового сектора – финансовая безопасность, внешнеэкономическая безопасность.

Наиболее вероятными угрозами экономической безопасности, на локализацию которых должна быть направлена деятельность органов государственной власти, являются:

- увеличение имущественной дифференциации населения, и повышение уровня бедности, что ведет к нарушению социального мира и общественного согласия;
- деформированность структуры экономики;
- возрастание неравномерности социально-экономического развития регионов;
- криминализация общества и экономической деятельности;

Для предотвращения данных угроз, а также обеспечения устойчивых темпов развития национальной экономики необходимо:

- льготное кредитование реального сектора экономики и инфраструктуры проектов;
- поддержка приемлемого уровня жизни населения и недопущение выхода показателей бедности, имущественной дифференциации населения и безработицы за пределы;
- устранение зависимости экономики от импорта и преобладание экспорта продукции;
- реструктуризация хозяйственного комплекса с целью удовлетворения потребностей населения;
- стабильность финансовой и банковской системы, национальной валюты;
- использование новейших технологий на предприятиях;
- обеспечение развития социальной инфраструктуры.

Таким образом, экономическая безопасность представляет собой один из важнейших элементов национальной безопасности, которая позволяет ей обеспечить экономическую независимость и суверенитет, социально-экономическую и военно-политическую стабильность общества и государства и их дальнейшее развитие.

Для обеспечения рационального уровня экономической безопасности государства, а, следовательно, и его национальной безопасности в целом необходимо проведение определенных мероприятий на общегосударственном уровне.

Литература
1. Мусаева, А. М. Экономическая безопасность секторов экономики: учебное пособие / А. М. Мусаева, Г. С. Султанов, М. К. Бамматханова. — Махачкала: ДагГАУ имени М.М.Джамбулатова, 2021. — 208 с. — ISBN 978-5-00128-799-5. — Текст: электронный // Лань : электронно-библиотечная система. — URL: [https://e.lanbook.com/book/254603] (дата обращения: 29.01.2023).
2. Шустикова А.С. Экономическая безопасность как часть национальной безопасности / Символ науки: международный научный журнал. – 2021. – № 5. – С. 76–79.

УДК 004.056

Беляев Михаил Романович
обучающийся 1 курса направления
подготовки 38.03.01 Экономика
Научный руководитель:
Романюк Е.В.
к.э.н., доцент кафедры экономической теории
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

КИБЕРБЕЗОПАСНОСТЬ В БАНКАХ

Вопрос кибербезопасности в банковском секторе с каждым годом становится все более актуальным. Каждый год технологии взлома и системы программирования развиваются, и это отражается в статистике: за последний год количество кибер-атак увеличилось на 6,5%. Именно поэтому данная тема сейчас актуальна как никогда. Однако хакеры, взламывая систему, зарабатывают “копейку”, а ущерб системе наносят на "рубль", и не только на один, а зачастую за многие тысячи. Устранение последствий кибератак требует больших затрат: начиная с 2021 года, в течение следующих пяти лет они будут расти на 15% в год и к 2025 году достигнут $10,5 трлн, говорится в отчете RiskBased Security [1]. Хакеры рассматривают проведение кибератак как бизнес, и поэтому крайне заинтересованы в монетизации своей деятельности. Поэтому банки стали привлекать специальных хакеров, которые начали взламывать банковскую систему, демонстрируя тем самым методы взлома и уязвимости в цифровой защите банка – это стратегия, которая принесла наибольший успех среди всех защит. Тем самым удалось сократить затраты на проблемные сегменты в системе безопасности и поиск специалиста с нужным уровнем квалификации для устранения слабых мест. Поэтому можно сделать вывод, что банковские системы безопасности постоянно развиваются и совершенствуются, но при создании таких современных методов решений и даже выборе компонентов для них, следует помнить, что результат должен обеспечивать как кибербезопасность на современном уровне, так, они должны соответствовать требованиям закона № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ», 152-ФЗ «О персональных данных и многих других законов, под которые попадает деятельность банков» [1; 3].

Помимо национальных требований, банки должны строго соблюдать ряд требований, единых для всей мировой банковской структуры. Например, эмитенты платежных карт должны соответствовать PCI DSS, который является отраслевым стандартом безопасности. Существуют общие межбанковские правила, такие как: SWIFT Customer Security Controls Framework, в котором также прописаны требования кибербезопасности. Другой пример - UserGate NGFW, который предоставляет функции безопасности для сетей любого формата и размера, обеспечивая максимальную видимость событий безопасности и высокий уровень защиты от угроз [1;2]. "Благодаря различным форматам поставки, таким как устройство, виртуальный образ и SecaaS, открывается бесконечное количество сценариев для встраивания функций безопасности в ИТ-архитектуру. В результате мы имеем безопасную киберсреду благодаря тому, что банки проверяют свои слабые места с помощью современных решений и могут закрыть свои уязвимости благодаря гибкой среде UserGate NGFW. А еще они регулируются нашим правительством, которое не позволит банкам пренебрегать личной информацией клиентов и допускать утечки данных. Подводя итог, можно сказать, что вместе с развитием систем взлома идет активное развитие систем защиты, которые также стремительно развиваются, для защиты своих потребителей.

Литература
1. ИБ в банках: особенности межсетевых экранов нового поколения [Электронный ресурс]: - Режим доступа: https://banks.cnews.ru/articles/2022-05-23_ib_v_bankah_osobennosti_mezhsetevyh (дата обращения 29.01.2023).
2. Межсетевой экран следующего поколения [Электронный ресурс]: - Режим доступа: https://www.usergate.com/ru/next-generation-firewall (дата обращения 29.01.2023).

3. Законодательство об информационной безопасности: 5 ФЗ о том, как хранить и защищать информацию [Электронный ресурс]: - Режим доступа: https://mcs.mail.ru/blog/zakonodatelstvo-ob-informatsionnoy-bezopasnosti (дата обращения 29.01.2023).

УДК 338.23

Землячев Сергей Викторович
к.э.н., доцент кафедры гуманитарных
и социально-экономических дисциплин
Крымский филиал ФГБОУ ВО «Российский государственный университет правосудия»
Республика Крым, Россия

ИНДИКАТОРЫ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Построение системы финансовой безопасности невозможно без определения критериальных требований к ней. Следует отметить, что единого подхода по поводу этого важнейшего системообразующего элемента нет.

Так, Е. Ведута указывает, что критерием экономической безопасности государства служит степень соответствия проводимой экономической политики эффективной национальной стратегии и степень доверия к ней как внутри государства, так и со стороны международных организаций [1, с. 330].

Распространенной точкой зрения при этом является то, что как основной критерий может выступать достижение устойчивого, динамичного и эффективного развития экономики с первоочередным решением задач повышения качества жизни.

По определению К.Ипполитова, критерием уровня состояния экономической безопасности является состояние защищенности экономических отношений [2, с. 30].

Кроме интегрального, право на существование имеют и отдельные критерии. Так, например, ими могут выступать уровень жизни населения, уровень и структура безработицы, имущественная дифференциация, импортозависимость экономики, состояние научно-технического потенциала и др.

Достижение критериальных требований к экономической безопасности в целом и финансовой безопасности в частности определяется системой конкретных индикаторов. Индикатор (от лат. indico – указываю, определяю) – элемент, который отражает ход процесса или состояние объекта наблюдений, его качественные и количественные характеристики [3, с. 196].

Финансовая безопасность государства в значительной мере определяется характером формирования государственного и местного бюджета, состоянием его платежного баланса, соотношением денежных средств в официальной и теневой экономике, степенью обеспеченности денег, находящихся в обращении, движением валютных средств.

Именно с помощью разработки обоснованной системы индикаторов можно оперативно анализировать состояние экономической и финансовой безопасности различных объектов, предупреждать развитие негативных тенденций, вносить необходимые коррективы как в ежедневную деятельность, так и на перспективу, прогнозировать развитие событий.

Мы предлагаем разделять индикаторы на общие (уровень и качество жизни, темп инфляции, уровень безработицы, экономический рост, дефицит бюджета, государственный долг, внешний долг, встроенность в мировую экономику, доля «теневой экономики», структура собственности и др.) и региональные (доходы населения, уровень розничных цен, обеспеченность жильем, удельный вес региона в ВВП страны, платежный баланс региона).

Литература

1.Ведута Е.Н. Государственные экономические стратегии. – М.: Российская экономическая академия, 1998. – 440 с.

2.Ипполитов К.Х. Экономическая безопасность: стратегия возрождения России. – М.:Б.И., 1996. – 264 с.

3.Словарь иностранных слов. – М.: Русский язык, 1989. – 624 с.

УДК 338.23

Землячева Ольга Андреевна
к.э.н., доцент кафедры гуманитарных
и социально-экономических дисциплин
Крымский филиал ФГБОУ ВО «Российский государственный университет правосудия»
Республика Крым, Россия

КЛАССИФИКАЦИЯ УГРОЗ В СИСТЕМЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

На финансовую безопасность влияет действие многочисленных внутренних и внешних вызовов и угроз. Обеспечение же действенной системы финансовой безопасности предусматривает выяснение и систематизацию явлений, событий, действий, наступление или осуществление которых прямо или опосредованно может представлять угрозу тому или иному субъекту финансовой безопасности или элементу финансово-кредитной сферы. Значимость классификации угроз финансовой безопасности заключается в необходимости оценить существующую ситуацию, дать оценку существующим негативным моментам и тенденциям из развития, сгруппировать негативные и позитивные действий факторов и на этой основе разработать обоснованные рекомендации для принятия конкретных решений.

Отдельные авторы указывают, что основные угрозы финансовой безопасности (или же угрозы национальным интересам государства в финансово-кредитной сфере) можно классифицировать как внутренние и внешние, существующие и возможные [1, с.81]. По мнению других, перечень угроз можно разделить на три группы: антропогенные, техногенные и стихийные. При этом, критерием распределения угроз на существующие и потенциальные должно быть достижение или недостижение порогового значения по тому или иному индикатору, что характеризует ту или иную угрозу. Те угрозы, по которым уже превышены пороговые значения, следует считать существующими, а те, по которым такие значения не достигнуты, - потенциальными.

На наш взгляд, классификацию угроз финансовой безопасности можно представить таким образом (табл.1).

Таблица 1 – Классификация угроз финансовой безопасности

Классификационный признак	Виды угроз
Отношение к объекту (субъекту)	внутренние, внешние, транснациональные, глобальные
Реальность	существующие, формирующиеся, потенциальные, ожидаемые
Устойчивость	постоянные, внезапные, мгновенные, прогнозируемые
Длительность	длительные, быстро протекающие
Срок действия	долгосрочные, среднесрочные, краткосрочные, внезапные
Стадия	возникающие, затухающие, развивающиеся
Характер влияния	прямые, непосредственные, опосредованные, доминирующие
Обусловленность	вызваны общей социально-экономической ситуацией, специфические
Вид	внутриэкономические, внешнеэкономические, социально-политические, техногенные, природные, управленческо-правовые, антропогенные

Создание действенной системы финансовой безопасности предусматривает четкое определение источников потенциальной угрозы в той или иной сфере, а также существующих и необходимых ресурсов для их нейтрализации. Причем угроза может быть следствием как непредусмотренных обстоятельств, случайных событий, так и осознанных действий, направленных на создание кризиса. Материализоваться она может в прямых убытках или упущенной выгоде.

Литература

1.Землячев С.В. Сущность финансовой безопасности в национальной экономике // Проблемы информационной безопасности: труды VI Всероссийской с международным участием научно-практической конференции, (Симферополь-Гурзуф, 13-15 февраля 2020 г.) / под ред. проф. Бойченко О.В. – Симферополь: ИП Зуева Т.В., 2020. – 158 с. – с.81-82.

УДК 334.021

Иминова Сабина Сабриевна
обучающаяся 1 курса
направления подготовки 38.03.01 Э78кономика
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ

Финансовая безопасность – это одна из главных составляющих экономической безопасности страны. Она является одной из важнейших причин проведения самостоятельной финансово-экономической политики, которая соответствует национальным интересам государства. Благодаря ей, государство может обеспечить устойчивость финансово-экономического развития страны. Фактически, финансовая безопасность помогает определить способность государства осуществлять самостоятельную финансово-экономическую политику в соответствии с национальными интересами своей страны.

Известно, что на динамику финансовой деятельности предприятий влияют как внешние, так и внутренние факторы, однако на российские компании негативно сказываются в основном внешние факторы. К основным элементам создающих положительное обеспечение финансовой безопасности относят: финансы домовладения и домашних хозяйств, финансы юридических лиц различных организаций и финансы некоммерческого сектора.

Финансовая безопасность государства состоит из объекта и субъекта. Объектом данной деятельности является система национальных финансов. Она рассматривается как явление и механизм, именно она направляет деятельность соответствующих органов на предоставление защиты от неблагоприятных факторов, которые сдерживают развитие. Субъектом же в данной системе выступает государство, которое рассматривается относительно трем ветвям власти, но также им может являться и отдельная финансовая система, которая состоит из определенных институтов, регионов и населений. В результате их сотрудничества появляется предмет финансовой безопасности. Предметом является деятельность различных субъектов, осуществляющих комплекс принципов защиты и определенных действий для устойчивого экономического развития, снижения рисков. Именно через концепцию и стратегию финансовой безопасности, государство достигает своей цели, а именно – определения тенденций и факторов, которые влияют на экономику страны.

Что касается элементов финансовой системы безопасности, так это то, что они обеспечивают слаженность развития данной системы. К ним относятся: безопасность системы долговых обязанностей, системы банковских операций и сферы валютных операций, также защищенность денежно-кредитных отношений и бюджетной системы. Главным условием стабильного экономического роста, является слаженная работа всех перечисленных элементов, но если в одной из сфере финансовой системы будет обнаружена проблема, то все остальные ее составляющие будут страдать. Именно поэтому необходимо создавать системный подход в управлении национальной безопасности.

Итак, механизмом обеспечения финансовой безопасности государства называют систему, которая закреплена на уровне законодательства и включающая в себя определенные органы и институты, осуществляющие целенаправленные действия, для положительного развития национальной экономики. Функционирование данного механизма проводится несколькими составляющими. Во-первых, это когда на правовом уровне механизма разрабатывается определенные законодательные акты и нормативные базы, они выступают регулятором финансовых отношений на всех уровнях. Во-вторых, на институциональном уровне, когда регулируется качество выполнения установленных принципов и нормативов. В-третьих, инструментальный уровень, когда субъекты данной системы производят те действия, которые в итоге направлены на достижения цели – обеспечение национальной безопасности.

Литература

1. Экономика предприятия: Учебник. Под ред. Проф. Н.А.Сафронова.: Юрист– М., 2015.
2. Бусыгин А. Предпринимательство. Основной курс: Учебник для ВУЗов.: Инфра - М., 2009.
3. Голубев Ю.Н. и др. Предпринимательство: истоки, проблемы, перспективы. – М., 2017.

УДК 338.2 : 004.9

Круликовский Анатолий Петрович
доцент
Гусев Егор Александрович
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КРИПТОВАЛЮТА, КАК УГРОЗА ФИНАНСОВОЙ БЕЗОПАСНОСТИ СТРАНЫ

Криптовалюта - это цифровая валюта, которая является альтернативной формой платежа, созданной с использованием алгоритмов шифрования. Использование технологий шифрования означает, что криптовалюты функционируют и как валюта, и как виртуальная система учета. Чтобы использовать криптовалюты, вам нужен криптовалютный кошелек. Эти кошельки могут представлять собой программное обеспечение, представляющее собой облачный сервис или хранящееся на вашем компьютере или на вашем мобильном устройстве. Кошельки - это инструмент, с помощью которого вы храните свои ключи шифрования, которые подтверждают вашу личность и ссылаются на вашу криптовалюту.

Несмотря на инновационность технологии «блокчейн» и ряд возможностей, для улучшения систем финансовых услуг или создания новых систем и функций, которые криптовалюта предоставляет во множестве сфер, например, медицине, для контроля изменений и многих других, она может стать серьезной угрозой для финансовой безопасности как страны, так и для обычных граждан [1].

В работе А.А. Крохиной и О.А. Ждановой [2] показано, что риски использования криптовалют можно разделить на микро- и макро- уровни.

К микроуровню относятся риски для использования обычными гражданами. Самым простым примером будет потеря носителя, на котором хранится ключ для кошелька или если пользователь забудет пароль для своего кошелька криптоактивов. Так как данная система децентрализована, то ключ и пароль имеются только в одном экземпляре и возможности как-то восстановить ключ нет. Еще одним примером является перевод на неправильно счёт. Из-за децентрализации, нет возможности в полной мере отследить и вернуть деньги. Из-за технических рисков, пользователь также может потерять свои сбережения. Это может быть как взлом криптокошелька на бирже, так и вирус, который можно «подцепить» из самых разных источников.

К рискам на макроуровне в первую очередь относится спекуляция на рынке цифровых валют. Многие криптоактивы не имеют материальной ценности - в отличие от традиционных ценных бумаг, таких как акции или облигации, которые дают владельцам права на будущие денежные потоки или требования по активам фирмы в случае ликвидации. В результате, большинство криптоактивов в высшей степени спекулятивны, что означает, что их стоимость зависит исключительно от динамики спроса и предложения. Спекулятивные рынки, как правило, нестабильны (в основном обусловлены новостями и техническими показателями, а не фундаментальными), подвержены манипуляциям или мошенничеству и часто способствуют возникновению «пузырей», которые в конечном итоге могут лопнуть, вызвав значительное перераспределение богатства.

Спекуляции на рынках криптоактивов усугубляются агрессивными маркетинговыми кампаниями, рассчитанными на общественность, включая менее искушенных частных инвесторов – в некоторых случаях годовая доходность рекламы достигает 20% [3]. Криптофирмы также продвигали все более сложные продукты, часто без надлежащего раскрытия рисков и с небольшой ответственностью за то, что делали вводящие в заблуждение заявления.

Другим фактором риска, стоящим за спекуляциями, является кредитное плечо, которое доступно розничным инвесторам через маржинальные счета при обмене криптоактивами, традиционные деривативы (особенно фьючерсы или опционы) и через специальные производные криптоактивов (т.е. бессрочные контракты). Большинство крупных бирж криптоактивов позволяют инвесторам делать чрезмерно большие инвестиции по сравнению с их капитальной базой и, следовательно, брать на себя риск, превышающий их способность оставаться платежеспособными.

Из-за своей относительной анонимности, криптовалюта является главным средством для проведения незаконных сделок в сегменте Интернета, известным как даркнет, а также «отмывания» денег. А.С. Ястремский в своей работе [4] показал, что использование анонимных транзакций несет в себе угрозу как для социальной, так и для финансовой сферы страны. Это связано как с незаконными сделкам с продажей оружия, запрещенных веществ и другими запрещенными товарами, так и с уклонением от налогов. Из-за недостаточного регулирования

оборота цифровых валют, сделки с их использованием почти не облагаются налогом, что делает криптовалюту современным аналогом оффшорных зон. Некоторые страны уже вводят законы для регулирования цифровых валют. В работе «Безопасность финансовой системы в рамках появления криптовалюты» [5], приведены примеры, как некоторые из них борются с ними радикальными методами, другие пытаются сохранить баланс между традиционной финансовой системой и крипторынком. Россия, в свою очередь, также стремится к регулированию оборота цифровых валют в стране, создавая новые законопроекты.

Из-за неустойчивых циклов роста и до тех пор, пока не будут применяться соответствующие нормативные положения, криптоактивы влекут за собой многочисленные риски, которые в будущем могут стать актуальными для финансовой стабильности [6]. До сих пор потрясения на рынке криптоактивов, большая часть которых может быть объяснена врожденной уязвимостью рыночной структуры и лежащих в ее основе технологий, не перекинулись на традиционные финансовые системы. Однако могут возникнуть побочные эффекты, в зависимости от того, как будут сдержаться текущие риски и как будут развиваться взаимосвязи между обеими системами. Хотя такие угрозы еще не материализовались, понимание их коренных причин является важным первым шагом в формировании надлежащей реакции регулирующих органов и смягчении последствий рыночных спадов в будущем.

Литература

1. Крылов, А.А. Криптовалюта биткоин – новая форма финансового взаимодействия: основные принципы работы и угрозы экономической безопасности / А.А. Крылов, М.Д. Валерьевич // Микроэкономика. - 2017. - №6. – С.95-100.
2. Крохина, А.А. Влияние криптовалюты на личную финансовую безопасность и финансовую безопасность страны / А.А. Крохина, О.А. Жданова // От научных идей к стратегии бизнес-развития. - 2019.- №1 -С. 105-111.
3. TRV Risk Analysis Crypto-assets and their risks for financial stability [Электронный ресурс]. — Режим доступа: https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf (дата обращения: 10.02.2023г.)
4. Ястремский, А.С. Криптовалюта как источник возникновения угроз финансовой безопасности субъектов экономики / А.С. Ястремский // Аллея Науки. – 2018. - № 10(26). – С.579-584.
5. Мамаева, Л.Н. Безопасность финансовой системы в рамках появления криптовалюты / Л.Н. Мамаева, В.А. Лазарева, К.С. Рыбакова, М.В. Кирюхина // Экономическая безопасность и качество. – 2018. - №1(30). – С. 53-56.
6. Сильченков И.А. Криптовалюта как современный вызов экономической системе безопасности государства / И.А.Сильченков // Научный вестник Южного института менеджмента. – 2019. - №3. – С.83-87.

УДК 336.027

Мустафаева Эсма Рустемовна
обучающаяся 1 курса направления
подготовки 38.03.01 Экономика
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Байракова Ирина Викторовна
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ ХОЗЯЙСТВОВАНИЯ

На современную экономику все больше оказывают влияние новые революционные технологии, появление и внедрение которых ученые соотносят с четвертой промышленной революцией. Экономика сталкивается с новыми вызовами и проблемами, для преодоления которых необходима разработка и реализация новых программ развития. Очевидно, что в этих условиях важным фактором осуществления прорыва в научно-технологическом и социально-экономическом прогрессе страны является становление цифровой экономики, подразумевающей создание систем, в которых данные в цифровой форме станут ключевым фактором производства во всех сферах социально-экономической деятельности.

К цифровым технологиям относят новые поколения роботов, использование больших данных, 3D-печать, нейротехнологии, биотехнологии, виртуальную и дополненную реальность, так называемый Интернет вещей и т.д. В последние годы основой функционирования и

ключевым фактором развития экономики стало применение искусственного интеллекта, применение которого обеспечивает повышение экономических показателей страны.

В любой современной экономике важной составляющей является финансовая система, представляющая собой организацию денежных отношений. С развитием финансовых взаимодействий возникло понятие финансовая безопасность субъектов хозяйствования, предусматривающая состояние защищенности финансовых отношений от внешних и внутренних угроз.

В экономической теории выделяют субъекты экономических отношений, к ним относят: домашние хозяйства, предприятия и государство. Рассмотрим роль искусственного интеллекта в обеспечении их финансовой безопасности.

Искусственный интеллект активно используется для совершенствования работы в кредитно-банковской сфере, в рамках бюджетно-налоговой и валютно-денежной систем, в том числе с целью создания условий, которые обеспечат финансовую безопасность домашних хозяйств, предприятий и государства. Применение голосовых помощников, чат-ботов способствует ускорению обслуживания, консультированию с учетом индивидуальных предпочтений клиента в круглосуточном режиме, предоставлению широкого спектра информации о различных услугах в кратчайшие сроки. Это позволяет человеку или группе лиц своевременно получать информацию о состоянии своих доходов и расходов, определять план действий с учетом текущей ситуации на различных рынках. Кроме того, искусственный интеллект на основе прошлогодних данных может оценить риски тех или иных инвестиций, это способствует принятию клиентами более обоснованных инвестиционных решений, которые в будущем максимизируют прибыль.

Анализируя большие объемы информации, искусственный интеллект предоставляет государству информацию о балансе доходов и расходов государственных и местных бюджетов, повышает рациональность и качество распределения бюджетных средств, определяет оптимальные объемы налоговых поступлений, соотношения объемов иностранных инвестиций в страну и отечественных инвестиций в другие страны. Это способствует разработке экономической стратегии государства, которая в текущих условиях позволит обеспечить стабильное развитие и функционирование финансовой системы государства и национальной экономики.

Деньги все время находятся в движении, переходят из рук в руки, списываются с одного счета и переводятся на другой. Искусственный интеллект снижает вероятность человеческой ошибки при совершении сделок. Он помогает корректно ввести необходимые данные, что сокращает риски потери денежных средств.

Субъекты хозяйствования применяют искусственный интеллект для борьбы с мошенничеством. Используя данные о прошлых преступлениях, искусственный интеллект анализирует сходства и выстраивает закономерности поведения человека при намерении совершить хищение чужого имущества путем обмана. Таким образом, ему удается обнаружить и предотвратить попытку мошенничества, при этом минимизировав угрозы, связанные с финансами, обеспечив устойчивое экономическое развитие государства, платежно-расчетной системы и основных финансово-экономических параметров.

Итак, в XXI веке использование искусственного интеллекта значительно меняет многие отрасли экономики. Технологии с использованием искусственного интеллекта совершают прорыв в научно-технологическом и социально-экономическом развитии страны, а также в области финансовой безопасности субъектов хозяйствования.

Литература

1. Искусственный интеллект в сфере финансовых технологий [Электронный ресурс]: сайт. – Режим доступа: https://cdo2day.ru/cifrovoj-analiz/iskusstvennyj-intellekt-v-sfere-finansovyh-tehnologij/

2. Свирина М.В. Роль искусственного интеллекта в системе обеспечения экономической безопасности страны // Современная наука. 2021. №6. С. 55-56.

Остапенко Ирина Николаевна
к.э.н., доцент
Кривцова София Сергеевна
обучающаяся
ФТИ ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ДЛЯ ЗАЩИТЫ КИБЕРБЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ

Финансовая выгода часто является основоположником передовых атак. Вредоносное ПО может использовать уязвимости в финансовой платформе SWIFT банка, изменив определенную библиотеку, заставив хост-приложение определить, что неудачная проверка безопасности на самом деле прошла успешно [1].

Во время атаки APT (Advanced Persistent Threat или постоянная угроза повышенной сложности) злоумышленники внедряются в сеть, обеспечивая загрузку передовых вредоносных программ с целью выгрузки целевых баз данных.

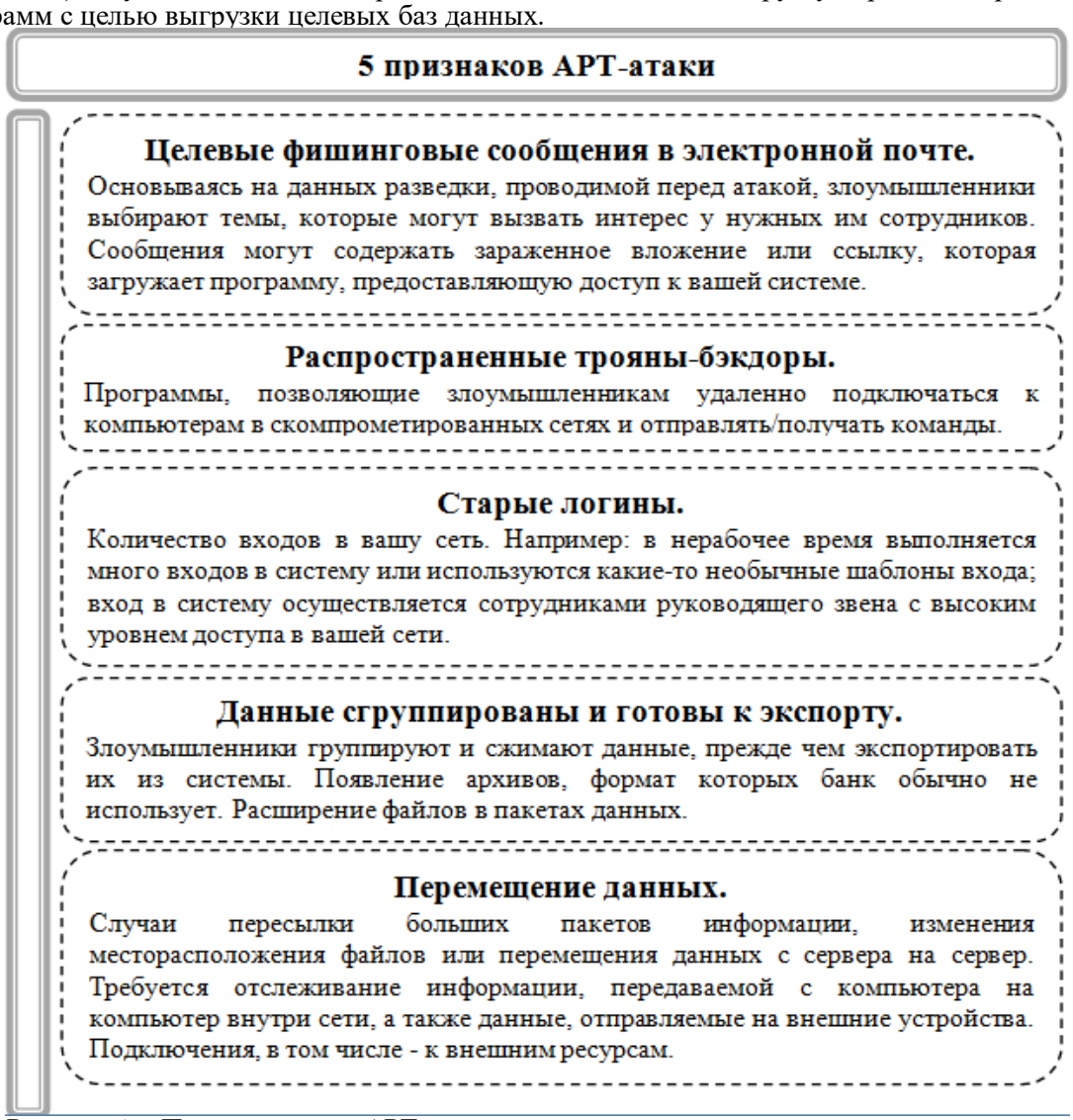

Рисунок 1 – Пять признаков APT – атаки
Источник: составлено авторами на основании [2].

Решения для анализа данных, разработанные с учетом предотвращения мошенничества, могут выявить потенциальное мошенничество в широком спектре контекстов.

Например, клиенты, которые имеют депозитные или текущие счета или имеют кредитную карту, обычно имеют определенные модели использования. Аналитические инструменты могут объединять эти шаблоны из разных источников, а затем проверять показатели мошенничества.

Используя аналитическое решение, банки могут сравнить данные обработки для данной транзакции с базовым уровнем того, как система обрабатывает платеж. В результате можно

распознать, когда транзакция использует стороннюю службу, и организация может быть идентифицирована как новый потенциальный метод мошенничества.

Большинство банков используют несколько технологий в рамках своей деятельности по борьбе с мошенничеством. Сегментация является фундаментальным компонентом борьбы с отмыванием денег (AML) и связана с группировкой клиентов на основе аналогичных транзакционных атрибутов. Используя передовые методы интеллектуального анализа и агрегирования данных, банки могут перейти от небольшого количества сегментов высокого уровня, основанных на сегментации, базирующейся на гипотезах, к сегментам более низкого уровня, управляемым поведением, посредством сегментации, управляемой данными [3].

Сегментация на основе данных включает в себя следующие шаги:

1. Определение совокупного объема данных.
2. Создание аналитической базовой таблицы для уникальности профиля.
3. Построение алгоритмов топологической модели.
4. Проверка модели с помощью наборов тестовых и учебных наборов данных.
5. Генерирование сегмента.

Поскольку традиционные процессы и изолированные команды не поддерживают гибкое реагирование на потребности клиентов и рынка, банки смоделировали новые «пути работы», включая ИИ и RPA. Интеллектуальная автоматизация в RPA создала рост благодаря набору функций, расширяющих традиционные решения по автоматизации. Банки рассматривают RPA как отправную точку на своем пути к раскрытию ощутимых преимуществ, предоставляемых ИИ.

Чтобы справиться с растущими требованиями экосистемы мошенничества и рисков, банки добились значительного прогресса в самообучении, интеллектуальных и оптимизированных услугах за счет внедрения передовых инновационных инструментов и технологий, таких как машинное обучение, RPA, большие данные, API, блокчейн и облачные технологии. Это принятие позволило банкам добиться критически важных результатов трансформации бизнеса путем расширения существующей структуры, что привело к повышению операционной эффективности и управлению рисками [4].

Литература

1. Андреев Никита Олегович Современные проблемы безопасности корпоративных сетей // Прикладная информатика. 2008. №1.
2. 5 признаков APT-атаки. Как предотвратить APT-атаку. – URL: https://www.kaspersky.ru/resource-center/threats/advanced-persistent-threat
3. Умаров Т.С., Баженова И.Ю. Современные подходы к механизмам извлечения причинно-следственных связей из неструктурированных текстов на естественном языке // International Journal of Open Information Technologies. 2019. №7.
4. Гарифуллин И.М. Использование нейросетей для выявления мошеннических транзакций // Инновационная наука. 2021. №3.

УДК 339.972

Румачик Наталья Андреевна
к.э.н., доцент
Киваева Виктория Алексеевна
студентка
ФГАОУ ВО «Северо-Кавказский федеральный университет»
Ставропольский край, г. Ставрополь, Россия

ВЛИЯНИЕ САНКЦИЙ НА ОБЕСПЕЧЕНИЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ЭКОНОМИКИ РОССИИ

Финансовая безопасность является одной из важнейших частей, входящих в состав экономической безопасности, которая значительно влияет на состояние экономики государства в целом. Именно поэтому одной из главных задач является обеспечение эффективного функционирования всех её подсистем.

Финансовая безопасность страны подразумевает обеспечение независимости и конкурентоспособности государства в финансово-кредитной и экономической сферах.

Существует два вида воздействия на безопасность в сфере финансов.

На сегодняшний день государство подвергается негативному воздействию внешней среды, что приводит к дисбалансу в различных сферах деятельности, затрудняя работу входящих в них систем.

Таблица 1 – Виды угроз, оказывающих воздействие на финансовую безопасность государства

Виды	Примеры
Внешние угрозы	1. Утрата внешнеэкономических позиций 2. Нарушение национальных приоритетов 3. Противодействие в принятии участия страны в структурах финансового регулирования на международном рынке
Внутренние угрозы	1. Сокращение ресурсов 2. Рост экономической преступности 3. Повышение уровня инфляции

Рассматривая возникшую ситуацию, можно выделить ряд возможных последствий для государства такие, как: изменение макроэкономических показателей; дестабилизация импорта и экспорта товаров; ухудшение работы денежно-кредитной политики и т.д.

В настоящее время на Россию наложено весомое количество санкций. Среди них моно выделить: блокировку валютных резервов Банка России; нефтяное, золотое, угольное эмбарго; блокировка зарубежных активов и многие другие запреты, которые повлияли на состояние финансовой и экономической безопасности страны.

Так, например, в ходе введения новых санкций в стране наблюдалось изменение в динамике такого показателя, как инфляция.

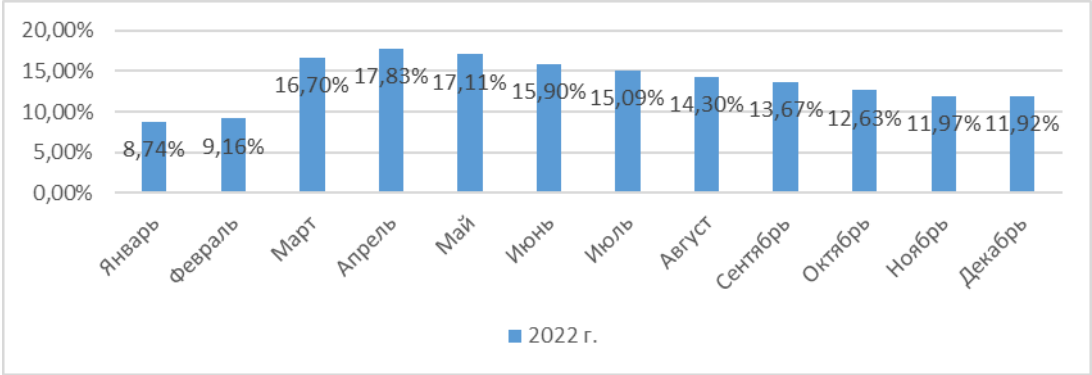

Рисунок 1 – Изменение уровня инфляции

Исходя из данных, представленных на рисунке, можно наблюдать увеличение инфляции в Марте на 7,52 % по сравнению с прошлым месяцем. В Апреле значение показателя почти достигло 18%. Такое резкое изменение показателя произошло в результате введения санкций, что в дальнейшем повлияло на ослабление национальной валюты и увеличения потребительского спроса. Но благодаря увеличению процентной ставки до 20% инфляцию удалось снизить до 11,9%. На сегодняшний день значение данного показателя продолжает оказывать влияние на торговые отношения из-за падения реального дохода населения.

Состояние бюджета в Российской Федерации изменилось в худшую сторону.

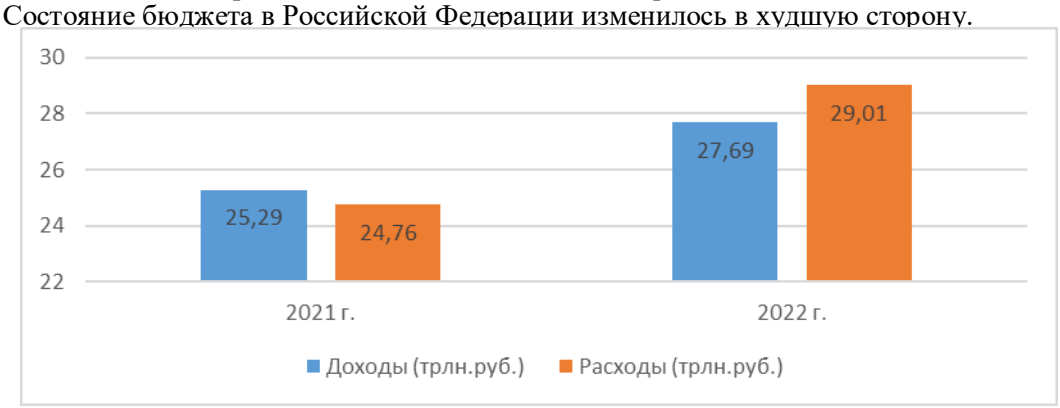

Рисунок 2 – Параметры бюджета Российской Федерации

Исходя из данных проекта Федерального бюджета, 2022 году наблюдается увеличение расходов по сравнению с доходами на 1,32 трлн. руб., что говорит о переходе бюджета страны из профицитного в дефицитное состояние.

По данным пояснительной записки к проекту закона «О Федеральном бюджете на 2023 год и на плановый период 2024 и 2025 годов» можно наблюдать следующие изменения:

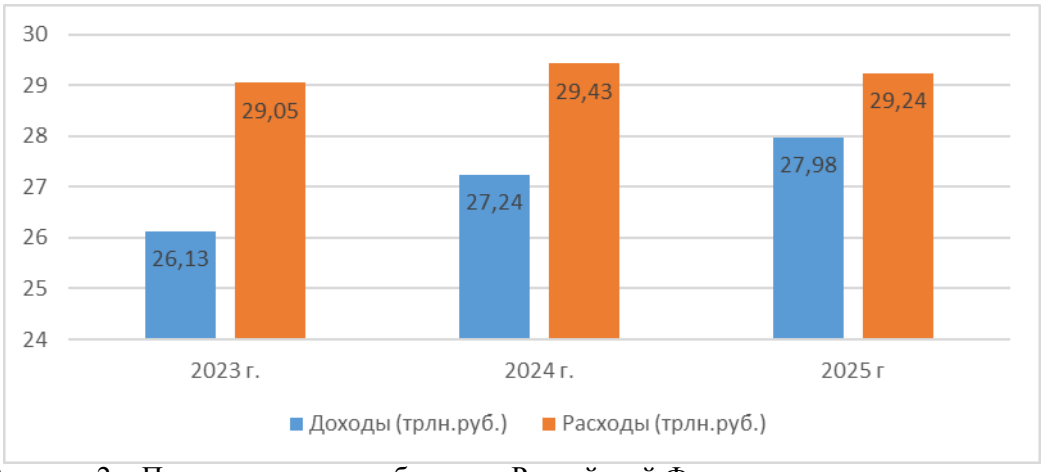

Рисунок 2 – Прогноз изменения бюджета Российской Федерации

Исходя из показателей диаграммы, можно предположить, что состояние бюджета будет дефицитным. Предполагаемые расходы бюджета в 2025 году по сравнению с 2023 увеличиваются на 0,6%. С помощью разработанного проекта планируется увеличить прибыль до 27,98 трлн. руб., что позволит сократить расходы бюджета в 2025 году по сравнению с 2023 на 57%.

Таким образом, можно говорить о том, что состояние российской экономики из-за рекордного количества санкций ухудшилось. Но благодаря быстрому реагированию удалось избежать кризиса в банковском секторе. Стране удалось сформировать денежные резервы благодаря экспорту сырьевых товаров в первом полугодии 2022 года. С помощью разработанного проекта к 2025 году планируется нормализовать экономику государства, там самым обеспечив ей финансовую и экономическую стабильность.

УДК 336

Саврадым Виктория Михайловна
к.э.н., доцент
Севастопольский филиал
РЭУ им. В.Г. Плеханова
Севастополь, Россия

ПРОБЛЕМЫ РАЗРАБОТКИ ЕДИНОЙ КОНЦЕПЦИИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА КАК ВАЖНЕЙШЕЙ СОСТАВНОЙ ЧАСТИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В условиях рыночных отношений, а тем более – в условиях стремительно развивающихся цифровых отношений, проблема обеспечения финансовой безопасности государства приобретает самостоятельное значение как важная составная часть национальной безопасности в целом и функционирования финансовой системы в частности.

Однако в настоящее время данный процесс находится ещё только в начальной стадии свого развития (табл. 1.).

Таблица 1. – Проблемные спектры в сфере обеспечения финансовой стабильности государства

Необходимость	Действительное состояние
1. Научная теория финансовой безопасности	Отсутствует единый системный подход
2. Наличие единой концепции финансовой безопасности государства	Отсутствует
3. Наличие стратегии и тактики обеспечения финансовой безопасности	Частично отражены в государственной программе «Стратегия национальной безопасности»
4. Законодательная база	Многочисленные (иногда разрозненные) законодательные акты, регламентирующие функционирование структурных элементов финансовой системы
5. Информационная база	Носит разрозненный характер
6. Наличие системы обеспечения финансовой безопасности	Отсутствует

Изначальным этапом на пути формирования системы обеспечения финансовой безопасности является научно обоснованная теория финансовой безопасности.

Целостной теории финансовой безопасности в отечественной и зарубежной экономической литературе пока нет. Действующая практика официальной отчетности по показателям финансовой стабильности[1], применяемая многими развитыми странами, касается, в первую очередь, банковского сектора, что явно недостаточно для системного научного обобщения.

Необходимо учитывать многоаспектность категории финансовой безопасности, сложность взаимосвязей и взаимозависимостей её структурных элементов. При этом достаточно много показателей, связанных с финансовой стабильностью: а) носят разрозненный характер; б) рассматриваются в структуре разных экономических категорий, не пересекаясь и взаимно не дополняя друг друга; в) затрудняют систематизацию своим большим количеством и, в некоторых случаях, дублированием.

Г. Шинази, рассматривая вопрос о существовании предела возможностей контроля изменений финансовой стабильности, отмечает, что «Большинство инструментов политики, используемых для поддержания финансовой стабильности, в первую очередь предназначены для решения других задач, таких как защита интересов вкладчиков (инструменты нормативного регулирования), повышение стабильности цен (меры денежно-кредитной политики) или обеспечение быстроты расчетов по финансовым операциям (политика в отношении систем платежей и расчетов)». Тем не менее, изучение мирового и отечественного опыта, зарубежных и отечественных разработок позволили нам наметить пути соответствующего поиска.

В целях формирования единой концепции финансовой безопасности необходимо объединение принципов системного подхода и глобального видения ситуации.

Последовательность разработки и реализации концепции финансовой стабильности государства представлена на рис.1.

Рисунок 1 – Порядок формирования и реализации концепции финансовой безопасности

При разработке концепции финансовой безопасности особое значение отводится современной структуризации финансовой системы, прошедшей в своем развитии длинный исторический путь, поскольку именно достижение и поддержание безопасности её состояния является стратегической целью всей концепции.

Литература

1. Поветкина Н.А. Финансовая устойчивость Российской Федерации. Правовая доктрина и практика обеспечения: монография / под ред. И.И. Кучерова. М.: ИЗиСП, КОНТРАКТ, 2016. 344 с.
2. Саврадым В.М. Финансовая стабильность государства: индикативный подход // Сборник научных трудов по результатам международной научно-практической конференции «Актуальные проблемы и перспективы развития экономики». Симферополь, 2022. – Симферополь: Изд-во КФУ им. В.И. Вернадского, 2022 – С. 199-202.
3. Шинази Г. Дж. Сохранение финансовой стабильности // Вопросы экономики. – 2005. -№ 36. – 27 с.

[1] В более ранних публикациях автор показал взаимосвязь категорий «стабильность» и «безопасность». Одним из положений авторской концепции является следующее: индикаторы безопасности в выступают пограничными в сфере определения стабильности функционирования финансовой системы. В связи с этим, все разработанные теории, закрепленные инструментарии в сфере финансовой стабильности государства логично увязываются с базисным аппаратом развивающейся концепции финансовой безопасности.

УДК 33.01

Цхададзе Нелли Викторовна
д.э.н., профессор
Горшков Фёдор Павлович
ФГОБУ ВО «Финансовый университет при Правительстве РФ»
г. Москва, Россия

БЕЗОПАСНОСТЬ БАНКОВСКОЙ СИСТЕМЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ ЗА ПЕРИОД 1990-2021

Безопасность банковской системы в Российской Федерации вызывает серьезное опасение с момента перехода страны к рыночной экономике в 1990-х годах. За последние три десятилетия российский банковский сектор претерпел существенные изменения, что привело к значительному повышению безопасности банковской системы. Однако все еще существуют проблемы, которые необходимо решить для дальнейшего повышения безопасности банковской системы в Российской Федерации.

1990-е годы - период значительных потрясений для российского банковского сектора, поскольку страна переходила от централизованной плановой экономики к рыночной. В этот период времени банковская система претерпела значительные реформы, включая введение рыночных ставок по кредитам и депозитам, создание частных банков и формирование нормативной базы для банковского сектора. Несмотря на эти реформы, банковский сектор оставался сильно фрагментированным и слабым, многие банки испытывали финансовые трудности из-за отсутствия прозрачности и плохой практики управления.

Одной из основных проблем, с которыми столкнулся банковский сектор в 1990-х годах - отсутствие хорошо разработанной нормативно-правовой базы. Это привело к тому, что многие банки работали без надлежащего надзора, что повысило риск финансового мошенничества и нестабильности. Кроме того, высокий уровень фрагментации банковского сектора затруднял эффективный контроль за ним со стороны регулирующих органов.

В ответ на эти проблемы российское правительство провело ряд реформ, направленных на укрепление нормативно-правовой базы банковского сектора. Эти реформы включали создание Центрального банка России (ЦБ РФ) в качестве основного регулятора банковского сектора, введение системы страхования вкладов для защиты клиентов и создание системы урегулирования проблем несостоятельных банков.

В результате этих реформ за последние два десятилетия банковский сектор Российской Федерации претерпел значительные улучшения. ЦБ РФ завоевал прочную репутацию эффективного регулятора, а система страхования вкладов повысила доверие вкладчиков к банковской системе. Кроме того, система разрешения проблем несостоятельных банков снизила риск банкротства банков и помогла стабилизировать банковский сектор.

Несмотря на эти улучшения, все еще существуют проблемы, которые необходимо решить для дальнейшего повышения безопасности банковской системы в Российской Федерации. Одной из основных трудностей является высокий уровень концентрации в банковском секторе, что повышает риск финансовой нестабильности. Кроме того, банковский сектор по-прежнему сталкивается со значительными проблемами в области финансовой прозрачности и борьбы с отмыванием денег.

Для решения этих проблем российское правительство приняло ряд мер, направленных на повышение безопасности банковской системы. А именно: Введение новых правил, направленных на повышение финансовой прозрачности и борьбу с отмыванием денег, а также разработку новой системы разрешения проблем несостоятельных банков.

В последние годы банковский сектор в России переживает значительный рост: количество банков, работающих в стране, увеличилось с нескольких государственных банков в 1990-х годах до более чем 700 банков сегодня. Рост развития банковского сектора был обусловлен рядом факторов, включая либерализацию банковского сектора, усиление конкуренции и внедрение новых финансовых продуктов и услуг. Несмотря на это, банковский сектор в России по-прежнему сталкивается с рядом сложностей, представляющих угрозу его стабильности и безопасности.

Одним из основных нюансов, с которыми сталкивается российский банковский сектор, является высокий уровень концентрации в нем. На рынке доминирует небольшое количество крупных банков, что повышает риск финансовой нестабильности в случае кризиса. Результатом такой концентрации является быстрое расширение сектора, слабая нормативная база, действовавшая в 1990-е годы, и ограниченная конкуренция в секторе.

Еще одной проблемой, с которой сталкивается российский банковский сектор, - необходимость повышения финансовой прозрачности. Несмотря на введение новых

нормативных актов, отсутствие прозрачности остается серьезной проблемой. Это особенно четко проявляется в отношении деятельности государственных банков, которые по-прежнему активно участвуют в секторе. Отсутствие финансовой прозрачности затрудняет для регулирующих органов эффективный контроль и надзор за сектором, что повышает риск финансового мошенничества и нестабильности.

Борьба с отмыванием денег - еще одна ключевая задача, которая стоит перед российским банковским сектором. Несмотря на введение новых нормативных актов, направленных на борьбу с выводом денег, эта проблема по-прежнему вызывает серьезную озабоченность. Отсутствие эффективных механизмов правоприменения и слабая нормативная база, действовавшая в 1990-е годы, способствовали росту отмывания денег в секторе.

Чтобы избежать данную проблему российское правительство приняло ряд мер, направленных на повышение безопасности и стабильности банковского сектора. Эти меры включают в себя введение новых нормативных актов, направленных на повышение финансовой прозрачности и борьбу с отмыванием денег, а также разработку новой системы разрешения проблем обанкротившихся банков. Правительство также предприняло шаги по повышению конкуренции в секторе, включая внедрение новых финансовых продуктов и услуг, а также либерализацию сектора.

В дополнение к этим мерам российское правительство также предприняло шаги по повышению квалификации и мастерства работников банковского сектора: внедрение новых программ обучения и разработку новых квалификаций для банковских работников. Правительство также поощряет развитие новых технологий в секторе, включая использование цифровых платформ для предоставления финансовых услуг.

Несмотря на эти усилия, предстоит еще многое сделать для дальнейшего повышения безопасности и стабильности банковского сектора в России. Правительству необходимо продолжить реализацию эффективных мер по решению проблем, стоящих перед сектором, включая необходимость повышения финансовой прозрачности, борьбу с отмыванием денег и необходимость повышения конкуренции в секторе. Правительству также необходимо продолжать инвестировать в развитие рабочей силы и внедрение новых технологий в секторе.

Другая серьезная проблема - высокий уровень неработающих кредитов (НЗК) в секторе. Неработающие кредиты — это банковские кредиты, по которым допущен дефолт и которые вряд ли будут погашены. Высокий уровень неработающих кредитов в секторе повышает риск финансовой нестабильности и снижает способность банков предоставлять кредиты, что, в свою очередь, может оказать негативное влияние на экономику в целом.

Одной из основных причин высокого уровня неработающих кредитов в российском банковском секторе является слабая нормативная база, существовавшая в 1990-е годы. Отсутствие эффективного регулирования и надзора в этот период позволило банкам применять рискованную практику кредитования, что в итоге привело к высокому уровню неработающих кредитов в секторе. Кроме того, быстрое расширение банковского сектора и ограниченная конкуренция в нем также способствовали росту неработающих кредитов в секторе.

Российское правительство предприняло ряд мер, направленных на снижение уровня неработающих кредитов в секторе: введение новых правил, направленных на повышение качества практики кредитования, и разработку новых механизмов разрешения проблем обанкротившихся банков. Правительство также оказало поддержку банкам в виде вливаний капитала и других мер, что способствовало повышению их финансовой устойчивости.

Еще одной задачей, стоящей перед банковским сектором России, является необходимость повышения финансовой грамотности населения (финансовая грамотность — это способность людей понимать и эффективно использовать финансовые продукты и услуги). Отсутствие экономической эрудированности у населения может привести к ряду проблем, таких как чрезмерная задолженность граждан, рост мошенничества, связанного с долгами, и неправильное распределение финансовых ресурсов.

Правительство России, чтобы повысить уровень финансовой грамотности, реализует ряд мер, направленных на улучшение финансовой грамотности населения. Эти меры включают в себя внедрение новых программ финансового образования в школах, разработку новых учебных материалов и расширение инициатив по финансовому образованию, направленных на повышение финансовой грамотности населения.

Помимо этих мер, российское правительство также предприняло шаги по повышению доступности финансовых продуктов и услуг: расширение цифрового банкинга и разработку новых финансовых продуктов и услуг, направленных на повышение доступности финансовых продуктов и услуг для физических лиц и малого бизнеса. Правительство также начало работу по улучшению инфраструктуры для предоставления финансовых услуг, включая разработку новых платежных систем и расширение электронных банковских услуг.

Однако правительству Российской Федерации предстоит сделать еще многое для дальнейшего повышения безопасности и стабильности банковского сектора в России. Правительству необходимо будет продолжить реализацию эффективных мер по решению стоящих перед сектором проблем, включая необходимость снижения уровня неработающих кредитов в секторе, повышения финансовой грамотности населения и доступности финансовых продуктов и услуг.

Следующей проблемой, влияющей на безопасность банковского сектора в России, является растущая угроза киберпреступности. С ростом использования цифровых технологий и увеличением зависимости от цифровых банковских услуг риск кибератак и других форм киберпреступности в последние годы значительно возрос. Кибератаки могут привести к потере конфиденциальной информации, финансовым потерям и ущербу для репутации банков.

Для решения этой проблемы российское правительство приняло ряд мер, направленных на повышение кибербезопасности банковского сектора. Это включает в себя разработку новых нормативных актов в области кибербезопасности и создание национальной стратегии кибербезопасности, направленной на повышение устойчивости банковского сектора к кибератакам. Помимо этого, правительство оказывает поддержку банкам в повышении уровня кибербезопасности, включая организацию обучения сотрудников по вопросам кибербезопасности и внедрение новых технологий для защиты от киберугроз.

Российский банковский сектор сталкивается с необходимостью повышения прозрачности и подотчетности сектора. Отсутствие прозрачности в секторе может привести к отсутствию доверия среди клиентов и инвесторов, что может подорвать стабильность сектора. Кроме того, отсутствие подотчетности может привести к плохой практике кредитования, что может привести к росту неработающих кредитов в секторе.

Чтобы помочь в решение данной проблемы российское правительство ввело новые правила, направленные на повышение качества практики кредитования, разработку новых механизмов разрешения проблем несостоятельных банков и расширение требований к финансовой отчетности банков. Кроме того, правительство предприняло шаги по повышению независимости банковского сектора путем снижения влияния государства на этот сектор и повышения уровня конкуренции в нем.

В последние годы российское правительство также предприняло шаги по повышению стабильности банковского сектора путем укрепления нормативно-правовой базы сектора. А именно: введение новых правил, направленных на повышение качества практики кредитования, разработку новых механизмов разрешения проблем несостоятельных банков, а также расширение требований к финансовой отчетности банков. Кроме того, правительство оказывает поддержку банкам в виде вливаний капитала и других мер, направленных на повышение их финансовой стабильности.

В заключение следует отметить, что безопасность банковской системы в Российской Федерации за последние годы значительно улучшилась, однако все еще существуют проблемы, требующие решения. Правительству необходимо будет продолжить реализацию эффективных мер по решению этих проблем, включая необходимость снижения уровня неработающих кредитов в секторе, повышения финансовой грамотности населения, повышения доступности финансовых продуктов и услуг, повышения кибербезопасности сектора, а также повышения прозрачности и подотчетности сектора. Благодаря этому банковский сектор в России сможет продолжать играть важную роль в поддержке роста и стабильности экономики в целом.

Литература

1. Экономическая безопасность банковской системы России// Киберленинка //22.03.2020 //URL: https://cyberleninka.ru/article/n/ekonomicheskaya-bezopasnost-bankovskoy-sistemy-rossii/viewer (дата обращения: 08.02.23).
2. Обеспечение информационной безопасности банковской системы// searchinform//04.02.2020 //URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/bezopasnost-informatsionnykh-sistem/obespechenie-informatsionnoj-bezopasnosti-bankovskoj-sistemy/ (дата обращения: 09.02.23).
3. Банковская безопасность // sravni//13.07.2022// URL: https://www.sravni.ru/enciklopediya/info/bankovskaja-bezopasnost/ (дата обращения: 09.02.23).
4. Банковская безопасность: современная ситуация // InformationSecurity//02.09.2021// URL: https://lib.itsec.ru/articles2/tema/bank_bezopasn_sovremen_situac (дата обращения: 09.02.23).
5. Стандарты Банка России // CBR//25.03.2021// URL: https://www.cbr.ru/information_security/Gubzi_docs/ (дата обращения: 09.02.23).

УДК 330.341.42

Чепоров Валерий Владимирович
к.ф.-м.н., доцент
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ГОСУДАРСТВЕННЫЕ РЕШЕНИЯ, ОСНОВАННЫЕ НА ДАННЫХ В УСЛОВИЯХ ПАНДЕМИИ

Пандемия COVID-19 создала серьезные проблемы для здравоохранения, экономических и социальных систем во всем мире. Столкнувшись с кризисом такого масштаба, органы власти были вынуждены ежедневно принимать трудные решения. В идеале такие политические решения должны основываться на проанализированных данных и предметных знаниях. В частности, лицам, принимающим решения, следует искать полезную информацию, полученную в результате надежного и тщательного анализа точных и актуальных данных. На самом деле конкретные варианты политических решений сильно различались: от полной изоляции до карантина и политики невмешательства. По мере развития пандемии возникают новые дилеммы. В зависимости от чрезвычайности ситуации используемые инструменты и глубина анализа может различаться. Но в любом случае изменчивая реальность, проявляющаяся во времена кризиса, требует обоснованного и надежного подхода к принятию решений на основе данных. Возможность быстро получать высококачественные данные и своевременно их анализировать нельзя считать само собой разумеющимся.

Пандемия предоставляет статистикам и лицам, определяющим политику, возможность пересмотреть роль статистики в широком спектре областей политики. Чрезвычайная ситуация, будь то пандемия, землетрясение или экологическая катастрофа, требует быстрого реагирования от властей. Часто, как в случае с COVID-19, по мере развития чрезвычайной ситуации возникают новые проблемы. Специалисты в области статистики обладают высокой квалификацией для решения таких задач благодаря навыкам анализа и получения обоснованных выводов из зашумленных данных. Несмотря на этот опыт, статистические сообщества во многих странах часто не участвовало в принятии политических решений.

Следует отметить значительную роль проекта «Отслеживание реакции правительства» (Oxford Covid-19 Government Response Tracker OxCGRT), который систематически собирает информацию о политических мерах, которые правительства приняли для борьбы с COVID-19. В проекте отслеживаются различные меры политики с 1 января 2020 года и охватывают более 180 стран и кодируются в виде 23 показателей, таких как закрытие школ, ограничения на поездки, политика вакцинации. Правительственная политика регистрируется по шкале, отражающей масштабы действий правительства, а баллы объединяются в набор индексов политики. Эти данные могут помочь лицам, принимающим решения, и гражданам последовательно понимать ответные меры правительства, способствуя усилиям по борьбе с пандемией.

Задача достижения хорошо информированного принятия решений выходит далеко за рамки наличия «правильных», высококачественных данных или хороших моделей. Успешный подход к принятию решений, основанный на данных, требует эффективного междисциплинарного сотрудничества, которое, в свою очередь, в решающей степени зависит от наличия доверия и общего языка между разрозненными областями.

УДК 330.033.04

Бойченко Олег Валерьевич
д.т.н.. профессор
Луповка Андрей Витальевич
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ СОЦИОИНЖЕНЕРНЫМ АТАКАМ КАК ОСНОВНОЙ УГРОЗЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Повсеместное использование информационных технологий во всех сферах современной жизни, в том числе и в государственных целях влечет за собой сбор и хранение персональных данных пользователей, конфиденциальной информации организаций в информационном пространстве, что требует особого контроля информационной безопасности [3].

В рамках реализации национальной программы «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7, в качестве угроз для реализации цифровой экономики одним из пунктов выделяют: недостаточный уровень кадрового обеспечения в области информационной безопасности.

Существенную роль в системе обеспечения безопасности информации играет человеческий фактор, поскольку человек, являясь пользователем информационной системы, был и остается самым уязвимым ее местом. Люди, работающие с информацией, могут рассматриваться как звено в цепочке механизма, который обеспечивает работоспособность и безопасность всей системы. Человек, имеющий доступ к конфиденциальной информации, преднамеренно или случайно может нарушить ее безопасность (конфиденциальность, целостность или доступность). В связи с этим возникло понятие «социоинженерная атака» [4].

В работе Тулупьевой Т. В. дается следующее определение: «Социоинженерная атака (СИА) — это нетехнический тип атаки, основанный на взаимодействии человека и дополняющий технические атаки» [2, С. 125]. Социальную инженерию в контексте кибербезопасности описывают как тип атаки, в которой злоумышленники используют человеческий фактор в целях хищения, изменения и нарушения целостности данных. Одной из особенностей таких атак можно выделить то, что они являются якобы «безобидны» и законны, поскольку пользователи не подозревают и не понимают то, что они из-за обмана и манипуляции стали жертвами атаки.

Многие отличительные особенности делают социальную инженерию довольно популярной и серьезной, универсальной и постоянной угрозой кибербезопасности [5]:

1. Социальная инженерия использует человеческий фактор без необходимости взлома системы с антивирусным ПО;
2. Зачастую прибегнуть к методу социальной инженерии намного проще относительно проникновению в систему путем взлома, например, выдача себя за другого или телефонный звонок;
3. Так как происходит постоянное совершенствование технологий безопасности ПО и ежедневного обновления баз данных антивирусов, всё чаще злоумышленники используют методы социальной инженерии;
4. Любая информационная система (ИС) полагается на человека или группу лиц, а значит для доступа к ИС невозможно исключить человеческий фактор;
5. Благодаря современным технологиям, таким как машинное обучение, искусственный интеллект, социальная инженерия становится более эффективной и достаточно автоматизированной, что в каком-то смысле приводит к ее распространению и использованию пользователями, которыми не обладают особенными навыками работы с современными технологиями, например: спам-рассылка, чат-боты, автоматизированное ведение диалогов с пользователями социальных сетей и мессенджеров.

Всевозможные действия, произведенные человеком, следствием которых является нарушение безопасности информации условно делят на две группы: намеренные и ненамеренные.

Намеренные (осознаваемые) атаки, выполняемые сотрудниками, связаны с удовлетворением их потребностей. С определенной потребностью связан мотив, где под мотивом понимается: побуждение к деятельности, связанное с удовлетворением потребности субъекта. Такими мотивами могут быть:

— получение финансовой выгоды за счет кражи и продажи конфиденциальных данных;

— получение конкурентных преимуществ;
— желание самореализоваться и др.

Примером ненамеренных или неосознаваемых действий, которые приводят к нарушению безопасности, является обработка человеком почтовых вложений, которые были получены из недостоверных источников или замаскированными под достоверные источники.

В работе Бондарева В. В. [1, С. 15] выделены основные направления деятельности психологов в области защиты информации:

— совершенствование практики подбора кадров, уделяя особое внимание для выявления возможных инсайдеров;
— взаимодействие службы или администратора по обеспечению информационной безопасности с конечным пользователем;
— противодействие методам социальной инженерии.

Основным способом защиты от воздействия методов социальной инженерии в организациях является обучение сотрудников, которое необходимо проводить с учетом рекомендаций психологов. Всем работникам компании необходимо предоставить информацию об опасности раскрытия персональных данных и конфиденциальной корпоративной информации, а так же они должны знать способы предотвращения утечки данных. Каждый сотрудник компании, в зависимости от должности и подразделения, должен иметь личные инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставить в службу технической поддержки, какой информацией могут обмениться сотрудники между собой внутри компании.

Литература

1. Бондарев, В. В. Организационно-психологические аспекты информационной безопасности / В.В. Бондарев // Защита информации. Инсайд. – 2018. – № 6(84). – С. 12-19.

2. Тулупьева, Т. В. Психологические аспекты информационной безопасности организации в контексте социоинженерных атак / Т. В. Тулупьева // Управленческое консультирование. – 2022. – № 2(158). – С. 123-138.

3. Бойченко О.В. Новые виды мошенничества в цифровом пространстве/ О.В. Бойченко // В сборнике «Актуальные проблемы и перспективы развития экономики », 18 Всероссийская с международным участием научно-практическая конференция. – Симферополь: КФУ им. В.И Вернадского, 2019. – С. 10-12.

4. Бойченко О. В. Пути решения проблем противодействия киберугрозам / О.В. Бойченко // В сборнике: Теория и практика экономики и предпринимательства: XVII Всероссийская с международным участием научно-практическая конференция. – Симферополь: Крымский федеральный университет имени В. И. Вернадского, 2020. - С. 29-31.

5. Бойченко О.В. Управление рисками кибербезопасности / О.В. Бойченко // В сборнике: Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической конференции. - Симферополь, 2022. - С. 6-8.

УДК 519.87

Киселев Валерий Георгиевич
к. ф-м. н., доцент
ФИЦ ИУ РАН
Москва, Россия

НАДЕЖНОСТЬ И ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ В СИСТЕМЕ АГРОСТРАХОВАНИЯ

Введение. Аграрное страхование как способ возмещения рисков в сельскохозяйственном производстве в той или иной форме использовалось практически всегда. Известно, что даже в древнем Египте крестьяне (феллахи) использовали некоторый способ страхования как средство борьбы с природными катаклизмами. Страхование зародилось там еще в период разложения первобытнообщинного строя и поначалу носило натуральную форму, когда за счет запасов зерна, фуража, формируемых путем подушных натуральных взносов, оказывалась материальная помощь отдельным пострадавшим крестьянским хозяйствам. По мере развития товарно-денежных отношений страхование в форме натуральных продуктов уступило место страхованию в денежной форме.

В условиях современного общества страхование превратилось в универсальное средство возмещения ущерба практически во всех отраслях человеческой деятельности и, в частности, в растениеводческой отрасли сельского хозяйства, в значительной степени подверженной влиянию погодных факторов.

В растениеводческой отрасли существует два вида программ страхования – программы страхования урожая, в которых страхуются риски, связанные с погодными явлениями, и

программы страхования дохода, которые гарантируют компенсацию потерь производителя сельскохозяйственной продукции не только от недобора урожая, но и от падения цен на производимую продукцию.

Все существующие программы как на этапе разработки, так и на этапе применения используют различную информацию и эффективность применения конкретных программ страхования зависит от надежности и достоверности такой информации.

Данная работа посвящена исследованию информации, необходимой для обеспечения различных программ агрострахования. К этой информации относятся как урожайности сельскохозяйственных культур, так и цены на производимую продукцию (для программ страхования дохода). Под этим подразумевается разработка методик ее получения, обработки и использования. В эпоху цифровизации все это должно быть осуществлено с применением компьютерных технологий и с использованием современных методов.

1. Основные виды информации, используемые в агростраховании

Суть процесса любого страхования заключается в следующем. В начале года страховая компания и агрофирма заключают договор о страховании некоторой культуры, по которому агрофирма должна выплатить страховщику некоторое количество денег, называемой премией. В момент уборки оценивается количество полученного урожая (или дохода, в зависимости от вида страхования) и страховая фирма выплачивает фирме некоторую компенсацию в размере r. Величина этой компенсации определяется по алгоритму, заложенному в содержание используемой программы страхования. Эту связь величины компенсации и величины премии продемонстрируем на примере нескольких программ.

1.1 Индивидуальное мультирисковое страхование урожая

Уровень покрытия по данной программе базируется на средней урожайности каждого отдельного хозяйства. Если полученная в хозяйстве урожайность культуры меньше гарантированной, то застрахованному хозяйству будет выплачена сумма, которой не хватает до гарантированного уровня.

Рассмотрим простой случай страхования урожая одной культуры одной фирмой на площади S со случайной урожайностью y. Пусть прогнозная (фьючерсная) цена единицы производимой продукции на рынке равна $\overline{c}$. Страховая урожайность y_α – то значение урожайности, ниже которой страховая компания выплачивает страховое возмещение, равное стоимости недополученного урожая. Страховое возмещение $r = \max[\overline{c}\, S\,(y_\alpha - y), 0]$. Зная эти выражения, вычисляются все необходимые показатели программы страхования, такие как величина премии, надежность получения дохода и средний доход хозяйства. Здесь y – случайная величина и для вычисления любых параметров, зависящих от нее, необходимо знать по крайней мере функцию распределения этой случайной величины

1.2 Страхование по индексу урожайности

По этой программе компенсация выплачивается исходя из урожайности не отдельного хозяйства, а исходя из средней урожайности всех хозяйств региона, участвующих в данной программе. Премии и компенсационные выплаты вычисляются пропорционально величинам застрахованных в хозяйствах площадей.

В данной программе необходимо знать характеристики средней урожайности застрахованных хозяйств.

1.3 Программа страхования дохода

Данная страховая программа гарантирует определенный уровень дохода, который называется полной гарантией. Для расчета полной гарантии используется цена, которая является максимальной из двух цен – прогнозной весенней цены на урожай (базовой цены) и осенней цены в момент уборки урожая. Страховая же премия рассчитывается исходя из базовой (весенней) цены. Возмещение выплачивается тогда, когда полученный доход (вычисляется исходя из осенней цены в период уборки урожая) меньше полной гарантии на всей застрахованной площади.

Пусть c_n – прогнозируемая весной на период уборки цена, c – реальная цена продукции в момент уборки урожая, $c_г$ – так называемая «гарантированная» цена. и $c_г = \max\left[c_n, c\right]$.

С помощью гарантированной цены вводится понятие полной гарантии дохода $в_г = c_г y_\alpha$, где y_α – то же, что и в программе страхования урожая. Страховые выплаты вычисляются по формуле $r = \max[(в_г - cy), 0]$.

В этой программе страхования добавляется еще один неопределенный фактор – цена реализации произведенной продукции.

Для реализации данной программы необходимо знать кроме данных об урожайности еще информацию о цене продукции и связи ее с величиной урожайности.

1.4 Страхование по индексу дохода

Эта программа базируется на показателях всего района, а не на показателях отдельного хозяйства. По данной программе клиенты получают выплату, если среднегодовой доход всех хозяйств в районе снижается из-за падения урожайности и/или цены на выращенную продукцию.

В данной программе страхования необходимо знать среднюю по региону информацию о доходах хозяйств и прогнозную цену на производимую продукцию.

2 Необходимость цифровизации в системе агрострахования

Мы кратко выше описали несколько основных программ страхования в простейшем случае страхования одним хозяйством одной культуры с позиций одного из участников страховой операции – фермерского хозяйства. Реальная ситуация гораздо сложнее, поскольку страховая компания заключает договора по страхованию многих культур с большим количеством фермерских хозяйств. В этом случае приходится учитывать корреляцию урожайностей культур и корреляцию страховых случаев в различных хозяйствах ([3], [4]), причем важную роль для страховой компании играет проблема финансовой устойчивости. Показателем финансовой устойчивости в актуарной математике принято оценивать вероятностью неразорения. Эта задача для агрострахования была частично исследована в работах ([1], [2]).

Учитывая масштабы страны и разнообразия ее климатических зон, можно сделать очевидный вывод о том, что для решения задачи развития системы агрострахования необходимо привлекать самые современные научные и технические средства с широким использованием компьютерных технологий. Выражаясь современным языком, необходимо использовать цифровизацию в этой области.

Весь анализ как существующих программ агрострахования, так и новых разрабатываемых программ, необходимо проводить с использованием надежной разнообразной информации. для каждого региона. Компьютерный банк данных должен содержать агроклиматические, статистические данные урожайностей всех культур, экономические и другие данные, относящиеся к данной проблеме агрострахования.

3 О методах решения задач актуарной математики в агростраховании

В работах ([1]-[6]) были проведены исследования различных проблем агрострахования. В этих работах были использованы как аналитические методы, так и методы статистического моделирования. При исследовании проблем аналитическими методами необходимо вычислять интегралы Стильтьеса вида

$$\int f(y)dF(y), \int f(c)dF(c), \int f(y,c)dF(y,c),$$

где символом F обозначена соответствующая функция распределения.

Можно сделать некоторые определенные выводы относительно эффективности этих методов в данном случае. Основной вывод заключается в том, что аналитические методы только в модельных случаях помогают выявить основные особенности данной проблемы, а точные рекомендации возможно разрабатывать только с применением методов статистического моделирования.

Однако как в первом, так и во втором случае для проведения расчетов требуется надежная и достоверная информация. Основная информация, требуемая для проведения соответствующих исследований – это информация об урожайности страхуемых культур для всех хозяйств а также информация о рыночных ценах на производимую продукцию и связь урожайностей с этими рыночными ценами. Этим вопросам были посвящены исследования ([5]-[6]). Здесь мы приведем основные результаты этих исследований.

4 О построении функции распределения урожайностей культур в хозяйствах

Для построения эмпирической функции распределения урожайности в каждом хозяйстве необходимо иметь достаточно длинные статистические ряды. Такая информация имеется для административных единиц в ежегодных статистических справочниках.

Известно, что урожайность в данном районе зависит от трех основных факторов:

- климатических условий, которые со временем имеют тенденцию к изменению;
- научно-технического прогресса – использования новых перспективных сортов, современных технологий и современной техники;

- человеческого фактора – качества выполняемых работ.

По-видимому эти и, возможно, другие факторы определяют видимые тренды в статистических рядах урожайностей. Имея конкретный статистический материал, можно провести исследования на предмет существования и изменения тренда. Для этого можно воспользоваться существующими многочисленными методами математической статистики, которые, например, изложены в работах [8-12].

Для построения эмпирических закономерностей по данным наблюдениям желательно использовать максимум имеющейся информации при наличии выявленных трендов. В работе [5] предложен метод обработки статистической информации, использующий весь ее объем. Этот метод предполагает, что общий тренд можно представить в виде линейного сплайна, т.е. на каждом интервале имеется свой тренд в виде линейной функции, а во внутренних граничных точках значения соседних линейных функций совпадают. (Сплайны более высокого порядка в данном случае рассматривать не имеет смысла).

Таким образом, на n- м интервале урожайность определяется уравнением $y^n(t) = a^n + b^n t + \varepsilon(t)$, где $\varepsilon(t)$ – на всех интервалах – случайные некоррелированные величины с $E\varepsilon = 0$ и постоянной дисперсией.

Неизвестные коэффициенты α^n, β^n, определяющие тренд на n -м интервале, будем определять методом наименьших квадратов с дополнительными условиями равенства значений трендов слева и справа в каждой точке излома.

Вычитая из имеющихся измерений величину тренда в каждой точке, получим последовательность M (это общее количество всех точек) значений случайной величины.

Из них построим вариационный ряд $\varepsilon_1, \varepsilon_2, ...\varepsilon_M$, а по нему построим $F(\varepsilon)$ – эмпирическую функцию распределения величины ε. Эмпирическая функция распределения урожайности y будет отличаться от $F(\varepsilon)$ только сдвигом, т.е. $F(y,t) = F(\varepsilon + \alpha^n + \beta^n t)$.

Далее, страховая компания заключает страховой договор со многими агрофирмами по целому ряду культур и должна знать информацию об урожайности страхуемых культур в данных хозяйствах. Однако поскольку таких агрофирм-страхователей может быть очень много, то следует ожидать, что для всех фирм необходимой информации не найдется. Поэтому нужен способ использования агрегированной информации. Что под этим подразумевается? В каждом административном районе имеется необходимая информация о средней по району урожайности культур за ряд лет. Эта та наиболее подробная информация, на которую можно рассчитывать. Таким образом, район будем считать минимальной информационной зоной для страховой компании.

На областном уровне хорошо известно деление всей территории на природно-экономические зоны, которые определяются средней оценкой пашни (в баллах), среднегодовой температурой, суммой температур выше десяти градусов, количеством осадков, продолжительностью безморозного периода.

Естественно, что в разных таких зонах урожайности будут различаться. Это можно учесть следующим образом. Пусть y_i, S_i – урожайность некоторой культуры и занятая под ней площадь в i-й административной единицы, а y_{ij}, S_{ij} – соответственно урожайность и площадь под этой культурой, расположенной в i-й административной единице и в j – й природно-экономической зоне. Тогда можно записать следующие соотношения

$$y_i = \sum_j y_{ij} S_{ij} / S_i, \quad y_{ij} / y_{ik} = \alpha^0_{jk},$$

где величину константы α^0_{jk} можно определить по данным опытных хозяйств по соотношению $y_{0j} / y_{0k} = \alpha^0_{jk}$, в котором переменные с индексом 0 относятся к опытным хозяйствам. Из этих соотношений можно найти искомые данные y_{ij} и построить соответствующую функцию распределения.

Таким образом, территорию, которую обслуживает страховая компания, можно разбить на ряд информационных зон, которые характеризуются одинаковыми природно-климатическими условиями и, следовательно, одинаковыми урожайностями культур.

5. Информационная база для страхования дохода

Из работы [6] следует, что в общем случае для реализации программы страхования дохода необходимо знать совместную функцию распределения урожайности и цены реализации производимого продукта.

Сразу возникает вопрос – что это за цены? Это могут быть либо местные цены, либо региональные или даже общегосударственные. Далее, очень важным аспектом для построения упомянутых выше функций распределения является установление связи между уровнем урожайности и ценой. Например, насколько цена продукции на этапе сбора урожая отражает местный или региональный уровень урожайности данной культуры? Ответ на этот вопрос требует знаний не только о ситуации на местном рынке (ситуации местных производителей), но и знаний о ситуации на региональном, а иногда и национальном рынке.

Идеальный рынок предполагает, что снижение уровня урожайности приводит к снижению объема предлагаемой продукции на рынке и, таким образом, способствует повышению цен и наоборот, уровень урожайности, превышающий средний, является причиной снижения цены. Таким образом, в условиях идеального рынка должна существовать отрицательная корреляция уровня урожайности и цены, но реальный рынок отличается от идеальной модели.

В обзорах экономических аналитиков и, в частности, компании Munich Re выделяется 4 основных отличия.

- Наблюдается большое количество случаев значительного снижения урожайности на местном уровне без всякого влияния на глобальный рынок, поскольку, например, в других регионах показатели урожайности превышают средний уровень и, следовательно, компенсируют снижение урожайности в данном регионе.
- Значительные запасы продукции могут компенсировать последствия снижения уровня урожайности на региональном или глобальном уровне.
- Мировой кризис может способствовать снижению спроса на определенные виды сельскохозяйственной продукции и удерживать цены от повышения.
- Реакция финансовых рынков на колебания цен или только ожидания колебаний часто является иррациональной (необъяснимой с точки зрения разума).

Для того, чтобы системно исследовать любую программу страхования дохода, необходимо проанализировать и по возможности подготовить надежную информационную базу. Это типичная задача теории исследования операций – принятие решения при наличии неопределенности. Для принятия решения необходимо задаться некоторой гипотезой информированности.

1. Во-первых, следует признать, что построение совместной функции распределения по статистическим данным невозможно (из-за отсутствия таковых).
2. Можно задаться некоторым прогнозным значением цены, рассчитывая на реализацию какого-либо варианта (от худшего до реально лучшего).
3. Можно задаться некоторой зависимостью урожайности и цены, например, можно считать, что что цена и урожайность связаны линейной зависимостью $c = \lambda + \mu y + \eta$, где η – случайная величина с заданными характеристиками. Эта гипотеза позволит провести все необходимые расчеты.

Заключение. В работе приведены и обоснованы объемы информации, необходимые для реализации основных программ агрострахования. Приведены особенности связи случайной урожайности и цены на выращенную продукцию. Для использования надежной необходимой информации необходима цифровизация в данной отрасли.

Литература

1. Киселев В.Г., Системный анализ основных систем агрострахования, М.: ВЦ РАН. 2012 28с.
2. Киселев В.Г. Актуарная математика в агростраховании. М.: ВЦ РАН. 2011. 29 с.
3. Киселев В.Г. Математические модели экономики страховой агрокомпании, М.: ВЦ РАН.2013.30с.
4. Киселев В.Г. Информационная база региональной системы агрострахования. //Труды 5-й международной конференции «Управление большими системами» М.: ИПУ РАН, 2011.
5. Киселев В.Г. Особенности информационного обеспечения системы страхования сельскохозяйственного производства.// Материалы международной научно-практической конференции «Математика и ее приложения. Экономическое прогнозирование: модели и методы».г.Орел, 2011, С.236-240.
6. Киселев В.Г. Математические модели в программе страхования дохода агрофирм, М.: ВЦ РАН. 2015. 28 с.
7. Павловский Ю.Н. Имитационные модели и системы. М.: Фазис, 2000. 166 с.
8. Четыркин Е.М. Статистические методы прогнозирования, М.: Статистика, 1977. 200с.
9. Грешилов А.А., Стакун А.А., Стакун В.А. Математические методы построения прогнозов, М.: Радио и связь, 1997. 112с.
10. Гамбаров Г.М. и др. Статистическое моделирование и прогнозирование, М.: Финансы и статистика, 1990. 383с.
11. Андерсен Т. Статистический анализ временных рядов, М.: Мир, 1971
12. Льюис Х.Д. Методы прогнозирования экономических показателей, М.: Финансы и статистика, 1986. 133с.

УДК 32.019.51

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Агеева Каринэ Григорьевна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СИСТЕМНЫЙ АНАЛИЗ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОГРАММНЫХ ПРИЛОЖЕНИЙ ДЛЯ СКЛАДСКОГО УЧЕТА

Автоматизация может рассматриваться в виде одного из направлений, связанного с научно-техническим прогрессом. При этом применяются саморегулирующие технические средства, экономико-математические методы и системы управления [1].

Управление современным предприятием непосредственным образом связано с решением двух задач:

1. Построения интегрированной информационной среды, которая содержала бы актуальные знания и осуществляла информационную поддержку всех этапов проектирования и производства;
2. Обеспечения безопасности функционирования предприятия в смысле снижения рисков потери, порчи или разглашения информации, подлежащей защите. Эти задачи являются одними из самых актуальных в настоящее время, благодаря высокому научно-техническому прогрессу в области автоматизации и информатизации производственных процессов.

Цель автоматизации связана с повышением производительности труда. Улучшается качество продукции, происходит оптимизация в управлении. Человек устраняется от производств, которые опасные для здоровья. В автоматизация, за исключением простейших случаев, необходимо, чтобы был комплексный, системный подход для решения задач [2].

Задача автоматизации тех или иных процессов возникает в современном бизнесе довольно часто. Она актуальна практически для всех компаний, и в особенности тех, которые предоставляют набор товаров и услуг для своих клиентов. В настоящее время без использования компьютерной техники не мыслим практически ни один бизнес, информационные технологии проникли во все сферы жизни человека [3].

Компьютерный учёт товара полностью отличается от классического, рукописного. Компьютерные программы упрощают учёт товаров, сокращают время, требуемое на оформление документов для анализа торговой деятельности, следовательно, при применении компьютерных программ, повышается эффективность работы персонала торгового предприятия, уменьшается время обучения персонала.

Проблема информационной безопасности возникла с появлением средств информационных коммуникаций, а также с осознанием наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путём воздействия на средства информационных коммуникаций, функционирование и развитие которых обеспечивает информационный обмен между всеми элементами социума.

Вопросы безопасности – важная часть концепции внедрения новых информационных технологий во все сферы жизни общества. Увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости [4].

В сфере складского учета фигурируют большие массивы данных, и их утечка может предоставить конкурентам много важной информации о деятельности организации. Необходимость постоянного обновления данных для эффективного мониторинга складских остатков, частое добавление новых позиций и товаров увеличивают количество обращений к данным, а, следовательно, повышают их уязвимость [5].

В большинстве приложений для автоматизации складского учета содержится множество различной конфиденциальной информации.

Последствия от утечки данной информации могут вызвать значительное снижение конкурентной способности оганизации. Особенно это относится к торговым складам. Ведь кроме информации о движении товаров и клиентской базы в системах складского учета для торговли содержатся договора и спецификации, как с поставщиками, так и с клиентами.

Концентрация внимания на вопросе безопасности автоматизации складского учета будет способствовать созданию более надежной организации с точки зрения кибербезопасности.

Автоматизация также увеличивает сложность информационных систем в организации, именно поэтому по мере масштабирования информационной системы необходимо выдвигать инициативы по кибербезопасности для внедрения автоматизированных решений. Пока информация доступна, конфиденциальность, целостность и доступность программ кибербезопасности должны быть гарантированы [6].

Следует отметить, что наряду с развитием новых средств технического обеспечения безопасности, появляются новые методы, алгоритмы и стандарты оценки качества функционирования информационных систем.

Оценить допустимые риски в стратегии развития предприятия невозможно без детального и разностороннего изучения всех возможных угроз. На основе проведенного анализа должны быть выработаны мероприятия по снижению вероятности рисков и степени возможного ущерба. Эти мероприятия могут быть объединены в набор стратегий для оперативной поддержки принятия решений.

В работе Прохорова С.А. [7] показано, что определение величины рисков и набора мероприятий может осуществляться на основе экспертных оценок лиц, принимающих решение. Выбор между стратегиями, а также комбинирование стратегий, должно быть автоматизировано в системе поддержки принятия решений на основе событий.

Развитие интегрированной информационной среды и средств обеспечения безопасности находятся в противодействии. Сохранения тенденции развития предприятия, активных взаимоотношений с партнерами довольно часто ограничивается с целью обеспечения безопасности. В связи с этим, необходимо определить методику взаимодействия различных подразделений предприятия при решении задач повышения эффективности и качества производства за счет совместного развития интегрированной информационной среды и системы обеспечения безопасности.

Литература

1. Ермолова, В.В. Методика построения семантической объектной модели / В.В. Ермолова, Ю.П. Преображенский // Вестник Воронежского института высоких технологий, 2012. — № 9. — С. 87-90.
2. Преображенский, Ю. П. Некоторые проблемы автоматизации процессов / Ю.П. Преображенский // Техника и технологии: пути инновационного развития, 2019. – С. 62-64.
3. Эм, А. А. Разработка автоматизированной информационной системы учета товаров в автотехцентре «АВТОЛИГА» / А. А Эм, Р. И Баженов // Постулат. – 2017. – №. 2.
4. Минаков, А. В. Направления совершенствования порядка проведения инвентаризации с целью обеспечения экономической безопасности предприятия / А. В. Минаков // Роль бухгалтерского учета, контроля и аудита в обеспечении экономической безопасности России. – 2017. – С. 95-102.
5. Толстенко, Д. С. Автоматизация складского учета торговой организации: задачи, этапы, проблемы / Д. С. Толстенко, И. Е. Егорова // Управление, бизнес и власть, 2013. – №. 1. – С. 34.
6. Mohammad, S. M. Security automation in Information technology / S. M. Mohammad, L. Surya // International journal of creative research thoughts (IJCRT)–Volume 6, Issue 2? 2018. – p.p. 901-905
7. Прохоров С. А. Автоматизация комплексного управления безопасностью предприятия / С. А. Прохоров, А. А. Федосеев, А. В. Иващенко. — Самара: СНЦ РАН, 2008 – 55 с.

УДК 657.1.011.56

Соколова Жанна Владимировна
к.и.н., доц. кафедры документоведения
и архивоведения
Волощук Анна Станиславовна
бакалавр
Таврическая академия
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КОНЦЕПЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННЫХ СИСТЕМАХ БУХГАЛТЕРСКОГО УЧЕТА (НА ПРИМЕРЕ КОМПАНИИ «БУХГАЛТЕРСКИЙ ЦЕНТР»)

Проблематика обеспечения качества и надёжности информационных технологий в сфере бухгалтерского учёта особенно актуальна в последние годы. Прежде всего это связано с различными вариантами его организации: создание бухгалтерского отдела, назначение ответственного лица, ведение учета руководителем фирмы, наем приходящего бухгалтера и привлечения аутсорсинговых компаний.

Рассмотрим укрупненные группы более подробно.

Бухгалтер в штате. Это официальное трудоустройство, выплата налогов, затраты на рабочее место в офисе, заработная плата, постоянное обучение, правовые риски, возможен конфликт или увольнение, а также не существует гарантий того, что бухгалтер качественно выполняет свои обязанности.

Приходящий бухгалтер. Данный сотрудник не трудоустроен, позволяя говорить о риске ответственности. Работа осуществляется зачастую в устаревшей программе, возможна потеря данных, а главное оценка деятельности компании осуществляется со стороны, не вникая в ее особенности. Однако выделяется положительная сторона – отсутствие необходимости содержать рабочее место.

Обслуживание онлайн или передача бухгалтерского учёта на аутсорсинг. Отсутствие налогов, сохранность данных, свежая версия программы 1С, гарантия безопасности, полная ответственность, а главное осуществление операций только профессиональными, которые проходят обучение и аттестации. Именно так можно охарактеризовать данный аспект работы.

Таким образом, на основе выделенных сторон организации работы бухгалтерского учета, можно сделать вывод, что в первом случае требуется постоянный контроль и дополнительный аудит, следовательно, данный вид обходится очень дорого для компании и не подходит для малых предприятий. Второй способ меньший по цене, однако подвергается большому риску компании. Третий вид позволит за минимальные деньги получить максимальную ответственность и полный контроль своей деятельности. Аутсорсинг в современных реалиях является более выгодным вложением, позволяя минимизировать риски и выбрать именно тот пакет услуг, который нужен при масштабах и специфики компании.

Осуществив поиск в сети Интернет, на основе критериев масштаба предоставления услуг и опыта работы, была выбрана компания «Бухгалтерский центр» с филиалом в г. Севастополе. Она работает с клиентами в самых различных сферах: начиная с постановки на учёт с нуля, заканчивая счётом налогов. Если говорить коротко, то это профессиональный аутсорсинг, который обеспечивает комплексную поддержку на всех этапах развития. Для начала, стоит отметить, что главным плюсом такой системы является ее адаптация под любой вид деятельности.

Из возможностей, стоит выделить следующие виды услуг: сдача отчётности в электронном виде; ведение книги учёта, доходов и расходов; налоговая оптимизация; выстраивание выгодных договорных отношений с контрагентами; использование налоговых льгот; регистрация ООО, ИП; подготовка пакета учредительных документов для государственной регистрации и внесение в них изменений; ведение кадрового учёта и зарплаты, составляется штатное расписание, приказы трудовые договоры и т.д.; оформление накладных, счетов фактуры; подготовка платёжных поручений клиент банков и уплата налогов, взносов и др.

Таким образом, бухгалтерский центр предоставляет услуги в самых разных сферах деятельности бухгалтерского учёта, что позволяет вести деятельность качественно и без рисков для самой организации. Комплексный пакет услуг позволяет подобрать необходимые для конкретной организации составляющие и избавится от недочетов в данной сфере. Вся информация, которая стала известна в ходе выполнения обязанностей, полностью конфиденциальна, за что несут ответственность сотрудники.

Стартовая цена тарифа 3000 р., которая может варьироваться как в большую, так и в меньшую сторону, полностью позволяя подстроиться под потребности определенной компании. Работа максимально удобна, так как все операции осуществляется онлайн: от отправки заявки до доступа в 1С и обучения.

Стоит отметить главные плюсы такой системы. Во-первых, крымская специализация. С 2014 г. главный офис стал располагаться в Севастополе, это связано некими тонкостями, в том числе и льготном налогообложении. Во-вторых, опыт. Данная компания существует с 1990 г. и по статистике к ней обратилось более 300 организаций. В-третьих, экономичность услуги. Методы оптимизации позволили снизить расходы и налоги клиентов в 3-5 раз. В-четвертых, надёжность и безопасность. По условиям договора компания несёт ответственность за отчётность, гарантирует полную безопасность данных и качество выполнения работы. В-пятых, объективность. Работа только с действующей законодательной базой. В-шестых, современные технологии. Они позволяют быстро и правильно оформлять документы и моментально отправлять их на e-mail.

Самый главный минус возникает в понимании того, что дистанционно невозможно изучить всю специфику организации, в связи с чем могут возникнуть некоторые трудности в работе.

Многие компании как Крыму, так и по всей России сотрудничают с «Бухгалтерским центрам»: ООО «Промышленная компания», ООО «Центр кузнечных технологий», «Новохим», «Легокласс» и др.

Подведём итог. На сегодняшний день все больше руководителей переводят бухгалтерский учет на аутсорсинг, снижая риски и расходы. Приведенный пример «Бухгалтерского центра» позволяет понять, что такие действия реальны и эффективны. Центр работает как с частными лицами, так и с государственными и муниципальными организациями. Адаптация под специфику организаций, в зависимости от масштабов, деятельности, статуса, позволяет говорить о экономии затрат, времени и комплексного подбора услуг под клиента. Аутсорсинг позволяет облегчить деятельность руководителя, оставляя время на стратегические задачи.

Литература

1. Бухгалтерский центр. – URL: https://krym-buhgalter.ru/(дата обращения 06.02.2023). – Текст: электронный.

2. Гарант. Ру «Вся правда про бухгалтерский аутсорсинг». – URL: https://www.garant.ru/1c-wiseadvice/guide/vsya-pravda-pro-buhgalterskij-autsorsing/ (дата обращения 06.02.2023). – Текст: электронный.

Солдатов Максим Александрович
к.ф.-м.н., доцент
Троценко Анастасия Юрьевна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ИНСТРУМЕНТЫ UX-ДИЗАЙНА ДЛЯ СОЗДАНИЯ САЙТА ЭНЕРГОСНАБЖАЮЩИХ ОРГАНИЗАЦИЙ

Инструменты UX оказывают кардинальное влияние на качество мобильных или веб-продуктов. Если выбрать неправильные, то может пострадать качество всей работы.

Два важнейших аспекта дизайна — это пользовательский интерфейс (UI) и пользовательский опыт (UX). Оба относятся к людям, использующим продукт, но смотрят на вещи с другой точки зрения. Пользовательский интерфейс фокусируется на эстетических элементах того, как кто-то взаимодействует с продуктом, например, типографике, цветах, меню и т.д. UX, однако, больше фокусируется на том, как человек использует продукт. Эти две части связаны и иногда разрабатываются в тандеме, но есть очевидные различия. Определение основного пользовательского опыта должно предшествовать детализации дизайна пользовательского интерфейса.

Есть некоторые ключевые аспекты, которые имеют значение при выборе правильного инструмента пользовательского интерфейса (UX) для дизайна энергосбытовых организаций [2]:

1. Полезность: насколько хорошо этот инструмент решает проблемы вашей энергосбытовой организации (передача показаний, просмотр документов и подача заявок на заключение договоров)?
2. Удобство использования: прост ли инструмент в повседневном использовании (оплата сватов, просмотр задолженности)?
3. Сотрудничество: легко ли делиться своей работой с другими (каким образом Вы будете передавать свой дизайн программистам компании)?
4. Интеграция: существуют ли какие-либо интеграции с другими инструментами? Облегчает ли это переход между этапами проектирования?

Рассмотрим некоторые инструменты [1]. Sketch описывает себя как универсальный набор инструментов дизайнера. В нем была предпринята попытка охватить весь процесс проектирования. Он также предназначен для работы с другим вашим программным обеспечением и поставляется с более чем 700 расширениями – фреймворками, плагинами и интеграциями.

Adobe XD включает в себя множество ценных функций, которые помогут вам в создании прототипов. К ним относятся инструменты векторного рисования, 3D-преобразования, повторно используемые компоненты, повторяющиеся сетки, автоматическая анимация и макет с учетом содержимого. Визуализируйте анимации, вставляйте воспроизводимые видео и создавайте яркие и реалистичные прототипы с помощью движения.

Balsamiq — это инструмент для создания каркаса пользовательского интерфейса, который воспроизводит процесс создания эскизов в блокноте или на доске на компьютере. Вы можете использовать его, чтобы думать и сообщать о структуре программного обеспечения или веб-сайта, который вы создаете.

Figma объединяет всех в процессе проектирования, чтобы команды могли быстрее создавать более качественные продукты. Figma — это платформа для проектирования "все в

одном". Кроме того, у компании есть связанный инструмент FigJam, который действует как онлайн-доска для команд. Figma отлично подходит для проектирования, прототипирования и проектирования систем. Затем дизайнеры UX / UI, в свою очередь, могут использовать FigJam для совместной работы и планирования процессов проектирования.

Marvel предлагает быстрое прототипирование, тестирование и передачу команд разработчиков. Его интуитивно понятные инструменты проектирования и прототипирования ускоряют создание макетов и прототипов.

FlowMapp предлагает UX-инструменты для веб-дизайна. Вы можете создавать исключительный UX для красивых продуктов, веб-сайтов и приложений с помощью онлайн-инструментов совместной работы FlowMapp.

Как можно заметить, на рынке есть много инструментов, которые помогают UX / UI-дизайнерам создавать интуитивно понятные сайты для энергосбытовых организаций. Некоторые сосредоточены в основном на дизайне, другие - на картах пути потребителей, макетах и многом другом. Некоторые даже позиционируют себя как универсальные дизайнерские наборы инструментов. Независимо от того, какой этап процесса проектирования интересует энергосбытовую организацию, можно найти качественный инструмент UX / UI-дизайна, который облегчит вашу жизнь и улучшит сотрудничество между вами и членами вашей команды.

Литература

1. Авдеева, Е. 9 инструментов, без которых не обойтись UX/UI-дизайнеру [Электронный ресурс] / Лайфхакер, 2021. – URL: https://lifehacker.ru/instrumenty-dlya-ux-ui-dizajna/ (дата обращения: 05.02.2023).
2. Шайхутдинов, Р. Обзор 20+ программ для UX-дизайнера: какую выбрать и когда. [Электронный ресурс] / UXJournal, 2021. – URL: https://ux-journal.ru/obzor-luchshih-programm-dlya-ux-dizajnera.html (дата обращения: 05.02.2023).

УДК 004.8

Усенко Роман Станиславович
старший преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

О СОВРЕМЕННЫХ НАПРАВЛЕНИЯХ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ: ГЕНЕРАЦИЯ ТЕКСТА

Нейронные сети могут применяться для решения широкого круга задач, они открывают огромные возможности во многих сферах человеческой деятельности. Эра искусственного интеллекта принесла с собой множество достижений, которые изменили наше представление о задачах, которые раньше были слишком сложными для машин [1]. Поскольку спрос на возможности нейронных сетей продолжает расти, технологии, лежащие в их основе, будут становиться еще более сложными, предоставляя нам еще более эффективные способы эффективного решения сложных задач.

Среди основных преимуществ нейронных сетей выделяют достаточно широкий диапазон их применения в различных отраслях науки и производства, среди которых: анализ данных, оптимизация, моделирование и прогнозирование, реклама и маркетинговая деятельность, распознавание изображений и д.р. [2-4]. Области применения нейронных сетей можно классифицировать по нескольким направлениям:

1. В зависимости от направления решаемых задач (классификация; кластеризация; прогнозирование).
2. В зависимости от рода данных, с которыми работает нейронная сеть (численные данные, изображения, текст и т.д.)
3. В зависимости от видов деятельности (экономика, медицина, социальные сети, творчество и др.)

Творческая деятельность всегда считалось прерогативой человека. И если в когнитивных задачах, таких как вычисления и обработка информации, уже признано превосходство искусственного интеллекта и активно пользуются плоды автоматизации, то в творческих видах деятельности, таких как живопись, поэзия или музыка алгоритмы пока уступают человеку [5].

В современном цифровом мире все большее значение приобретает возможность быстро и точно сгенерировать контент [6]. На самом базовом уровне нейронная сеть может генерировать тексты на основе входных данных, таких как набор слов или фраз. Для этого она берет входные данные и создает новый текст на основе закономерностей в этих данных. Помимо генерации

новых текстов на основе исходных данных, нейронные сети можно использовать для улучшения существующих текстов. Чтобы нейросеть работала, в нее на этапе обучения загружают так называемую обучающую выборку. Это множество текстов с определенными параметрами — такими, к которым нейросеть должна стремиться. Нейросеть меняет свою внутреннюю конфигурацию так, чтобы конечные тексты были максимально похожи на то, что находится в обучающей выборке. Чтобы нейронная сеть сравнялась по уровню с профессиональным автором, нужны миллиарды качественных текстов на самые разные темы. Но такого количества хорошего контента просто не существует. Поэтому на текущем этапе невозможно создать нейронную сеть, которая полностью заменит человека [7].

Искусственный интеллект уже повсеместно используется в индустрии высоких технологий, и на данных момент уже находит использование и в средствах массовой информации. На сегодняшний момент уже популярный новостной ресурс публикует статьи, написанные искусственным интеллектом и многие читатели, похоже, этого не заметили или отметили наличие ошибок [8].

В связи со сказанным, можно выделить следующие плюсы и минусы нейронных сетей. Основные плюсы: может сгенерировать текст на любую тему за пару секунд, проанализировать большой объем данных, помочь создать первый черновик: потом на его основе можно создать статью или пост.

Основные минусы: тексты получаются низкого качества, иногда нейросети уходят совсем не туда; нейронные сети нужно постоянно обучать, чтобы повышать качество и релевантность результатов; могут допускать ошибки: фактологические, грамматические, пунктуационные; нет тонких настроек, например, не всегда можно задать нужный объем текста или ключевые слова.

В целом, нейронные сети стали бесценным инструментом при создании нового или улучшении существующего контента, поскольку они способны генерировать реалистично звучащие тексты на основе исходных данных. Поскольку технология искусственного интеллекта продолжает развиваться быстрыми темпами, вероятно, в будущем будет разработано еще больше приложений для них в таких областях, как написание текста, где точность является ключевым фактором.

Большинство разработчиков отмечают, что их системы являются ассистивными. Они не претендуют на полноценную замену человеческого творчества, а, напротив, призваны помочь человеческой музе. Человек не перестанет творить по мере развития алгоритмов и программ, но будет использовать их в своей деятельности. Очень вероятно, что в будущем великие шедевры будут созданы людьми и искусственным интеллектом совместно.

Литература

1. Усенко, Р. С. Нейронные сети в цифровой экономике / Р. С. Усенко // Тенденции развития Интернет и цифровой экономики: Труды V Всероссийской с международным участием научно-практической конференции, Симферополь-Алушта, 02–04 июня 2022 года. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. – С. 189-190.
2. Зубричев, Н. В. Обзор областей применения нейросетей / Н. В. Зубричев, Ф. А. Ащепков // Концепция динамического равновесия в новых технологиях : сборник статей Международной научно-практической конференции, Казань, 22 октября 2017 года. – Казань: Общество с ограниченной ответственностью "ОМЕГА САЙНС", 2017. – С. 33-36.
3. Усенко, Р. С. Применение нейронных сетей для прогнозов различных сроков / Р. С. Усенко, В. Ю. Остапенко // Тенденции развития интернет и цифровой экономики: Труды III Всероссийской с международным участием научно-практической конференции, Симферополь- Алушта, 04–06 июня 2020 года. – Симферополь- Алушта: ИП Зуева Т.В., 2020. – С. 283-284.
4. Усенко, Р. С. Подход к моделированию туристического потока с использованием нейронных сетей / Р. С. Усенко // Управление экономическими системами: электронный научный журнал. – 2019. – № 9(127). – С. 24.
5. Нейронная соната: как искусственный интеллект генерирует музыку [Электронный ресурс]. – Режим доступа: https://trends.rbc.ru/trends/industry/ 5f84b49e9a794729fefb4c88 (дата обращения: 24.01.2023).
6. Нейросеть для генерации контента онлайн [Электронный ресурс]. – Режим доступа:https://bizznes.ru/nejroset-dlya-generacii-kontenta-onlajn/ (дата обращения: 24.01.2023).
7. Нейросети и тексты: что случится с профессией копирайтера в ближайшие 5 лет [Электронный ресурс]. – Режим доступа: https://www.unisender.com/ru/blog/ kuhnya/nejroseti-i-teksty/ (дата обращения: 24.01.2023).
8. AI writes articles for website for months and 'no one noticed' [Электронный ресурс]. – Режим доступа: https://www.sott.net/article/476264-AI-writes-articles-for-website-for-months-and-no-one-noticed (дата обращения: 24.01.2023).

УДК 330

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Свиридов Андрей Николаевич
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ ВЕБ-ПРЕДСТАВИТЕЛЬСТВ

Для многих компаний последние два года были связаны с переходом на удаленную работу в облачных корпоративных системах, и командам по безопасности приложений пришлось адаптироваться к изменениям в использовании и растущему числу проблем. Согласно отчету Verizon Data Breach Investigations Report 2020 года, уязвимости веб-приложений были причиной 43% утечек данных в 2019 году. Поскольку средняя стоимость утечек данных составляет 3,86 миллиона долларов, безопасность приложений, безусловно, не является тем, что предприятия могут игнорировать. Цифры растут - за последние пять лет они выросли на 12% [3].

По сравнению с другими ИТ-ресурсами, веб-приложения особенно уязвимы для атак, потому что они доступны в Интернете. Многие векторы атак на веб-приложения сосредоточены на манипулировании пользовательскими входами через веб-формы и машинными входами через API. Уязвимости веб-приложений — это слабые места безопасности, которые позволяют субъектам угроз манипулировать исходным кодом, получать несанкционированный доступ, красть данные или иным образом вмешиваться в нормальную работу приложения.

В документе OWASP Top 10 [2] перечислены наиболее важные риски безопасности для веб-приложений. Рассмотрим несколько широко известных векторов атаки:

1. SQL Injection - происходит, когда злоумышленники используют вредоносный SQL-код для манипулирования серверными базами данных. Результат может включать в себя несанкционированный список данных, удаление (удаление) таблиц и несанкционированный административный доступ.
2. Межсайтовые сценарии (XSS) - атака, нацеленная на пользователей приложения. Его можно использовать для доступа к учетным записям пользователей, введения троянов или изменения содержимого страницы, чтобы обмануть пользователей или исключить веб-сайт. Другим, более опасным вариантом является XSS, когда вредоносный код постоянно вводится в приложение. Отраженный XSS - это когда вредоносные скрипты отражаются из приложения в браузере пользователя.
3. Удаленное включение файлов (RFI) - удаленная инъекция файлов на сервер веб-приложений. Это может привести к вредоносному выполнению сценариев и кода в приложениях, компрометации веб-сервера и краже данных.
4. Подделка межсайтовых запросов (CSRF) - атака, которая может привести к нежелательным переводам средств, изменению пароля или краже данных. Включает злоумышленника, использующего открытый сеанс пользователя, в результате чего браузер пользователя неосознанно выполняет действия на сайте, на котором пользователь вошел.

Безопасность входов и выходов приложений и внедрение безопасных методов кодирования могут защитить приложения от большинства уязвимостей. Однако этого недостаточно. Веб-приложения постоянно разрабатываются, и тестирование безопасности должно быть включено в каждый этап жизненного цикла разработки, чтобы выявить и исправить уязвимый код на раннем этапе. Кроме того, большинство веб-приложений используют сторонние компоненты с открытым исходным кодом, которые сами по себе могут быть уязвимы и должны сканироваться на постоянной основе.

Рассмотрим некоторые методы проверки [2]. SAST обычно основан на правилах, и результаты сканирования обычно включают ложные срабатывания, поэтому вам нужно будет тщательно проанализировать и отфильтровать результаты, чтобы выявить реальные проблемы безопасности.

Динамическое тестирование безопасности приложений (DAST) включает в себя тестирование развернутого или запущенного кода для поиска уязвимостей. Это может быть выполнено как вручную, так и автоматически с помощью специальных инструментов. Ручное тестирование вращается вокруг работы с API приложений с такими инструментами, как Fiddler, Postman. Инструменты автоматизации DAST отправляют большое количество запросов на код приложения, включая неожиданные и вредоносные входные данные, поиск уязвимостей. Он анализирует результаты и выявляет слабые места безопасности.

Тестирование на проникновение — это метод безопасности, который сочетает в себе динамические инструменты сканирования и опыт работы с безопасностью человека, чтобы

найти пробелы в состоянии безопасности веб-приложения. По сравнению с SAST и DAST, этот метод более сложен в использовании, но может выявить дополнительные риски, которые могут упустить автоматизированные инструменты.

Решения eXtended для обнаружения и реагирования (XDR) — это новое поколение платформ безопасности, которые предоставляют командам безопасности один интерфейс, который позволяет им обнаруживать угрозы и реагировать на них, где бы они ни находились в ИТ-среде.

XDR собирает данные о безопасности со всех уровней стека безопасности, включая веб-приложения, сети, частные и публичные облака и конечные точки. Он применяет расширенную аналитику и автоматизацию для анализа, сортировки и обнаружения как известных, так и неизвестных угроз. Самое главное, он напрямую интегрируется с инструментами безопасности и может автоматически реагировать на угрозы в режиме реального времени.

Хотя это может показаться очевидным, многие веб-приложения не реализуют основные меры контроля доступа. Необходимо убедится, что компания следует этим принципам:

1. Применение надежных паролей - использование безопасного восстановления пароля, устанавливание разумные политики истечения срока действия пароля и, предпочтительно, используйте многофакторную аутентификацию.
2. Принудительная повторная аутентификация при доступе к чувствительным возможностям или выполнении транзакций.
3. Использование принцип наименьших привилегий (POLP) и предоставление каждому пользователю только те привилегии, необходимые для выполнения своей роли в системе.
4. Использование SSL и шифрование и проверка, что пароли и учетные данные всегда зашифрованы как в состоянии покоя, так и при передаче.
5. Отслеживание учетных записей пользователей и блокирование пользователей или запрос изменение пароля при обнаружении подозрительную активность.

Согласно отчету о безопасности и анализе рисков с открытым исходным кодом за 2020 год, использование библиотек и компонентов с открытым исходным кодом почти повсеместно, при этом около 99% приложений имеют по крайней мере один компонент с открытым исходным кодом [2].

В некоторых отраслях, таких как розничная торговля, здравоохранение и образование, наблюдался экспоненциальный рост доходов в 2020 году, в основном из-за поведения потребителей и изменений в социальном взаимодействии во время COVID. Поскольку эти отрасли использовали больше открытого исходного кода в своих приложениях, у них было наибольшее количество уязвимостей и уязвимостей высокого риска. Определение того, какие компоненты с открытым исходным кодом являются безопасными, должно быть главной проблемой для любой группы безопасности приложений.

Исключениями являются часто упускаемый из виду аспект безопасности веб-приложений. Обычно встречаются исключения или ошибки, отображающие длинные трассировки стека для пользователя - эта информация чрезвычайно ценна для злоумышленников. Вы никогда не должны отображать пользователю ничего, кроме сообщения об ошибке, которое объясняет, что пошло не так и что он может сделать для ее устранения.

Приложения остаются основной причиной внешних нарушений, а распространенность открытого исходного кода, API и контейнеров только усложняет команду безопасности. К счастью, компании начали признавать важность более тесного внедрения безопасности в фазу разработки. Необходимо оставаться в курсе новых инструментов и методов для обеспечения защиты разработки веб-приложений от уязвимостей.

Литература

1. Лучанинов, Ю. TOP 11 Web Development Trends: How to Stay Ahead in 2023 [Электронный ресурс] / Mobidev, 2022. – URL: https://mobidev.biz/blog/latest-web-development-trends-new-technologies (дата обращения: 05.02.2023).
2. VERIZON. 2022 Data Breach Investigations Report [Электронный ресурс] / VERIZON, 2023. – URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 05.02.2023).
3. OWASP. Top Ten [Электронный ресурс] / OWASP, 2020. – URL: https://owasp.org/www-project-top-ten/ (дата обращения: 05.02.2023).

УДК 004.056.53

Байракова Ирина Викторовна
к.э.н., доцент кафедры экономической теории
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Родюков Дмитрий Вадимович
студент 1 курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЗАЩИТА БАНКОВ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В организации существует локальная сеть, основанная на базе Active Directory, соответственно на файловом сервере имеются данные ограниченного пользования. В этой конфигурации защита от несанкционированного доступа (НСД) будет представлять собой комплекс мер по обеспечению доступа к информации, доступной ограниченному кругу лиц, определенных политикой информационной безопасности. Один из самых простых методов разграничения доступа - файловая система NTFS операционных систем семейства Windows NT, но и такая защита может быть недостаточна, так как однофакторная аутентификация не позволяет точно определить полномочия субъекта [3]. В nix-подобных системах имеется ядро, которое можно гибко настраивать под задачи по успешному функционированию операционной системы. Следует отметить условия, которые способствуют повышению возможности НСД:

— концентрация информации разного уровня важности и конфиденциальности;
— увеличение количества информации;
— расширение круга пользователей;
— увеличение числа удаленных рабочих мест;
— автоматизация обмена информацией.
— использование сетей общего доступа;

Методы защиты от НСД банков данных (как и любые другие методы защиты) делятся на два класса: технические и организационные. Главные организационные меры защиты от НСД представлены на рис. 1.

Рисунок 1 – Основные организационные меры зашиты от НСД
Источник: составлено на основе [1].

Для защиты информации от НСД проводятся технические меры:

Технические меры защиты информации — это комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки обрабатываемой или хранящейся информации путем исключения несанкционированного доступа к ней с помощью технических средств съема [6].

К техническим средствам относят:

— инженерные сооружения: забор, замок на двери, система сигнализаций, камеры видеонаблюдения, физическая охрана и т. д.;

— аппаратные средства: устройства идентификации пользователя (сканеры отпечатков пальцев, распознавание лица и т. д.), магнитные и пластиковые карты, электронные ключи и блокираторы;

— программные средства: процедуры идентификации (логин, пароль), аутентификации (электронная подпись), шифрование данных, антивирусная защита, программы защиты от несанкционированного доступа и изменения информации и информационных ресурсов[5].

Функции обеспечивающих средств для СРД:

— распознавание и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

— регистрация действий субъекта и его процесса;

— предоставление возможностей удаления и добавления новых субъектов и объектов доступа, а также изменение полномочий субъектов;

— реакция на попытки НСД (сигнализация, блокировка), восстановление после НСД;

— проверка;

— очистка оперативной памяти (RAM) и рабочих областей на магнитных носителях после завершения работы пользователя с защищенными данными;

— учет выходных печатных и графических форм, а также твердых копий в информационных системах;

— контроль общности программной и информационной части как СРД, так и обеспечивающих ее средств [2].

Среди дополнительных средств защиты банков данных можно отнести такие, которые нельзя прямо отнести к средствам защиты, но которые прямо влияют на безопасность данных. Они состоят из таких средств[4]:

— организации совместного использования объектов банков данных в сети;

— встроенные средства контроля значений данных в соответствии с типами;

— обеспечения целостности связей таблиц;

— повышения достоверности данных, которые вводятся.

Таким образом, можно сделать вывод, что, несмотря на множество различных подходов в организации защиты данных, к ним все равно можно получить несанкционированный доступ, но чем больше подобных подходов будет предпринято, тем наиболее вероятность того, что они отпугнут злоумышленника и данные останутся нетронутыми. Защита банков данных от несанкционированного доступа – комплексная задача. Начинать ее решение необходимо с проверки текущих возможностей системы, а созданную стратегию защиты дорабатывать по мере появления новых угроз.

Литература

1.«Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 28.01.2023). » (Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 28.01.2023). — Режим доступа: для авториз. пользователей. — С. 29).

2. «Определения безопасности систем персональных данных при их обработке в информационных системах персональных данных. Руководящий документ ФСТЭК России. – М., 2010.».

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 28.01.2023). — Режим доступа: для авториз. пользователей.

4. Studfile.net: официальный сайт. – URL: https://studfile.net/preview/9461030/ (дата обращения 20.01.2023).

5. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 55 — URL: https://urait.ru/bcode/518441/p.55 (дата обращения: 30.01.2023).

6. Столяров, Н. В. Понятие, сущность, цели и значение защиты информации / Н. В. Столяров // http://sec4all.net/infoprot-gl2.html (дата обращения: 30.01.2023).

УДК 004.056.35/4-2

Бойченко Олег Валериевич
д.т.н., профессор
Вусатый Владислав Витальевич
обучающийся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Актуальность исследования. В последнее время большинство информационных систем создаётся в виде веб-приложений, так как они являются наиболее универсальными, и вместе с тем значительно упрощают взаимодействие с информацией.

Веб-приложения являются полноценной клиент-серверной программой, в которой собираются, хранятся и передаются различные данные, к примеру информация о пользователях или же о важнейших финансовых операциях компаний [3]. Поэтому, учитывая особенности функционирования веб-приложений, процесс обеспечения безопасности таких информационных систем требует большого внимания.

Методы исследования. При организации защиты веб-приложений, в первую очередь, необходимо сфокусироваться на веб-сервере, так как именно он является ядром функционирования всей информационной системы, отвечая за приём и обработку запросов. Именно веб-сервер обеспечивает основной функционал и хранит персональные данные пользователей.

Ключевым моментом ещё является то, что на защиту сервера абсолютно не влияет его географическое положение. Совершить атаку возможно практически с любой точки мира. Также, из-за своей относительной открытости, в частности, что сервера рассчитаны на передачу данных между пользователями, они имеют множество уязвимостей [2]. К примеру, у преступника может появиться возможность внести какие-либо изменения в код сервера или же базы данных и тем самым поменять первоначальное функционирование. Поэтому, защищенность серверов является одной из самых главных задач любой ИТ-компании.

Безопасное использование информации в веб-приложениях, а также хранение необходимых данных зависит от трёх ключевых элементов, а именно: конфиденциальности, целостности и доступности. Конфиденциальность заключается в том, что информация, которая предназначена непосредственно для её владельца, не должна предоставляться другим пользователям.

Целостность представляет собой обеспечение точности, а также полноты предоставляемой информации на протяжении всего жизненного цикла. Доступность же обеспечивает свободный доступ к данным для субъектов, имеющих на это право, то есть должны исправно работать системы хранения и обработки данных, интерфейсы работы с информацией и тому подобное. Стоит отметить, что именно доступность выделяют наиболее важным элементом, так как отсутствие возможности предоставления информационных услуг наносит ущерб всем субъектам информационных отношений [4, 5].

Полученные результаты. Также, для обеспечения безопасности веб-приложений требуется постоянный мониторинг действий, которые происходят на веб-ресурсе. Поэтому, одним из основных методов защиты веб-приложений является межсетевой экран. Межсетевой экран, или же, другими словами, брандмауэр, представляет собой систему, которая обеспечивает защиту между малыми компьютерными сетями и глобальным интернетом, который и является небезопасным для локальной сети [1].

Межсетевой экран обеспечивает проверку и фильтрацию данных, которые приходят из глобальной сети. Таким образом, при обнаружении потенциально опасных соединений информация просто блокируется.

Выводы. Таким образом, основными факторами распространения атак на веб-приложения можно назвать невнимательность разработчиков, а также низкий порог входа для потенциальных злоумышленников. Стоит уделять особое внимание обеспечению безопасности веб-приложений, так как любая атака может стать критичной как для отдельного пользователя, так и для всей организации в целом.

Литература

1. Володин, А. Р. Обеспечение информационной безопасности web-приложений / А. Р. Володин // Наука и образование в контексте глобальной трансформации: Сборник статей IV Международной научно-практической конференции, Петрозаводск, 19 мая 2022 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2022. – С. 138-140.
2. Кононов, Д. Н. Обеспечение безопасности web-сайтов и web-приложений / Д. Н. Кононов // Вестник по безопасности: материалы Всероссийской научно-практической конференции по безопасности,

Тольятти, 20–21 декабря 2020 года. – Тольятти: Волжский университет имени В.Н. Татищева (институт), 2020. – С. 38-43.

3. Тахиева, А. Э. Безопасность информации на web-сайтах и приложениях / А. Э. Тахиева, И. И. Ишмурадова // Качество в производственных и социально-экономических системах: сборник научных статей 10-й Международной научно-технической конференции, Курск, 15 апреля 2022 года / Юго-Западный государственный университет. – Курск: Юго-Западный государственный университет, 2022. – С. 386-390.

4. Бойченко О.В. Управление рисками кибербезопасности / Бойченко О.В. // В сборнике: Актуальные проблемы и перспективы развития экономики. Труды XXI Международной научно-практической конференции. Симферополь, 2022. С. 6-8.

5. Бойченко О.В. Модель многоступенчатой кибератаки CYBER KILL CHAIN / Бойченко О.В. // В сборнике: Дистанционные образовательные технологии. Материалы VII международной научно-практической конференции. Симферополь, 2022. С. 246-250.

УДК 332.1

Назаров Дмитрий Александрович
аспирант
Морозова Наталья Ивановна
д.э.н, профессор
Казанский кооперативный институт (филиал)
Российского университета кооперации
Россия

СТРАТЕГИЧЕСКИЙ ВЕКТОР РАЗВИТИЯ БИЗНЕСА И СОЗДАНИЯ БЛАГОПРИЯТНОЙ ПРЕДПРИНИМАТЕЛЬСКОЙ СРЕДЫ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Цифровая ИТ-революция охватила практически все мировое пространство, и нет ни одной отрасли, которой удалось бы остаться от нее в стороне. Как показывает прошлый опыт, новые технологии принесут пользу бизнесу, только если обеспечат определённые экономические выгоды и повысят производительность труда. Как и в прошлом, организациям придётся находить оптимальное соотношение автоматизации и использования ручного труда, а также совершенствовать бизнес-процессы и оценивать влияние новых технологий на сотрудников организации. Ещё предстоит узнать, как именно люди и машины будут взаимодействовать друг с другом, причём определять это придётся в каждом конкретном случае. И только правильное понимание трендов и их значения позволит как повысить устойчивость бизнес-модели, так и получить финансовую выгоду в краткосрочной и долгосрочной перспективах.

Основной целью организаций и их руководителей должно стать создание производительных, эффективных и гуманных ИИ-решений. Искусственный интеллект (далее – ИИ) и когнитивные технологии способны потенциально преобразить бизнес стратегии и процессы, а потому работать с ними нужно всем. Если конец 1990-х и начала двухтысячных стали началом эпохи интернета, то сегодня настало время внедрения ИИ на предприятиях.

Если вы или непосредственные конкуренты вашей компании ещё не внедряют когнитивные технологии, то этим займутся прорывные стартапы. Не имеющая ИИ-компетенции организация не сможет выиграть в конкурентной борьбе. Если компания упорно отказывается создать свой сайт или использует исключительно аналоговые бизнес-процессы и фиксирует все транзакции на бумаге, то жизненный цикл такой компании станет довольно коротким в эпоху повсеместной цифровизации.

ИИ обладает фантастическим потенциалом расширения человеческих способностей. Выгоды от внедрения ИИ разделяют на жесткие и мягкие. К жестким относят такие как: сокращение затрат, удовлетворенность клиентов, соответствие правилам и регламентам, снижение рисков. А мягкие: изменение бизнес-культуры, конкурентное преимущество, различные косвенные выгоды, «цифровая трансформация». Стоит задуматься о создании новых возможностей, над модернизацией системы управления после реорганизации бизнес-процессjв на основе внедрения ИИ.

Однако ИИ имеет и проблемы, которые могут сильно снизить пользу от внедрения: низкое качество данных; достоверность, недостаток прозрачности; проблемы чрезмерной зависимости от ИИ; непреднамеренной предвзятости; наивности ИИ; неправильный выбор технологии. ИИ

также может быть опасен своей утечкой данных, поэтому, при внедрении новой технологии, стоит обратить внимание на создание экосистемы ИИ и выбор правильного провайдера.

К сожалению, многие из решений ИИ, разрабатываемых в настоящее время, не являются законченными – они нацелены лишь на очень специфические функции или услуги и быстро превращаются в отдельные товары или выстраиваются в существующие корпоративные системы.

Полное признание ИИ наступит тогда, когда организации перестанут нуждаться в специальных структурах по автоматизации: ИИ станет совершенно обыденным способом ведения бизнеса и каждый будет экспертом с навыками работы в области с ИИ. А чтобы защищать свой бизнес от негативных сторон ИИ, нужно последовательно провести себя и свою компанию через три стратегические фазы: понять искусство возможного, разработать стратегию ИИ и начать внедрение необходимых технологий.

В некотором смысле подход к внедрению ИИ не отличается от подхода к внедрению технологий другого типа. Прежде всего, нужно проводить оценку целесообразности внедрения и использования искусственного интеллекта, ведь такая оценка важна при внедрении любых технологий. Таким образом, осуществив эту оценку и приступив к эксперименту накоплению опыта, организации смогут извлечь огромную пользу из самых интересных и мощных технологий, созданных человеком.

Помимо использования ИИ, многие организации сегодня пытаются провести общую цифровую трансформацию. Однако некоторые топовые организации, наиболее активны взявшиеся за цифровую трансформацию, например Nike, Procter and Gamble и Burberry, вынуждены были приостановить темп своей деятельности в данном направлении и приоритизировать процессы в очереди на цифровизацию, поскольку подобные изменения требуют огромных финансовых вложений.

Набирают популярность в последнее время облачные технологии. Эксперты, в статьях бизнес журналов ставят прогноз, на то, что вскоре каждая топ-компания будет работать в среднем с 11 облачными приложениями на базе ИИ. Как известно, облако – это виртуальный, достаточно объемный ресурс, который организации применяют для своих информационно-технологических процессов. Это, как пространство на диске, оперативная память, сетевые соединения, приложения и сервисы. Они доступны на этих виртуальных серверах, и работают они как на базе обычных. Нагрузку можно распределять между ними в любой пропорции, при чем мощность северов можно изменять. Облака могут все: можно развернуть свой веб-сайт интернет-магазина, разместить мощный 1С-сервер организации или создать удаленные рабочие места для своих сотрудников. Облако – это просто, быстро и менее затратное. Основополагающим принципом данной технологии является доступ из любой точки мира. Использование виртуализации, так как пользователям необходимы цифровые системы, которые не зависят от конкретного оборудования и позволяют начинать и заканчивать работу в любой момент. Российские организации также начали активнее переходить на подобные сервисы, особенно после принятия федерального закона №152-ФЗ «Об использовании персональных данных».

Однако на пути к совершенствованию есть преграды, так как организации до сих пор не понимают, как под все технологии можно подстроиться и найти им применение в своей деятельности. Считаем, чтобы раскрыть потенциал цифровых технологий, например, к использованию ИИ, необходимо полностью пересмотреть модель бизнеса, так как недостаточно просто автоматизировать процесс или с его помощью проводить анализ процесса. Нужно определить области бизнеса, которые выгоднее всего модернизировать с помощью искусственного интеллекта и нацелить их на полное изменение от одной и более выбранных областей. Организациям потребуется применить новые информационные технологии, изменить операционные процессы и трансформировать методы совместной работы.

Литература

1. Морозова Н.И. Инновационно-инвестиционная политика как ключевой элемент экономического роста и повышения качества жизни населения России //Бизнес. Образование. Право. 2013. № 1 (22). С. 186-190.

2. Ломакин С.И., Морозова Н.И. Формирование цивилизованного малого бизнеса как стратегическое направление обеспечения устойчивого развития государства и его субъектов //Современная экономика: проблемы и решения. 2015. № 1 (61). С. 141-148.

УДК 004:316.622

Норец Надежда Константиновна
к.э.н., ассистент кафедры бизнес-информатики
и математического моделирования
Абилова Сусанна Рифатовна
магистрант
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

«ИНТЕРНЕТ ПОВЕДЕНИЯ» (INTERNET OF BEHAVIORS) КАК НОВЫЙ ЭТАП ИНФОРМАЦИОННОЙ ЭПОХИ

Логичным продолжением эволюции интернета стало появление объединенной системы, которая трактует собранные данные с точки зрения поведенческой психологии – это и называется «интернет поведения» (Internet of Behaviors). Концепция направлена на решение вопроса о том, как правильно понимать данные и как применять это понимание для создания и продвижения новых продуктов.

Internet of Behaviors (IoB) представляет собой логичное продолжение Internet of Things (IoT). Но если интернет вещей объединяет устройства из этой категории в одну сеть, интернет поведения позволит собирать в единую базу данные о людях. Они поступают из смартфонов, «умных» часов, чипов, внешних систем наблюдения, социальных сетей и т.д. Все эти данные – «цифровая пыль», которая остается после человека, она показывает не полную картину о человеке, но определенные части жизни пользователя отражает и является весьма ценной как минимум с точки зрения маркетинга.

К примеру, «умные» весы могут давать оценку физическому состоянию человека. При установке приложения пользователь дает согласие на обработку личных данных. А производитель весов в то же время может сотрудничать с сетью тренажерных залов. «Учитывая согласие пользователя, компания может узнать, у кого из покупателей весов есть потребность в занятиях спортом, и на основе этой информации, а еще – геолокации, маркетинговый отдел запустит рекламу о скидках на персональные тренировки. Рекламное предложение получат именно те люди, которые, с точки зрения программы весов, нуждаются в спортивных занятиях» [3].

По многочисленным прогнозам, интернет поведения является одной и основных стратегических технологических тенденций, которые IT-специалисты не смогут игнорировать. Развитие технологий, которые отслеживают и анализируют поведение человека в интернете, предоставит бизнесу новые возможности, хоть и создает угрозы утечек данных. Предпринимателям станет легче набирать персонал, продвигать свои услуги, создавать новые продукты и обслуживать клиентов.

Цифровизация достаточно серьезно проникла во все сферы общественной деятельности [5, 6]. Так, например «интеллектуальная IP-телефония уже способна находить ключевые слова в разговоре. Предполагается, что можно будет анализировать интонации голоса, язык тела, чтобы считывать сигналы невербальной коммуникации, например, клиента и сотрудника при видеосвязи. Эти же технологии способны помочь контролировать атмосферу среди сотрудников в компаниях, для которых важна гигиена общения – страховые, аудиторские, юридические фирмы». [2].

«Анализ содержания рабочего дня и отслеживание состояния работника в процессе, оценка поведения сотрудников при общении с клиентами, выявление потенциальных зон роста и интересов, на основе которых можно составлять индивидуальные программы обучения» [1]. Эти и множество других перспектив привнесет интернет поведения в управление персоналом.

В сферу страхования Internet of Behaviors также привнесет положительные изменения. «Появится возможность определять цену страховки не на основании субъективных параметров типа пола, возраста и стажа, а на основе достоверных объективных данных. В свою очередь аккуратные водители, туристы и домовладельцы перестанут переплачивать, покрывая риски за менее аккуратных и ответственных» [1].

Также в качестве примера можно привести видеофиксацию нарушения скоростного режима. Обычно доступ к данным, полученным с камер видеонаблюдения, установленных на обочинах дорог, имеет полиция. Но в перспективе ими могут воспользоваться и страховые компании. «Цифровая пыль», которая показывает статистику мелких правонарушений по автомобильному номеру, поможет страховщикам оценивать благонадежность клиентов и вероятность наступления более серьезных страховых случаев.

Интернет поведения стал мощным инструментом для глобальных продаж и маркетинговых кампаний, который дал сильный толчок развитию сектора продаж. Так, организации имеют большее представление о своих пользователях и получают глубокое понимание их потребностей, обеспечивая их полное удовлетворение.

С помощью интернет поведения компании получают доступ к информации о поведении и покупательских привычках клиентов, включая:

- «путь клиентов к совершению покупки;
- определение точки, с которой начинается интерес клиента к услуге или продукту;
- стратегия, используемая для покупки продукта или услуги» [1].

Владение подобного рода данными позволит создать множество точек соприкосновения с уже имеющимися клиентами для более эффективного взаимодействия, а также поспособствует активному привлечению новых пользователей.

В большинстве своем развитие технологий постоянно ставит перед человечеством вопрос о соблюдении границ между пользой и приватностью. IoB помогает собирать, объединять и обрабатывать данные из различных источников, таких как:

- «данные о клиентах;
- данные граждан, обрабатываемые государственными органами;
- социальные сети;
- распознавание лиц в общественном достоянии;
- отслеживание местоположения» [4].

Эти действия помимо описанных преимуществ могут иметь и ряд последствий, приведенных в таблице 1.

Таблица 1 – Негативное влияние Internet of Behaviors

Что вызывает опасения?	Каковы возможные последствия?
– Сбор, хранение или распространение сенсорных данных – Подключение к Интернету – Отсутствие корректной нормативной базы – Аппаратное обеспечение – Программное обеспечение	– Вызовы глобальной и национальной безопасности – Вмешательство в данные – Пассивный сбор или обмен данными без информированного согласия – Неправильное или неожиданное использование данных – Нарушение автономии тела

Источник: составлено автором на основе [1].

Потенциальные угрозы, прежде всего связанные с безопасностью и приватностью данных, подкрепляются отсутствием должного регулирования вопроса о персональных данных со стороны государства, что в свою очередь способно привести к массовым злоупотреблениям в использовании информации.

Несмотря на то, что люди уже сегодня выкладывают информацию о себе на своих страницах в социальных сетях и дают согласие на обработку персональных данных, с повсеместным внедрением Internet of Behaviors вмешательство в жизнь будет несколько глубже, чем раньше.

С одной стороны, полученную информацию используют лишь с целью целенаправленного маркетингового продвижения, а также обеспечивая повышенный уровень безопасности на дорогах или в общественных местах. Кстати, именно поэтому сбор «цифровой пыли» достаточно часто используется на уровне государства. Так, например, в Китае используют системы распознавания лиц в местах большого скопления людей, что помогает снизить уровень преступности в стране.

Однако «далеко не все готовы принимать тот факт, что даже минимальное количество их личных данных будет доступно третьим лицам. С внедрением интернет поведения проблем не возникнет, а вот этические нормы придется обсуждать, причем на уровне законодательства» [3], обеспечивая максимальный уровень безопасности.

Таким образом, Internet of Behaviors все еще развивается, но уже отмечается его высокая полезность в будущем, при условии эффективного регулирования и правильного подхода к использованию.

Литература

1. «Интернет поведения»: что это и почему пора узнать о нём сегодня? [Электронный ресурс]. – Режим доступа: https://sbercloud.ru/ru/warp/iob. (дата обращения: 18.10.2022).

2. IoB одна из главных технологических тенденций 2021 [Электронный ресурс]. – Режим доступа: https://www.kingservers.com/blog/iov-odna-iz-ghlavnykh-tiekhnologhichieskikh-tiendientsii-2021-ghoda/. (дата обращения: 24.10.202**2**).

3. The Internet of Behavior [Электронный ресурс]. – Режим доступа: https://techvice.org/blog/popular/internet-of-behavior/. (дата обращения: 18.10.2022).

4. Апатова Н. В. Интернет и бизнес / Н. В. Апатова, О. В. Бойченко, О. Л. Королев. – Симферополь : ИП Зуева Т. В., 2022. – 190 с.
5. Бабкин А.В., Буркальцева Д.Д., Лю С. Анализ применения технологий биометрии в финансовой сфере // А.В. Бабкин, Д.Д. Буркальцева, С. Лю / Цифровые технологии в экономике и промышленности (ЭКОПРОМ-2019): сборник трудов национальной научно-практической конференции с международным участием. – 2019. – С. 512-522.
6. Как интернет поведения поможет бизнесу управлять людьми и процессами [Электронный ресурс]. – Режим доступа: https://megaplan.ru/news/business/kak-internet-povedeniya-pomozhet-biznesu/. (дата обращения: 18.10.2022).
7. Круликовский А. П. Сущность и перспективы развития Internet of behaviors в финансово-кредитной сфере / А. П. Круликовский, С. Р. Абилова // Актуальные проблемы и перспективы развития экономики: Труды Юбилейной XX Всероссийской с международным участием научно-практической конференции, Симферополь - Гурзуф, 11–13 ноября 2021 года. – Симферополь: Издательский дом КФУ, 2021. – С. 229-231.
8. Норец Н.К., Станкевич А.А. Цифровая экономика: состояние и перспективы развития // Н.К. Норец, А.А. Станкевич / Инновационные кластеры в цифровой экономике: теория и практика (ИНПРОМ-2017), г. Санкт-Петербург, 17 мая 2017 г. – С. 173-179.

УДК: 007.51

Смирнова Оксана Юрьевна
старший преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

К ВОПРОСУ О ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СРЕДЕ «ИНТЕРНЕТ ВЕЩЕЙ»

По прогнозам некоторых ученых к 2025 году количество устройств, которые интегрированы в среду «Интернет вещей» (ИВ) будет достигать одного миллиарда. ИВ прочно вошел в нашу повседневную жизнь (Умный дом, Умный город) и широко применим во многих отраслях производства и жизнедеятельности человека. В связи с чем возникает вопрос о безопасности пользователей, критически важной информации, которая перемещается между «машинами». Производители зачастую отказываются внедрять компоненты безопасности в систему ИВ, поскольку необходимо задействовать большие вычислительные затраты. К таким затратам можно отнести большой расход электроэнергии, которая критически важна для устройств, работающих от автономного источника питания.

В настоящее время на рынке услуг существует огромное количество производителей системы ИВ, которые не защищены от угрозы несанкционированного доступа, утечки информации, перемещающейся между «машинами». В научной литературе описаны некоторые группы угроз системы ИВ, рассмотрим основные из них. В первую группу необходимо отнести такой элемент безопасности, как идентификация (применение RFID датчиков и считывателей идентификации устройства и его местоположения). Применение RFID технологии удовлетворяет условию экономии электроэнергии. Ко второй группе относят агрегацию данных (сбор большого объема информации от сенсоров, исполнительных устройств и RFID датчиков; передача информации в каком-либо формате на WEB-сервис или другое устройство, которое обладает необходимой вычислительной мощностью). К третьей группе элементов безопасности относят принятие решений (выделение из общего собранного объема данных той информации, которая более информативна). На основе полученных данных при взаимодействии «машина»-«машина», принимается какое-либо решение и выполняется действие. При взаимодействии «человек»-«машина», пользователь выбирает одно из представленных действий. Такой процесс важно сделать наиболее быстрыми при выполнении действия и незамедлительно отображать результат на сенсоре или устройстве. Четвертая группа объединяет элементы в единую систему для определения следующего уровня принятия решений. На этом этапе интероперабельность, взаимодействие устройств разных производителей, протоколов передачи, хранение и обработки данных играют важную роль.

Рассмотрим безопасность в системе ИВ с позиции процессов. Все процессы безопасности в системе ИВ можно разделить на три части.

1. Службы безопасности. Службы безопасности включают: аутентификацию, управление доступом, конфиденциальность, целостность, доступность и т.д.

2. Сетевой слой. Сетевой слой состоит из сетевой модели OSI с такими компонентами: физический слой, сетевой слой, пользовательский слой, слой управления.

3. Домен безопасности. Домен безопасности состоит из четырех доменов: домен исполнительных и сенсорных устройств (несет ответственность за требования к надежности и специфику эксплуатации), домен приложений (отвечает за безопасность информации перемещающейся внутри программного обеспечения), сетевой домен (определяет условия доступа к узлам сети, маршрутизацию трафика), домен доступа (определяет правомерность доступа к системе пользователя и устройств между собой).

Другие ученые предлагают классифицировать безопасность в системе ИВ на восемь компонент, которые представлены на рисунке 1. В этой классификации каждый компонент безопасности системы ИВ сравнивается с экспертной оценкой по параметрам: целостность, подлинность, конфиденциальность, секретность, доступность, регулирование.

Рисунок 1 – Классификация по восьми компонентам безопасности в системе ИВ

Подводя итог, можно заключить следующее: сегодня не существует единственного верного подхода к формализации безопасности в системе ИВ, поскольку темпы развития системы ИВ совпадают с растущими темпами развития и видоизменения угроз ее безопасности.

УДК: 004.056

Смирнова Оксана Юрьевна
старший преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Глобальная информатизация предоставила сети Интернет общедоступность и определила новый продукт – информационный ресурс, который пришел на смену материальным ресурсам. Сегодня Интернет является вектором социального, культурного и политического развития общества. Колоссальное распространение сети Интернет спровоцировало такое же быстрое развитие информационных угроз. Поскольку для гармоничного существования любого общества необходим баланс, рассмотрим некоторые аспекты обеспечения безопасности в сети Интернет.

В настоящее время информация и информационный продукт являются стратегическим ресурсом государства. Такое положение вещей привело к возникновению информационных угроз, направленных на нарушение полноты и доступности информации, целостности, конфиденциальности и адекватности информации. Доктрина информационной безопасности обеспечивает защитой информационное право. Угроза информационной безопасности в сети Интернет – это потенциальная возможность нанесения ущерба интересам личности, социума, государства посредствам применения цифровых и информационных технологий и средств.

Рассмотрим классификацию угроз в сети Интернет, которая представлена на рисунке 1.

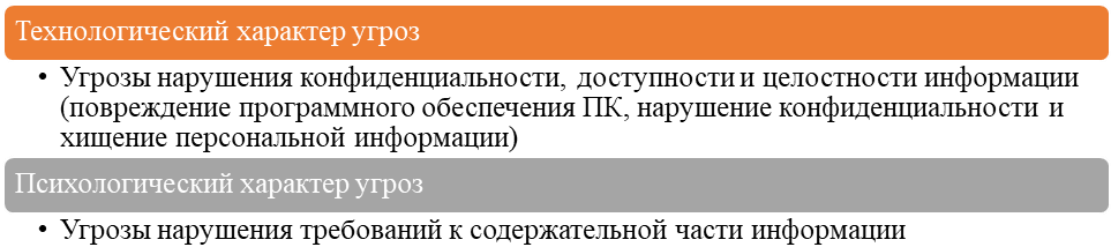

Рисунок 1 – Классификация угроз в сети Интернет

Незаконный контент в сети Интернет может нанести непоправимый ущерб личности, обществу и государству. Закон «О защите детей от информации, причиняющий вред их здоровью и развитию» способствует предотвращению распространения информационной продукции среди детей. Законодательство Российской Федерации предусматривает на законодательном уровне в нашей стране запрещение распространения:

- ✓ порнографии;
- ✓ экстремистских материалов;
- ✓ фашистской символики;
- ✓ информации, которая оскорбляет достоинство личности;
- ✓ информации с пропагандой употребления наркотических веществ.

Зачастую в сети Интернет подростки сталкиваются еще с некоторыми видами информационных угроз, которые представлены на рисунке 2.

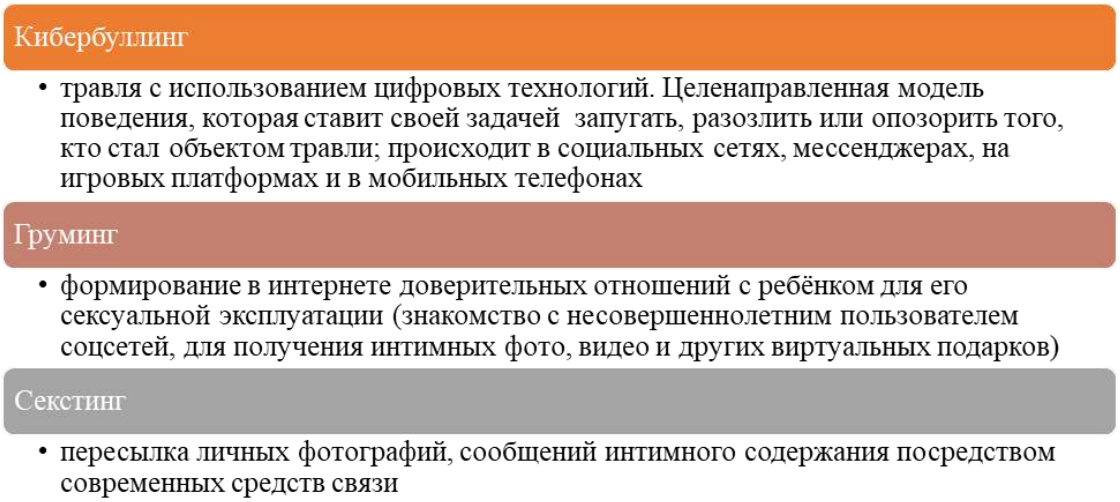

Рисунок 2 – Психологические угрозы в сети Интернет

Грамотно выстроенная психологическая атака способна нанести непоправимый ущерб, даже взрослому человеку, не говоря уже о подростке, не готового к такой агрессии в отношении себя. Такие методы психологического давления (открытые угрозы интересам личности, тому, что для нее очень важно и ценно) очень эффективны. Информационные угрозы во множестве случаев осуществляют воздействие на психику личности (общества, государства). Зачастую прямые угрозы необходимо рассматривать как показатель того, что агрессор желает договориться, так что хороший способ поведения при наличии прямой информационной угрозы – это выстроить коммуникацию с агрессором или отдельными членами кампании агрессора.

К сожалению, не всегда человек может справится с возникающими угрозами и постоянно находиться в спокойствии, контролировать ход общения и анализировать происходящее. В случаях, когда выстроенная коммуникация с агрессором не приносит желаемых результатов, необходимо прибегнуть к нормативно-правовым актам и законам о защите информации.

Солдатов Максим Александрович
к.ф.-м.н., доцент
Троценко Анастасия Юрьевна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ UX-ДИЗАЙНА ПРИ РАЗРАБОТКЕ САЙТА ДЛЯ ЭНЕРГОСНАБЖАЮЩЕЙ ОРГАНИЗАЦИИ

В Федеральном законе №250-ФЗ от 04.11.2007 в статье 1 говорится, что поставщик энергии — это предприятие или организация, которая продает электроэнергию, такую как электричество и природный газ, потребителям. Розничные поставщики энергии могут покупать энергию оптом у производителей, или они могут управлять своими собственными электростанциями, такими как ядерные генераторы или ветряные и солнечные фермы [2]. Приобретенная или произведенная мощность затем продается на открытом рынке по конкурентоспособным ценам. Розничные поставщики энергии также могут предлагать контрактные варианты и могут инвестировать в альтернативные технологии энергосбережения.

Коронавирус вызвал крупнейший глобальный кризис, вызвав волнения в экономической деятельности. Почти вся инвестиционная деятельность столкнулась с некоторыми трудностями из-за карантина, ограничений на передвижение людей или товаров, особенно в энергосбытовых организациях из-за снижения спроса и цен на энергоносители. Каждая компания справляется со своим воздействием в соответствии со своими возможностями и требованиями, обычно, приводя к сокращению спроса, финансовому стрессу и сбоям в цепочке поставок электроэнергии.

Необходимо менять ключевые бизнес-процессы и подходы к их построению в энергоснабжающих организациях. Для создания конечного продукта, который надежно отвечает потребностям пользователей, требуются соответствующие ресурсы и надлежащая продолжительность, включая этапы исследования, определения и создания идеи, прототипа и тестирования.

Энергоснабжающие организации не могут игнорировать меняющуюся анатомию бизнеса, поэтому они должны использовать возможности, предоставляемые мобильностью, для удовлетворения потребностей в услугах [1]. Для чего нужен UX-дизайн в энергоснабжающих организациях:

1. Улучшение обслуживания клиентов. Работники энергоснабжающей организации могут в любое время получать информацию о качестве поставляемой электроэнергии и жалобах, чтобы значительно улучшить обслуживание потребителей.

2. Плохой дизайн затрудняет чтение информации, а также может затруднить навигацию по сайту энергоснабжающей организации в целом. Потребители, которые заходят на сайт энергоснабжающей организации, хотят быстро находить информацию, и единственный способ сделать это - использовать простой, понятный и удобный макет. Чем быстрее потенциальный клиент сможет найти то, что ему нужно, тем быстрее он сможет превратиться в потребителя.

3. Внешний вид сайта. Современный, профессиональный веб-сайт может сэкономить клиентам. Использование цвета, различных шрифтов, различных шрифтов или других элементов для привлечения внимания потребителя. Делает его визуально привлекательным и в то же время простым в использовании.

4. Обратная связь. Необходима отдельная страница контактов с формой, которую посетители могут заполнить, чтобы связаться. Важно указать контактную информацию, адрес и номер телефона.

Для работников самой энергосбытовой организации это позволяет повысить эффективность работы, а именно [3]:

1. Отображение задач. Необходимо изучить и отобразить, как люди использовали текущий продукт. Карта для понимания порядка выполнения задач, приоритета и времени, затрачиваемого с подробным описанием того, как разные люди использовали сайт энергосбытовой организации. Это позволяет структурировать данные, улучшать процесс выставления счетов и эффективно управлять потребителями.

2. Повышение удобства использования должно рассматриваться в качестве ключевой стратегий наряду с устойчивостью при создании новых услуг на сайте энергосбытовой организации.

3. Сочетание внешнего вида, пользовательских исследований и бизнес-ценности продукта обеспечит объективные результаты при управлении ресурсами.

4. Конкурируя с сотнями компаний по всему миру, знание пользователя и простота использования продукта будут иметь реальное значение на рынке. Очень важно понимать, что дизайнеры должны делать в соответствии с потребностями пользователей.

5. Прототипы. В быстро меняющихся средах система может заставить принять дизайнерское решение за очень короткий промежуток времени. На быстро развивающемся рынке можно ожидать частых итераций.

6. Уменьшение размера изображения без ущерба для качества и проектирование каждой страницы с минимальным количеством данных могут предоставлять услуги экологически безопасным способом.

Получение энергии по справедливой цене с хорошим обслуживанием является целью для населения и юридических лиц. Потребители, которые заходят на сайт, хотят быстро получить ответы на свои вопросы, а в самой навигации помогает правильный дизайн сайта. Также необходимо сказать о том, что при грамотном построении архитектуры сайта и пути потребителя на нем, можно привести к снижению ошибок в заполнении данных, что обеспечит безопасность не только потребителей, но и их данных.

Литература

1. Осипова, Е. Какие задачи решает UX-дизайнер. [Электронный ресурс] / OrbitSoft, 2022. – URL: https://orbitsoft.com/ru/blog/ux-design/ (дата обращения: 05.02.2023).
2. ФЗ N 250-ФЗ от 04.11.2007 (ред. от 11.06.2022) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с осуществлением мер по реформированию Единой энергетической системы России» [Электронный ресурс] / КонсультантПлюс, 2022. – URL: https://www.consultant.ru/document/cons_doc_LAW_72255/3d0cac60971a511280cbba229d9b6329c07731f7/ (дата обращения: 05.02.2023).
3. Netology. Кто такой UX-дизайнер и за что ему платят. [Электронный ресурс] / Хабр, 2022. – URL: https://habr.com/ru/company/netologyru/blog/659701/ (дата обращения: 05.02.2023).

Солдатов Максим Александрович
к.ф.-м.н., доцент
Троценко Анастасия Юрьевна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОСОБЕННОСТИ РАЗРАБОТКИ ТЕХНИЧЕСКОГО ЗАДАНИЯ ПО СОЗДАНИЮ САЙТА ДЛЯ ЭНЕРГОСНАБЖАЮЩИХ ОРГАНИЗАЦИЙ

Техническое задание определяет цель и структуру проекта, комитета, встречи, переговоров или любого другого объединения людей, которые согласились работать вместе для достижения общей цели.

Техническое задание показывает, как будет определяться, развиваться и проверяться данный объект. Они также должны обеспечить документированную основу для принятия будущих решений и для подтверждения или развития общего понимания между заинтересованными сторонами. Чтобы соответствовать этим критериям, факторы успеха/риски и ограничения имеют основополагающее значение. Они определяют:

- видение, цели, масштабы и результаты (т.е. то, что должно быть достигнуто);
- заинтересованные стороны, роли и обязанности (т.е. кто примет в нем участие);
- ресурсные, финансовые планы и планы качества (т.е. как это будет достигнуто);
- структура и график разбивки работ (т.е. когда она будет достигнута).

Техническое задание на создание сайта для энергосбытовых организаций создается для того, чтобы [1]:

1. Понять, какой сайт отвечает под текущие цели энергосбытовой организации. Структура сайта будет намечена, определены основные функции и описана их работа. Также будет определен объем контента исходного ввода для тестирования сайта.
2. Установка бюджета проекта. После того, как определили тип сайта и его функциональность, рассчитывается окончательная стоимость.
3. Оценка необходимого количество времени. Как только задача будет поставлена, в техническом задании необходимо описать информацию об объеме информации и сроках, в течение которых должен быть создан сайт энергосбытовой организации. Энергосбытовая организация, со своей стороны, сможет рассчитать и установить крайний срок и дату запуска проекта.
4. Проверка проделанной работы. Когда сайт будет готов, после проведения всех тестов он может быть пересмотрен на основе технического задания. Если будут обнаружены какие-либо расхождения, компания-подрядчик, которая делала сайт, будет обязан устранить их.

Чем более подробными будут все требования и условия, описанные в техническом задании, тем лучше будет понимание того, как должен выйти сайт, и тем больше шансов, что все будут довольны результатом. Процесс написания технического задания начинается с того, что клиент предоставляет всю вводную информацию. Информация, которую получает компания-подрядчик, должна дать представление о том, какие особенности у энергосбытовой компании, какова целевая аудитория (например, ООО «СИГМА», которая занимается продажей электроэнергии, выработанной солнечными батареями, ориентирована в основном на юридические лица), какие ожидания она имеет от веб-сайта, кто ваши конкуренты и т. д. Также клиент может поделиться некоторыми примерами хороших сайтов с их точки зрения. По итогу первой встречи заполняется бриф, содержащий необходимый список вопросов, ответив на который клиент может предоставить необходимые первичные входные данные.

Бриф — это видение веб-сайта со стороны клиента, а техническое задание — это окончательный документ, который составляется на основе заполненного краткого описания с комментариями разработчиков, техническими аспектами и спецификациями. Структура является одним из наиболее важных этапов в техническом задании, так как структура является основой сайта. Именно на этом этапе решается, какие страницы и какие функции будет иметь сайт. Структура определяет, как будут связаны страницы - какая из них приведет к другой. И самое главное, это когда определяется, за какие вещи каждая страница будет отвечать и какие задачи они решат. Вот почему на этом этапе участвуют не только разработчики, но и маркетолог, SEO-специалист и руководитель отдела контента.

Самый простой способ создать структуру веб-сайта — сформировать карту в форме дерева. Это просто и понятно. В случае, если трудно продемонстрировать все ссылки или функции с древовидной формой карты сайта, создается индивидуальная карта или добавляются уточнения, также можно переходить к созданию прототипа. Прототип сайта представляет собой макет всех стандартных страниц, представленных в виде черно-белых блок-схем. Прототип позволяет четко видеть расположение всех блоков, элементов и функциональности на страницах. Прототип может отличаться по уровню детализации, разработке и интерактивности.

На этапе составления технического задания должно быть определено, кто несет ответственность за содержание. Контент играет важную роль в создании успешного веб-сайта, так как весь сайт — это просто рамка для представления контента. Уже на этапе составления технического задания определяется содержание страниц и степень его предоставления, а также учитываем задачи SEO. Если невозможно предоставить готовый текстовый материал, можно предложить энергосбытовой организации услугу по написанию всех необходимых текстов на основе интервью и анализа рынка [2].

В конечном итоге, составление технического задания для сайта энергосбытовой организации отличается спецификой рынка и продукта. Необходимо также учитывать особенность собираемых данных, так как информации о потребителях будет храниться намного больше, чем в обычном интернет-магазине - кроме личных данных, таких как ФИО, паспорт, и данные карты, также будет информация о договоре и предприятии. Таким образом, на этапе разработки технического задания необходимо учитывать требования к безопасности сайта и хранению данных пользователей.

Литература

1. Прияцелюк, Н. Разработка ТЗ: как составить качественное техническое задание дизайнеру. [Электронный ресурс] / Tproger, 2020. – URL: https://tproger.ru/experts/writing-good-technical-task/ (дата обращения: 05.02.2023).
2. IBM. Разработка технического задания [Электронный ресурс] / IBM, 2021. – URL: https://www.ibm.com/docs/ru/elm/6.0.5?topic=release-developing-vision (дата обращения: 05.02.2023).

УДК 004.056.53

Стус Елена Александровна
ассистент
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

К ВОПРОСУ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ ОТ ХАКЕРОВ С ПОМОЩЬЮ VPN

Обеспокоенность индивидуальной безопасностью растет среди пользователей сети Интернет после многочисленных утечек данных [3, 4]. Утечка данных из российских компаний за 2022 год составила более 300 миллионов записей персональных данных [4], содержащих персональные данные, такие как имя, номер телефона, адрес электронной почты, дата рождения, место жительства, серия и номер паспорта (рис. 1, рис. 2). Данные события заставляют

задуматься о том, как можно обеспечить безопасность своих данных. Возникает вопрос, может ли VPN помочь защитить данные пользователей в эпоху повышенной восприимчивости к кибервзломам.

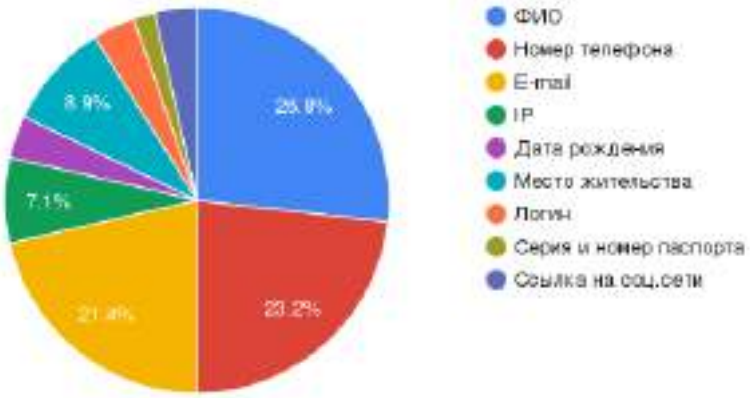

Рисунок 1 – Утекшие данные российских пользователей в 2022 году [4]

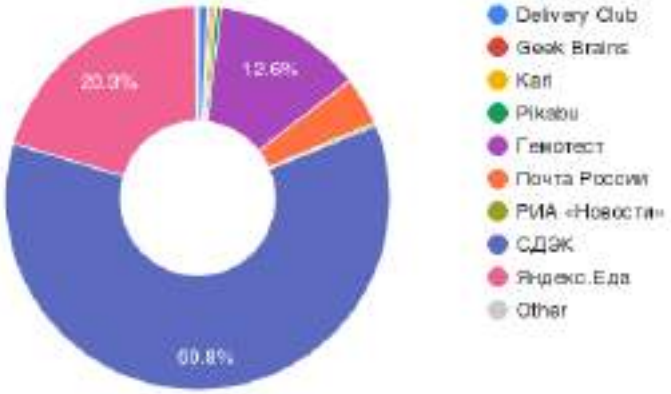

Рисунок 2 – Объем утечки данных в различных компаниях [4]

VPN – это «виртуальная частная сеть», т.е. услуга, защищающая наше подключение к Интернету и обеспечивающая конфиденциальность, а также позволяющая безопасно использовать общедоступные точки доступа wi-fi. VPN может буквально заблокировать IP-адрес от всех. Например, подключение к общедоступным wi-fi в кафе, аэропортах других общественных местах, невероятно рискованно. Достаточно одного хакера, подключенного к той же сети, который может легко следить за всеми действиями пользователя. VPN действует как плащ-невидимка, скрывая все, что человек делает на своем телефоне или компьютере. VPN может защитить пользователя от посторонних глаз, таких как Google и другие веб-сайты, которые отслеживают ваши привычки просмотра.

Как и большинство элементов большой паутины, виртуальные частные сети не все построены одинаково, и их по-прежнему можно взломать. SuperVPN считался популярным провайдером VPN, но был взломан в прошлом году, когда хакер продал базы данных учетных данных пользователей в Интернете в результате разрушительного взлома, из-за которого некоторые пользователи потеряли веру в VPN [5].

VPN защищают нашу конфиденциальность в Интернете, поэтому мы не можем стать мишенью на основе своего местоположения. Важно отметить, что мы также можем быть подвержены фишингу и заражению вредоносным ПО при наличии VPN, поэтому очень важно, чтобы наша система была обновлена со всеми обновлениями программного обеспечения и чтобы у нас было установлено надежное антивирусное программное обеспечение. Однако частым побочным эффектом использования VPN является потенциально более низкая скорость просмотра. Веб-трафик проходит больше шагов, чем обычно, при подключении через VPN, поэтому может быть некоторое замедление.

Таким образом, следует отметить, что теоретически VPN может защитить от хакеров, но данная программа не является надежной. Ни один подход не защитит пользователя сети Интернет от взлома, но VPN стоит рассмотреть, в зависимости от уже установленного программного обеспечения безопасности. VPN для смартфона особенно полезен при отправке большого количества личной информации. Лучшее, что можно сделать, чтобы защитить себя, –

сохранять бдительность и не нажимать на подозрительные ссылки или вложения от неизвестных пользователей.

Литература

1. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В. Олифер, Н. Олифер. – СПб.: Питер, 2016. – 992 с.
2. Статистика киберпреступлений 2022 [Электронный ресурс]. – Режим доступа: https://clickfraud.ru/statistika-kiberprestuplenij-2022/
3. Самые крупные взломы и утечки 2022 года [Электронный ресурс]. Режим доступа: https://habr.com/ru/post/706154/
4. Причины и следствия крупных утечек персональных данных 2022 года [Электронный ресурс]. Режим доступа: https://fbkcs.ru/utechki-dannikh-2022
5. If You Have This 'Very Dangerous' VPN On Your Phone, Delete It Now [Электронный ресурс]. Режим доступа: https://www.forbes.com/sites/zakdoffman/2021/03/01/if-this-app-is-on-your-samsung-galaxy-huawei-xiaomi-or-google-android-phone-delete-it/?sh=bd1ecda3b76b

УДК 004.056.53

Стус Мария Александровна
магистр
Научный руководитель:
Стус Елена Александровна
ассистент
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛАНДШАФТНОГО ДИЗАЙНЕРА: КАК ЗАЩИТИТЬ СЕБЯ И СВОИ АККАУНТЫ

Важной частью жизни и культуры общества является совокупность ландшафтного дизайна с удачным проектированием. В свою очередь ландшафтный дизайн является достаточно сложной услугой, которая не продается простой рекламой. Исполнитель проекта выбирается по множеству факторов, а сами клиенты приходят из самых неожиданных мест. Поэтому требуется комплексная реклама своих услуг, в особенности представление информации виртуально – в социальных сетях. Однако на этом пути ландшафтного архитектора могут подстерегать опасности, угрозы и риски в сети Интернет. По статистике [4] 95% всех киберпреступлений происходит из-за человеческой ошибки, 10% приходится на утечку данных в связи со шпионажем, а 86% из-за денежной мотивации. Следовательно, необходимо повышать осведомленность о медиасфере и знать базовые принципы медиаграмотности, чтобы не дать мошенникам «подмочить» свою репутацию и репутацию фирмы, а также сохранить бюджет.

Сейчас каждый из нас имеет большое количество аккаунтов в интернете и благодаря большому проникновению у пользователей сети накапливается «цифровое богатство», нуждающиеся в защите. Люди ежедневно оставляют цифровые следы. Под угрозой находятся аккаунты (взлом аккаунта с помощью подбора пароля, фишинга, социальной инженерии), деньги (мошенничество с помощью маскировки под рекламные и личные сообщения, выгодные предложения, сообщения, вызывающие эмоции, фишинг), ПК (заражение компьютерными вирусами), смартфоны (например, кибербуллинг).

Чтобы защитить свое устройство необходимо в первую очередь использовать только лицензионное [3], обновленное ПО, скачанное с официальных сайтов или интернет-магазинов приложений (App Store, Google Play), а также настроить разрешения для приложений, используемых для продвижения своих услуг ландшафтного архитектора, на смартфоне, использовать антивирусные программы с обновлениями, не использовать автозапуск устройств.

Мы становимся беззащитными, как только выходим в интернет, т.к не контролируем соединение. Не рекомендуется подключаться к публичному wi-fi, переходить по подозрительным ссылкам и сайтам, использовать старые версии браузеров, игнорировать предложения девайсов по созданию резервных копий. Необходимо научиться создавать надежные пароли, т.к. пароль – это самое главное на сегодняшний день в онлайне, что нас защищает. Ненадежность пароля несет в себе такие угрозы как «угон аккаунта» или шантаж, доступ к личной информации, доступ к группе или сайту, мошенничеству и краже. Не менее опасным является вход в свой аккаунт с чужих компьютеров, на которых может быть включено автоматическое сохранение паролей, сохранение файлов cookies. Следует использовать браузер в режиме инкогнито, а после использования закрыть браузер, если существует острая необходимость входа в свой аккаунт с чужого компьютера. Неправомерный доступ к чужим данным с точки зрения правового аспекта защищен законом, статьей 272 УК РФ [5]. Какой бы ни был взлом, какое бы ни было проникновение, можно по специальным логам определить, кто

подключался. Нужно стараться не выкладывать в сети Интернет свой основной адрес электронной почты, номер телефона, любые свои контактные данные во избежание спама, ненужных рассылок и утечки информации. Стоит опасаться буллинга или кибербуллинга. Бороться с агрессивным онлайн преследованием можно бороться различными способами, например, мгновенной блокировкой сообщений и жалобами в СП. Из-за невозможности сделать свой аккаунт приватным ландшафтному дизайнеру и другим активным пользователям социальных сетей нужно придерживаться подавляющему большинству правил, хотя на первый взгляд они могут показаться совершенно «безобидными» и ненужными. Следуя правилам безопасности, контролируя настройки приватности своих социальных сетей, чекины и отметки геолокаций можно значительно увеличить свою информационную безопасность.

Интернет – это безграничный мир информации, который дает широкие возможности для общения, обучения, организации работы и отдыха и в то же время представляет собой огромную, ежедневно пополняющуюся базу данных, которая содержит интересную для злоумышленников информацию о пользователях.

Литература

1. Как выяснить, не опасен ли веб-сайт [Электронный ресурс]. – Режим доступа: https://www.comss.ru/page.php?id=1709
2. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В. Олифер, Н. Олифер. – СПб.: Питер, 2016. – 992 с.
3. Стус М. А. Об опасности использования взломанных платных программ / М. А. Стус // VIII Международная научно-практическая конференция «Проблемы информационной безопасности социальноэкономических систем». – Симферополь-Гурзуф, 2022. – С.14-15.
4. Статистика киберпреступлений 2022 [Электронный ресурс]. – Режим доступа: https://clickfraud.ru/statistika-kiberprestuplenij-2022/
5. УК РФ Статья 272. Неправомерный доступ к компьютерной информации [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/

УДК 004.056

Иванов Сергей Викторович
к. ф.-м. н., доцент
Иванова Екатерина Валериевна
ассистент
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ WEB-ПРИЛОЖЕНИЙ

Вопросы безопасности WEB-приложений являются одними из самых сложных, важных и постоянно меняющих свой характер задач, стоящих перед разработчиками. В арсенале злоумышленников появляются все новые способы и возможности нанести вред работающим приложениям.

Решать такие вопросы самостоятельно – достаточно опасный подход. Гораздо разумнее воспользоваться опытом людей, сталкивающихся с подобными проблемами ежедневно и имеющих определенные наработки. В использовании сторонних библиотек и решений, безусловно, имеется один серьезный недостаток. Поскольку это решение является чаще всего открытым и используется множеством приложений, то и внимание злоумышленников оно привлекает гораздо сильнее.

Периодически появляются сообщения о том, что в какой-то библиотеке найдена уязвимость, что означает потенциальную угрозу для всех приложений ее использующих. Стоит отметить, что и решение этих проблем появляется достаточно быстро в виде выхода новой исправленной версии.

Одной из важнейших проблем безопасности является несанкционированный доступ к защищенным данным, который потенциально может привести к потере или повреждению этих данных, что может стоить миллионы и привести к различным финансовым и юридическим санкциям. Каждое приложение нуждается в надежном инструменте для управления идентификацией и доступом своих пользователей.

При поиске готового решения стоит обращать внимание на следующие функциональные возможности:

- Поддержка нескольких протоколов. К наиболее часто используемым протоколам можно отнести OpenID Connect, OAuth 2.0 и SAML 2.0.
- Поддержка SSO (Single Sign-On – система единого входа).
- Наличие графического web-интерфейса, который позволяет выполнять настройку конфигурации системы так, как это требуется.
- Возможность настройки локальной идентификации пользователя и доступов. Такая функциональность допускает создание базы данных пользователей с настраиваемыми ролями и группами.
- Работа с внешними источниками идентификации. Такая возможность позволяет синхронизироваться с уже существующими сервисами и базами данных для предоставления прав доступа.
- Возможность настройки идентификации через социальные сети. Такая функциональность очень упрощает работу для некоторых видов приложений.
- Настройка специализированных страниц для пользователей. Это не столько важная, сколько удобная возможность. В процессе работы с подобными системами часто выполняется перенаправление пользователя на специализированную страницу. Возможность настраивать такие страницы позволяет сохранить единообразие вида и дизайна приложения.

В настоящее время на рынке имеется множество решений — как бесплатных, так и платных — которые обещают предоставить такие функции. Большинство из них предоставляется достаточно широкие возможности. Рассмотрим одно из таких решений – Keycloak.

Официально это инструмент для «управления идентификацией и доступом» с открытым исходным кодом, который в настоящее время распространяется под лицензией Apache License 2.0. Немаловажным плюсом этого решения является то, что оно бесплатное. Если провести исследование доступных решений, то большинство инструментов с такими функциями, как AuthO или Okta, являются платными.

Кроме того, он поддерживает несколько различных протоколов аутентификации, что дает возможность охватывать множество приложений с различными требованиями безопасности с помощью одного инструмента. Можно выбрать протокол аутентификации в зависимости от

того, что вам нужно или что, по вашему мнению, будет лучше для вашего приложения, и вы не ограничены используемым инструментом.

Keycloak имеет большую поддержку сообщества, поэтому есть много примеров того, как что-то делать, и можно рассчитывать на помощь других в решении ваших проблем. Также он предоставляет графический веб-интерфейс, который упрощает любые изменения конфигурации. Благодаря поддержке Keycloak SSO можно упростить доступ пользователей к нескольким службам, которыми управляет ваша компания.

Выбор в сторону готового решения является более оправданным и рациональным, который сэкономит время реализации и позволит использовать опыт и наработки тех, кто сталкивается с подобными задачами безопасности. Но выбор решения все равно зависит от целей приложения и возможностей (в основном финансовых) его разработчиков.

УДК 004.056.5

Титаренко Дмитрий Викторович
к. э. н., доцент
Сеитнебиева Эльмира Февзиевна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

В современном мире, число пользователей мобильных устройств постоянно и стремительно растет, что влечет за собой бурное развитие рынка мобильных приложений. Ежедневно запускаются сотни приложений, которые зачастую запрашивают и хранят уязвимые персональные данные, такие как: номера телефонов и кредитных карт, электронную почту, данные о геолокационные пользователя, профили в социальных сетях, средства удаленного доступа и управления предприятием, фотографии, видео. Несанкционированный доступ к таким персональным данным может привести к критической ситуации.

В соответствии с классификацией открытого проекта обеспечения безопасности web-приложений OWASP (Open Web Application Security Project), к основным уязвимостям, которым подвержены мобильные устройства, относятся[2]:

1) Неправильное использование платформы. Эта категория охватывает неправомерное использование функции платформы или отказ от использования элементов управления безопасностью платформы.

2) Небезопасное хранение данных. Уязвимости небезопасного хранения данных возникают, когда группы разработчиков предполагают, что пользователи или вредоносные программы не будут иметь доступа к файловой системе мобильного устройства и последующей конфиденциальной информации в хранилищах данных на устройстве. В случае, если противник физически получает доступ к мобильному устройству, злоумышленник подключает мобильное устройство к компьютеру с и при помощи специального программного обеспечения может видеть все каталоги сторонних приложений, которые часто содержат сохраненную личную информацию.

3) Небезопасное клиент-серверное взаимодействие. Злоумышленники могут использовать уязвимости для перехвата конфиденциальных данных во время их передачи по сети.

4) Небезопасная аутентификация и авторизация. Мобильные приложения подразумевают, что пользователь может работать оффлайн, поэтому часто используется онлайн-авторизация с последующим хранением данных. После того как были введены идентификационные данные и приложение авторизовало пользователя, оно сохраняет токен, который в дальнейшем предъявляется серверу при каждом запросе, поступающему от приложения. Если злоумышленник получил идентификатор пользователя то он сможет получить доступ в систему с аккаунта пользователя. Также к данному пункту можно отнести, недостаточную сложность пароля, который может быть легко угадан или подобран методом полного перебора[1].

5) Недостаточная криптография. Существует два случая, в которых криптография системы может быть скомпрометирована для раскрытия чувствительных данных: слабый внутренний алгоритм шифрования/дешифрования; пробелы в реализации самого процесса криптографии.

6) Низкое качество кода. Обычно такие проблемы трудно обнаружить с помощью ручной проверки кода. Вместо этого злоумышленники будут использовать сторонние инструменты, которые выполняют статический анализ или фаззинг.

7) Фальсификация кода. Как правило, злоумышленник использует модификацию кода с помощью вредоносных форм приложений, размещенных в сторонних магазинах приложений. Воздействие модификации кода может быть самым разным, в зависимости от характера самой модификации, к примеру: несанкционированные новые функции; кража личных данных; мошенничество.

8) Обратный инжиниринг. Злоумышленник обычно загружает целевое приложение из магазина приложений и анализирует его в своей локальной среде, используя набор различных инструментов. Воздействие обратного инжиниринга: кража интеллектуальной собственности; репутационный ущерб; кража личных данных; компрометация серверных систем.

9) Лишняя функциональность. Злоумышленник загрузит и проверит мобильное приложение в своей локальной среде. Они изучат файлы журналов, файлы конфигурации и, возможно, сам двоичный файл, чтобы обнаружить любые скрытые переключатели или тестовый код, оставленный разработчиками. Они будут использовать эти переключатели и скрытые функции в серверной системе для проведения атаки.

Литература

1. Зубков, К. Н. Проблемы защиты информации в приложениях для мобильных систем / К. Н. Зубков, С. В. Диасамидзе // Интеллектуальные технологии на транспорте. – 2017. – № 2(10). – С. 40-46.

2. OWASP Top 10 Mobile Risks - Final List 2016. The OWASP Foundation, February, 2016.[Электронный ресурс]. URL: https://owasp.org/www-project-mobile-top-10/

УДК 330

Апатова Наталья Владимировна
д.э.н., д.п.н., профессор
Свиридов Андрей Николаевич
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

СБОР И СОХРАННОСТЬ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ НА ВЕБ-САЙТАХ

Безопасность веб-сайта требует бдительности во всех аспектах дизайна и использования веб-сайта. С большой регулярностью мы слышим о том, что веб-сайты становятся недоступными из-за атак типа "отказ в обслуживании" или отображения измененной (и часто вредной) информации на своих домашних страницах. В других громких случаях миллионы паролей, адресов электронной почты и данных кредитной карты были «слиты», подвергая пользователей веб-сайта как личному смущению, так и финансовому риску.

Целью безопасности веб-сайта является предотвращение таких (или любых) атак. Более формальное определение безопасности веб-сайта - это действие или практика защиты веб-сайтов от несанкционированного доступа, использования, изменения, уничтожения или сбоя. Эффективная безопасность веб-сайта требует усилий по дизайну всего веб-сайта: в веб-приложении, конфигурации веб-сервера, политиках создания и обновления паролей и клиентском коде. Другие атаки могут быть смягчены с помощью конфигурации веб-сервера, например, путем включения HTTPS. Наконец, есть общедоступные инструменты для сканирования уязвимостей, которые помогут узнать, совершили ли вы какие-либо очевидные ошибки.

Методы сбора данных об интернет-пользователях [2]:

1. Самый простой способ для DMP собрать необходимую информацию об аудитории клиента — это добавить теги на его же сайт. Получаемые таким образом данные — данные третьего порядка (third-party data ссылка), а теги — это сниппеты (фрагменты кода), которые вставляются в код самой веб-страницы.

2. Рекламные платформы — DMP, SSP, DSP, рекламные сети, рекламные биржи — и иные поставщики информации зачастую обмениваются между собой готовыми аудиторными сегментами, созданными с помощью файлов cookies. Они представляют собой текстовые файлы, хранящие в себе информацию о просмотренном контенте, посещенных страницах пользователем и т.п. Файлы cookies создаются браузером при каждом визите пользователя на сайт и сохраняются на его компьютере.

3.Если компания использует онлайн и оффлайн данные о своих клиентах, то можно осуществить их интеграцию с помощью первичного ввода данных.

4. DMP-платформы также могут собирать информацию с помощью веб-служб API, которые обмениваются объектами JSON с веб-сервера на сервер DMP и в обратном направлении. Таким способом может передаваться большое количество информации, но использование API требует тщательной настройки и много времени.

Веб-службы API используются для обмена данными между веб-серверами и DMP. Этот вариант обмена информацией идеально подходит компаниям, в распоряжении которых находится несколько хранилищ данных. API (Application Programming Interface — интерфейс прикладного программирования) — это способ, с помощью которого можно писать код, который взаимодействует с другим кодом. JSON (англ. JavaScript Object Notation) — текстовый формат обмена данными, основанный на JavaScript.

Почти все нарушения безопасности успешны, когда веб-приложение доверяет данным из браузера. Что бы пользователь ни делал для повышения безопасности веб-сайта, организация должна очистить все данные пользовательского происхождения, прежде чем они будут отображаться в браузере, использоваться в SQL-запросах или передаваться операционной системе или вызову файловой системы.

Самый важный урок, который необходимо извлечь о безопасности веб-сайта — это то, что нельзя никогда доверять данным из браузера. Это включает в себя, помимо прочего, данные в параметрах URL-адресов GETзапросов, POSTзапросов, HTTP-заголовков и файлов cookie, а также загруженных пользователем файлов. Всегда необходимо проверять и очищайте все входящие данные [1].

Подводя итог, можно сказать, что есть некоторые способы достижения наиболее безопасного хранения данных, например, использование более эффективное управление паролями. Поощряйте надежные пароли. Рассмотрите двухфакторную аутентификацию для вашего сайта, чтобы в дополнение к паролю пользователь должен ввести другой код аутентификации (обычно тот, который доставляется с помощью какого-либо физического

оборудования, которое будет иметь только у пользователя, например, код в SMS, отправленном на его телефон). Также можно использовать инструменты сканирования уязвимостей для выполнения автоматизированного тестирования безопасности на вашем сайте.

Хранение и отображение только тех данные, которые нужны. Например, если ваши пользователи должны хранить конфиденциальную информацию, такую как данные кредитной карты, отображайте только достаточно номера карты, чтобы она могла быть идентифицирована пользователем, и недостаточно, чтобы она могла быть скопирована злоумышленником и использована на другом сайте. Наиболее распространенным шаблоном в настоящее время является отображение только последних 4 цифр номера кредитной карты. Веб-фреймворки могут помочь смягчить многие из наиболее распространенных уязвимостей.

Литература

1. Торбенко, М. Как собирать персональные данные пользователей на сайте, не нарушая закон. [Электронный ресурс] / REG, 2020. – URL: https://www.reg.ru/blog/kak-sobirat-personalnye-dannye-polzovatelej-na-sajte-ne-narushaya-zakon/ (дата обращения: 05.02.2023).
2. MARKETING TEAM. Методы сбора данных об интернет-пользователях. [Электронный ресурс] / NT.TECHNOLOGY, 2019. – URL: https://nt.technology/ru/blog/user-data/ (дата обращения: 05.02.2023).

УДК 004.62

Гончаров Артём Максимович
обучающийся
Научный руководитель:
Гончарова О. Н.
д.п.н., профессор
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ЦЕНТРАЛИЗОВАННОЕ ХРАНЕНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ КАК СРЕДСТВО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Биометрические данные зарекомендовали себя как простой, надёжный и удобный способ аутентификации пользователя. Более того, некоторые классы биометрических данных однозначно соответствуют своему владельцу. Такими данными являются, например отпечатки пальцев. Значит, в частных случаях механизм идентификации пользователя может быть основан на биометрических данных. В случае непроизвольной коллизии данных при идентификации может быть запрошена дополнительная информация.

На сегодняшний день биометрические данные массово используются локально, в пределах одного устройства. Такой подход имеет ряд преимуществ: данные физически не покидают устройство; не передаются сторонним сервисам; функционируют в режиме API. Функционирование в режиме API позволяют приложениям, использующим данные, интегрировать биометрическую аутентификацию «одной строкой». Основным недостатком такого подхода является неполное использование возможностей, предоставляемых интеграцией биометрической идентификации-аутентификации. Зачастую биометрические данные только дублируют другие методы аутентификации для ускорения введения основных данных. Однако, государство, централизованное по своей структуре, с появлением технических возможностей организовало соответствующее централизованное хранение биометрических данных.

При вводе биометрических данных человек производит информацию как биологический генератор случайных значений. Например, рельеф отпечатка пальца будем считать неизменным, но сила нажатия на сенсор, смещение этого нажатия, распределение влаги и жира по поверхности пальца, влияющее на электропроводимость – уникальны. Модель лица в трёх измерениях в целом всегда гомогенна, но мелкие детали выражения лица невозможно воспроизвести в точности. Таким образом, существует набор способов, позволяющих получить верный, но строго уникальный экземпляр биометрических данных для последующего ввода в проверяющую модель. Теоретический подход предполагает, что считывающее устройство совершенно. На практике же возможно достижение уникальности каждого нового сканирования с большой долей вероятности только путём постепенного увеличения сложности и точности считывающего устройства до определённого предела. В этом случае кража биометрических данных в цифровом формате становится бессмысленной. Повторное введение идентичных данных можно считать недействительным. Введение идентичных данных в течение малого промежутка времени недействительно для обоих введений, так как нельзя гарантированно выделить первичное. Однако, для реализации такого механизма необходимо применение

централизованной системы, так как «центральный авторитет» должен выполнять проверку на оригинальность данных. Поддержки с серверной стороны хеш-таблицы размером в 5Мб для одного класса биометрических данных одного пользователя должно быть достаточно для эффективного выполнения такой проверки.

УДК 005.92

Деркач Ю. В.
доцент, к. пед. н.
Соколова Ж. В.
доцент, к и.н.
кафедра документоведения и архивоведения
исторический факультет
Институт «Таврическая академия»
ФГАОУ ВО «КФУ им. В И. Вернадского»
Республика Крым, Россия

ДОКУМЕНТАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Развитие электронного документооборота позволило сделать более удобной обработку персональных данных, но вероятность возникновения рисков, связанных с их утечкой или невольным раскрытием третьим лицам остается достаточно высокой.

К персональным данным относятся не только сведения в цифровой форме, но и данные на бумажных носителях, но по мнению специалистов «наибольшую озабоченность вызывает именно обработка цифровых данных, поскольку «цифра» позволяет автоматизировано обрабатывать большие массивы данных».

По данным Роскомнадзора «в России в 2022 году произошло около 150 крупных утечек персональных данных. В 16% случаев утечка произошла из-за действий мошенников, а 9% граждан пожаловались, что их персональные данные использовались в рекламных целях без согласия. В 2022 году в Роскомнадзор обратились почти 1,7 тыс. заявителей. Большая часть обращений (52%) касалась обработки личной информации без ведома и согласия человека. Многие пострадали от мошеннических действий с личными сведениями, а 10% заявивших защищали свои честь, достоинство и деловую репутацию».

Эффективная комплексная система защиты персональных данных предполагает ее соответствующее документационное сопровождение. В соответсствии с ФЗ № 152 одной из организационных мер защиты персональных данных наряду с необходимостью назначения ответственных лиц, корректировки бизнес-процессов и осуществления внутреннего контроля является разработка организационно-распорядительной документации.

Видовой состав основных рекомендуемых документов по защите персональных данных представлен в таблице 1.

Таблица 1 – Видовой состав ОРД по защите персональных данных

Документы	**Рекомендованные виды**
Положения – документы, определяющие основные требования к обработке и защите персональных данных, а также ответственность и обязанности работников и ответственных лиц в части обработки и защиты персональных данных.	Положение об обработке персональных данных Положение об обеспечении безопасности персональных данных
Регламенты – документы, устанавливающие порядок проведения мероприятий по обработке и защите персональных данных	Регламент предоставления доступа Регламент организации внутреннего аудита Регламент учета, хранения и уничтожения носителей персональных данных
Инструкции – документы, содержащие детализированные правила и указания по осуществлению определенных операций по обработке и защите персональных данных, изложенных в положениях и регламентах.	Инструкции для работника Инструкции для руководителей Инструкции техническим специалистам
Учетные документы – документы, содержащие записи о мероприятиях и результатах деятельности по обработке и защите персональных данных.	Журналы, реестры, перечни, протоколы, акты, листы ознакомления.

Индивидуальный комплект документов по защите персональных данных должен разрабатываться в зависимости от особенностей деятельности организации, но в полном соответствии с нормами действующего правового поля Российской Федерации.

Разработанный пакет организационно-распорядительных документов позволит сформировать в организации документальную основу для осуществления всех действий по обработке и защите персональных данных, а также в случае проведения инспекционных проверок может сыграть роль первоочередного документального свидетельства.

УДК 002:004.056

Ельчанинова Наталья Борисовна
к.т.н., доцент
Таловерова Дарья Вячеславовна
студент
Институт компьютерных технологий и информационной безопасности
ФГАОУ ВО «Южный федеральный университет»
г. Таганрог, Ростовская обл., Россия

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПО НОВОЙ МЕТОДИКЕ ФСТЭК

Моделирование угроз безопасности информации для объектов критической информационной инфраструктуры (КИИ) в настоящее время имеет важное значение. Летом 2017 года был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1]. По данному нормативно-правовому акту безопасность КИИ представляет собой состояние защищённости объекта, гарантирующее его нормальное функционирование в случае осуществления компьютерных атак. Основные функции данного закона: выявлять критически важные для государства объекты и обеспечивать их безопасность. По итогам проведения процедуры категорирования выделяют значимые объекты КИИ. Процесс моделирования угроз безопасности информации предоставляет возможность не только выявить такие угрозы, но и реализовать действенные меры сопротивления и, таким образом, повысить уровень защищённости объекта КИИ в соответствии с установленной категорией значимости.

Особенности процесса моделирования угроз безопасности информации для объектов КИИ имеют тесную связь с отличительными признаками новой Методики оценки угроз безопасности информации, утверждённой ФСТЭК 5 февраля 2021 г. [2]. Ключевым моментом данного документа, в отличие от действовавшего до этого, является оценка сценариев реализации угроз безопасности информации, которая прежде не проводилась. В утративших силу методических документах концепция опиралась на вероятностную математическую модель, что способствовало проведению оценки актуальности угрозы с субъективной стороны.

Согласно приказу ФСТЭК № 239 [3] при установлении требований к обеспечению безопасности объекта КИИ следует обозначить первоначальный перечень средств по обеспечению безопасности значимого объекта и приспособить комплекс средств, учитывая угрозы безопасности информации, используемые технологии и отличительные характеристики работы объекта. Также надлежит выработать восполняющие действия для обезвреживания угроз безопасности с необходимым уровнем защищённости значимого объекта и подготовить техническое задание на создание соответствующей системы безопасности. Полный анализ угроз безопасности информации происходит при подготовке организационных и технических мер, в результате чего формируется соответствующая модель угроз безопасности информации для объекта КИИ.

Моделирование угроз обязательно на этапе создания информационной системы или информационно-телекоммуникационных сетей объекта КИИ для установления необходимых критериев безопасности информации. Также моделирование требуется в процессе функционирования таких систем или сетей с целью обнаружения новых угроз, что способствует поддержанию модели угроз в актуальном состоянии и проведению своевременной модернизации защитных мер. В новом методическом документе ФСТЭК предложена иная последовательность оценки угроз безопасности информации. В этот алгоритм входят три действия, отвечающих на следующие вопросы: для чего реализуется угроза безопасности информации в отношении значимого объекта КИИ, кто осуществляет такую угрозу, и как тот или иной нарушитель может реализовать угрозу в отношении объекта, чтобы наступили конкретные негативные последствия? Все этапы моделирования угроз разработаны так, чтобы дать ответы на эти вопросы: определение того, какие негативные последствия могут наступить при осуществлении угроз безопасности информации; выделение перечня объектов воздействия, для которых наступают негативные последствия от таких угроз; выявление источников угроз и

характеристика потенциала нарушителей; оценка возможности осуществления угроз и определение их актуальности.

Одной из особенностей нового процесса моделирования угроз является этап определения возможности возникновения негативных последствий, который является началом к построению модели угроз безопасности информации. Также важно отметить, что в основе моделирования угроз находится тесная связь базы данных уязвимостей программного обеспечения и программно-аппаратных средств со списком соответствующих актуальных угроз безопасности информации [4].

К главным особенностям процесса моделирования стоит отнести тот факт, что новый метод носит универсальный характер и в равной степени успешно может быть применен к различным типам систем (ИСПДн, ГИС, объектам КИИ, АСУ ТП, киберфизическим системам) в отличие от предыдущего метода, ориентированного исключительно на информационные системы персональных данных. Отличительным моментом является возможность автоматизации процесса моделирования для упрощения работы специалиста, которому в таком случае необходимо разработать перечень всех возможных сценариев, используя для этого набор тактик и техник. Тактика – это цель злоумышленника, для достижения которой используется последовательность различных действий. Техника – это точная операция или шаг, которые могут привести к исполнению тактики.

При внимательном рассмотрении сценарного подхода видно, что угроза считается актуальной при наличии хотя бы одного варианта сценария осуществления этой угрозы. Для того чтобы определить сценарий, необходимо установить возможные тактики и техники, которые используются злоумышленниками для осуществления угрозы безопасности информации, с обозначением уровня возможностей для её реализации. При выявлении сценария угроза признаётся актуальной и входит в выстраиваемую модель угроз. Таким образом, данный подход приближает к практической безопасности объекта.

Для ключевых моментов при проведении моделирования угроз безопасности информации для объекта КИИ, ввиду особой значимости, характерна оценка угроз экспертной группой. Необходимо учитывать угрозы для инфраструктуры от поставщика услуг. Также процесс моделирования угроз должен иметь непрерывный, не дискретный характер, при этом важно учитывать сговор определённых категорий нарушителей. Помимо исключения тактик и техник ввиду их неприменимости, происходит разграничение негативных последствий относительно возможного ущерба.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства РФ. – 2017. – № 31 (ч. 1). – Ст. 4736.

2. Методический документ. Методика оценки угроз безопасности информации: утверждён ФСТЭК России 5 февраля 2021 г. // Официальный сайт ФСТЭК России. – URL: https://fstec.ru (дата обращения 02.02.2023). – Текст: электронный.

3. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения 02.02.2023). – Текст: электронный.

4. Серёдкин, С. П. Моделирование угроз безопасности информации на основе банка угроз Федеральной службы по техническому и экспортному контролю России / С. П. Серёдкин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2022. – № 1(13). – С. 43-54.

УДК 347

Калугина М. Р.
обучающаяся направления подготовки 38.03.06 Торговое дело
Норец Н. К.
к.э.н., ассистент кафедры бизнес-информатики
и математического моделирования
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ОНЛАЙН-СДЕЛКИ: ВОЗМОЖНЫЕ РИСКИ И СПОСОБЫ ИХ НИВЕЛИРОВАНИЯ

Аннотация. *В данной работе рассматриваются основные риски по совершении онлайн-сделок в Интернете. Были определены: сущность онлайн-сделок как важной составляющей системы торговых отношений; преимущества онлайн-сделок в Интернете; выделены возможные риски, связанные с совершением онлайн-сделок, и методы минимизации упомянутых рисков.*

Ключевые слова: *онлайн-сделки, риски, платежная система, безопасность, цифровая торговля, онлайн-магазины.*

Как всем известно, XXI век – это век технологий и инноваций. И в настоящее время процесс цифровизации всё глубже и глубже стал проникать во все сферы жизни общества: экономическую, социальную, политическую и даже духовную. Многие виды работ и оказания услуг, которые раньше выполнялись людьми (рабочей силой), в быстром темпе заменяются машинами и искусственным интеллектом. За последние десятки лет было создано невероятное количество технологий, помогающих оптимизировать время, затраты и усилия не только в сфере производства, но и в сфере услуг. Среди таких технологий можно выделить онлайн-сделки в Интернете. Чтобы глубже разобраться в теме научного исследования, для начала определим сущность онлайн-сделок в Интернете.

Онлайн-транзакции и онлайн-сделки стали более распространенными в эпоху цифровых технологий. С тех пор как пришла пандемия 2020 года, процесс цифровизации ускорился буквально во всех сферах, включая бизнес. В то время, когда мобильность людей становится все более и более ограниченной, онлайн-сделки становятся возможностью удовлетворить различные потребности, начиная от первичных, таких как еда, напитки и другие предметы домашнего обихода, до третичных потребностей (гаджеты, автомобили или другие хобби) [8].

Интернет-магазины сделали электронную коммерцию успешной во всем мире. Люди, которые слишком заняты, чтобы ходить на розничный рынок, всегда предпочитали онлайн-покупки просто потому, что они экономят время и предлагают широкий ассортимент товаров по очень доступным ценам. В первую очередь это связано с веб-сайтами, которые предлагают уникальный опыт покупок в Интернете, где люди могут покупать товары, не вставая с дивана. В течение многих лет Интернет с его мгновенными онлайн-покупками давал людям определенное влияние на розничных продавцов. Одним щелчком мыши клиенты могут найти более выгодные онлайн-предложения в другом месте [7].

Есть много преимуществ, которые вы можете получить, активировав услуги онлайн-транзакций для своего бизнеса, в том числе:

1. **Предоставление практичной платежной системы.**

Онлайн-сделки обеспечивают удобство как для потребителей, так и для владельцев бизнеса. Это связано с тем, что системы онлайн-платежей, например такие как BRIVA и Direct Debit, обеспечивают мгновенный процесс проверки платежа. Потребителям не нужно вручную отправлять подтверждение платежа. Так что людям не нужно записывать его вручную. Этот процесс может свести к минимуму ошибки, которые могут возникнуть из-за человеческого фактора, такие как неправильный ввод данных покупателя или потеря записей из-за поврежденных файлов.

2. **Сокращение потребности в человеческих ресурсах.**

Процессы мгновенной проверки, безусловно, уменьшат потребность в человеческих ресурсах в команде, особенно для ведения бухгалтерского учета. Таким образом, людям будет легче работать в команде. Они даже могут выделить свои ресурсы на другие нужды.

3. **Обеспечение чувства безопасности для потребителей.**

Надежная система онлайн-транзакций даст потребителям чувство безопасности, особенно при совершении платежей, поскольку у них есть юридические доказательства при совершении транзакций и онлайн-сделок и т.д. [7].

Учитывая ограничения и изменения в графиках и условиях работы, самоизоляция и последующий выход сделали онлайн-транзакции особенно актуальными. Они позволяют свести к минимуму контакт с большими группами людей. Но это также увеличивает риск мошенничества со стороны злоумышленников. Разберемся, как закрыть сделку и не потерять деньги.

- **Фейковые документы.** При продаже недвижимости мошенники могут попытаться заработать, требуя документы, которые, по их мнению, необходимы для сделки. Например, создать выписку из ЕГРН. В письме вам пришлют ссылку, подпишите договор и согласитесь оплатить аванс, как только вы получите бумагу. Извлечение или иное исполнение документа платное и возвращает фиктивный ответ или вообще никакого ответа. Покупатель перестает отвечать на сообщения.

Как избежать: заходите на сайт и получайте платную информацию по поисковым запросам, а не по ссылкам из писем. Внимательно проверяйте адрес страницы и платежные реквизиты. Сохраняйте квитанцию об оплате.

- **Сайты-клоны.** Создаются копии страниц известных компаний и их продукции. В таких ситуациях может реализоваться сразу несколько схем мошенничества, включая кражу и дальнейшее использование персональных данных, покупку контрафактных товаров, хищение средств с карт или счетов.

Как избежать: убедитесь, что именно этот ресурс принадлежит вашей компании, и обратите внимание на написание адреса сайта и платежных реквизитов.

- **Фальшивый ажиотаж.** На рекламном сайте товар указан по цене ниже рыночной. Заинтересованным покупателям предлагается внести символическую предоплату для резервирования объекта, ссылаясь на ряд заинтересованных лиц. В этом случае цели продаж может вообще не быть.

Как избежать: давление со стороны продавцов, чтобы убедить вас заплатить вперед, следует предупредить о значительном снижении цен без видимых причин. Не стоит платить за товар, который вы видели только на картинках, советуют правоохранители [6].

Таким образом, стоить помнить про следующие правила:

— прежде чем совершать покупки, обязательно проверьте данные о компании (физическом лице), предлагающем товары;

— проверьте адресную строку сайта — часто фишинговые сайты отличаются от официальных одной-двумя буквами или символами;

— проверьте отзывы об этой компании;

— не нажимайте на ссылки и не открывайте вложения, которые вы не ожидали получить или которые пришли от неизвестного отправителя.

— используйте отдельную карту для онлайн-платежей (на ней не должно быть "лишних" средств).

Литература

1. Кравец Е. О. Цифровизация экономики как фактор повышения конкурентоспособности страны / Е. О. Кравец // Инвестиционно-инновационное развитие в условиях цифровизации экономики: стратегии, факторы, механизмы : Материалы Круглого стола, Донецк, 14 апреля 2021 года / под общ. ред. С. В. Беспаловой, Н. В. Шемякиной. – Донецк: Донецкий национальный университет, 2021. – С. 114-116.
2. Круликовский А. П. Автоматизация торговли и складского учета / А. П. Круликовский, К. Г. Карапетьян // Тенденции развития Интернет и цифровой экономики: Труды V Всероссийской с международным участием научно-практической конференции, Симферополь-Алушта, 02–04 июня 2022 года. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. – С. 134-135.
3. Круликовский А. П. Автоматизация торговли и складского учета / А. П. Круликовский, К. Г. Агеева // Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической конференции, Симферополь-Гурзуф, 20–22 октября 2022 года. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. – С. 252-253.
4. Норец Н. К. Обеспечение безопасности цифровой трансформации финансовых продуктов / Н. К. Норец // Региональные аспекты экономической безопасности: II Всероссийская молодежная научно-практическая конференция с международным участием, г. Уфа, 22 октября 2021 г.– С. 13-16.
5. Норец Н. К. Риски и безопасность цифровой трансформации финансовых услуг / Н. К. Норец // Возможности и угрозы цифрового общества: ежегодная Всероссийская научно-практическая конференция, Ярославский государственный университет им. П. Г. Демидова, Ярославль, 15 апреля 2021 г. – С. 206-209.
6. Онлайн-сделки: возможные риски и как их избежать [Электронный ресурс] /. — Электрон. журн. — 2020. — Режим доступа: https://klops.ru/news/2020-06-09/215041-onlayn-sdelki-vozmozhnye-riski-i-kak-ih-izbezhat, свободный.
7. 7 Online Transactions Advantages For Business Owners [Электронный ресурс] / BRIAPI. — Электрон. журн. — 2020. — Режим доступа: https://developers.bri.co.id/en/news/7-online-transactions-advantages-business-owners, свободный.
8. Explain on Online Deal [Электронный ресурс] /. — Электрон. журн. — 2021. — Режим доступа: https://assignmentpoint.com/explain-online-deal/, свободный.

УДК 004.056

Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Байракова Ирина Викторовна
к.э.н., доцент кафедры экономической теории
Теленик Евгений Васильевич
студент 1-го курса
Институт экономики и управления
ФГАОУ ВО *«КФУ им. В.И. Вернадского»*
Республика Крым, Россия

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К законодательным документам, регулирующим отношения субъектов информационной сферы в области защиты информации можно отнести:

1) Конституцию Российской Федерации;

2) Федеральные конституционные законы;

3) Федеральные законы;

4) Законы субъектов Российской Федерации.

Законодательство Российской Федерации о защите информации состоит из Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и других правовых документов, относящихся к сфере информационной безопасности. Данный закон регламентирует вопросы защиты информации, определяет основные взгляды на защиту информации, а также основные принципы, на которых защита информации должна базироваться [2].

Законодательная база включает в себя информацию об информационных технологиях и о защите информации. Основной принцип заключается в следующем: законодательство Российской Федерации об информационных технологиях и о защите информации в обязательном порядке основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Федерального закона и других регулирующих отношений по применению информации [5].

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;
- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Требования к защите информации, которая содержится в информационной среде формируются с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения», а также ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

Защита информации есть деятельность, направленная на предотвращение:

- утечки защищаемой информации;
- несанкционированных воздействий на защищаемую информацию;
- непреднамеренных воздействий на защищаемую информацию.

Таким образом, деятельность, называемая защитой информации, включает в себя три направления:

- защиту информации от утечки;
- защиту информации от несанкционированных воздействий;
- защиту информации от непреднамеренных воздействий.

Перечисленные направлений защиты информации установлены в статье 2.3 ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».

Общая цель защиты информации – предотвращение или существенное снижение величины ущерба, наносимого субъектам информационной сферы в результате утраты общедоступной информации и (или) утраты и утечки информации общего доступа.

Для обеспечения защиты информации, содержащейся в информационной среде, применяются средства защиты информации, соответствующие требованиям, а также Федеральному закону от 27.12.2002 №184-ФЗ «О техническом регулировании» [1].

Отметим, что 5 декабря 2016 г. Указом Президента РФ утверждена Доктрина информационной безопасности Российской Федерации. Этот документ дает совершенно четкую систему взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности в Российской Федерации и в субъектах Российской Федерации.

В вышеуказанном документе под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [3].

Доктрина информационной безопасности Российской Федерации состоит из следующих пяти частей:

1. В первой части перечисляются общие положения, то есть система взглядов правительства на информационную безопасность.

2. Эти взгляды базируются на таком понятии, как национальные интересы в информационной сфере и как они описаны в во 2 части данного документа.

3. Третья часть доктрина перечисляет основные информационные угрозы и состояние информационной безопасности. То есть в этой части формулируется то, от чего требуется защищать информацию, то на пресечении каких угроз направлены меры по обеспечению информационной безопасности

4. Стратегические цели и основные направления обеспечения информационной безопасности составляют предмет четвертой части данного документа. Они перечисляются и определяют таким образом направления деятельности по информационной безопасности в Российской Федерации

5. Пятая часть перечисляет организационные основы обеспечения информационной безопасности.

Доктрина информационной безопасности также является установочным документом, на который можно ссылаться при обосновании различных проектов, обосновании актуальности различных решений, их соответствия нормативным документам, однако данный документ не является законом [4].

Таким образом, вышеперечисленные документы показывают требования законодательных государственных органов управления на регламентирование информации, информационных технологий и защиты информации.

Литература

1. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 18 — URL: https://urait.ru/bcode/512268/p.18 (дата обращения: 28.01.2023).

2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 09.01.2023)

3. Доктрина информационной безопасности Российской Федерации. (утверждена указом президента Российской Федерации от 5 декабря 2016г. № 646

4. Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань : РГРТУ, 2021. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/220418 (дата обращения: 28.01.2023). — Режим доступа: для авториз. пользователей. — С. 28..

5. Поляков, Е. А. Основы информационной безопасности : учебное пособие / Е. А. Поляков. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2021. — 71 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/282890 (дата обращения: 28.01.2023). — Режим доступа: для авториз. пользователей. — С. 12.

Солдатов Максим Александрович
к.ф.-м.н., доцент
Троценко Анастасия Юрьевна
магистрант
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПРИМЕНЕНИЕ ПРИНЦИЦИПОВ UX-ДИЗАЙНА ДЛЯ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ

UX-дизайн и кибербезопасность взаимосвязаны. Пользователи обменивают свою личную информацию на веб-сайтах и в мобильных приложениях в обмен на цифровой продукт. Они ожидают, что эта информация будет обрабатываться честно. Веб-сайт с серьезными недостатками в защите данных не сможет завоевать доверие, которое имеет решающее значение для поддержания активного взаимодействия с клиентами. Таким образом, безопасность должна быть встроена в ваш веб-дизайн. В первой половине 2020 года утечки данных выявили 36 миллиардов записей, поэтому безопасности должно быть уделено определенное внимание [2]. Одна из самых больших проблем в дизайне интерфейса - согласовать UX и безопасность.

Хороший UX-дизайн может создать бренд, в то время как неудачные стратегии защиты данных привели к краху многих организаций. Использование UX для проектирования шлюзов безопасности гарантирует, что пользователи получат опыт, который не разочарует их с точки зрения удобства или безопасности их данных. С экспоненциальным ростом числа компаний, переходящих на облачные технологии, безопасность данных сейчас важнее, чем когда-либо прежде.

Пользователь — это тот, кто находится между UX и безопасности данных. Один стремится к лучшему дизайну, другой - к безопасности. Но предприятия и их клиенты не должны быть вынуждены выбирать между превосходным пользовательским интерфейсом или безопасным. В то время как 88% пользователей с меньшей вероятностью вернутся на веб-сайт после неудачного пользовательского опыта, 75% организаций не имеют технологий или процедур безопасности для предотвращения потенциальных кибератак. Вот семь способов, которыми вы можете использовать UX-дизайн для улучшения картины безопасности данных [3].

1. Построение безопасности с помощью UX. Пользователи, как правило, активны и внимательны. Однако, даже если пользователи лениво просматривают веб-страницы, все равно есть много причин убедиться, что они предупреждены о рисках безопасности. Вы можете сделать это с помощью хорошо продуманного UX-дизайна.

Необходимо сообщить пользователям, что безопасность установлена, и напомните им, что вы используете SSL-шифрование. Это повысит доверие к продукту и услугам. Внедрите функции, которые побуждают пользователей выбирать более надежные пароли и напоминают им о необходимости предоставлять как можно меньше личной информации.

Можно сделать уведомления о безопасности интуитивно понятными и значимыми. Если меры безопасности требуют дополнительных действий, сообщить пользователям, почему. Покажите свой опыт в дизайне. Вместо длинного документа по безопасности предоставьте краткие инструкции, используя копию и графику, чтобы сделать взаимодействие приятным. Если пользователи справятся с задачей, можно использовать картинки и текст, чтобы приветствовать их приверженность безопасности и упорство.

2. Упрощение аутентификации. Вход в систему, запоминание паролей, двухэтапная аутентификация, капча и т. д. Это определенно не удобно для пользователя. Пользователи хотят минимальной суеты, а двухэтапная аутентификация отнимает много времени и откровенно раздражает. Это отличная мера кибербезопасности, но ее можно улучшить с учетом UX. Единый вход - отличный способ улучшить пользовательский интерфейс. Также можно использовать двухфакторную аутентификацию при вводе кредитной карты или финансовой информации, но для обычных входов, когда собирается минимум данных, единый вход может быть лучше. Вместо сложной и трудоемкой аутентификации разработчики UX могут использовать ссылки, отправляемые на электронные письма, используемые для входа на веб-сайт. Примером может служить одноранговая видеоконференция. После того, как ссылка на собрание будет отправлена на ваш электронный адрес, вам не нужно снова входить в систему, чтобы присоединиться. Ссылка является достаточной для аутентификации. Сложная капча может испортить ваш UX. Попытки доказать, что они не роботы, быстро начнут раздражать ваших пользователей, и они могут решить не возвращаться на вашу веб-страницу. Вместо этого можно рассмотреть другие варианты. Технология CAPTCHA развивается быстрыми темпами, и теперь существуют менее громоздкие, но не менее эффективные альтернативы.

3. Минимизация сложности. Хороший UX-дизайнер знает, что дизайн зависит от понимания пользователем и плавного прохождения. Если в какой-то момент необходимо сообщить пользователю об угрозе безопасности, лучше всего сделать это как можно более простым языком. Можно предоставить простое объяснение того, как работает мера безопасности с точки зрения непрофессионала. Необходимо подумать о том, как технические детали могут быть интерпретированы пользователем, прежде чем записывать их. Не надо использовать расплывчатые термины, которые могут заставить пользователей обходить функции безопасности, а просто скажите им, в чем проблема. Хорошо спроектированная UX-платформа, которая обеспечивает безопасность и соответствует стандарту UX, с большей вероятностью будет успешной по сравнению с плохо спроектированной. Удобный интерфейс внушает доверие и выглядит безопаснее. Четкое указание функций, которые обеспечивают защиту безопасности, а не просто их наличие, также позволит пользователям чувствовать себя безопаснее.

4. Устранение часто нарушаемые области UX для укрепления доверия. Чтобы действительно удовлетворить потребности пользователей в безопасности, дизайнеры и эксперты по безопасности данных должны работать вместе и понимать намерения, поведение и ожидания пользователей. Используя инструменты совместной работы для проектных групп, они могут ориентироваться в аспектах проектирования, предвидя связанные с этим риски. Игнорирование заинтересованных сторон удваивает риск. Конфиденциальность должна быть встроена в ваш дизайн по умолчанию.

Продукт должен быть удобным, желательным, доступным и безопасным. Необходимо протестировать его на удобство использования и безопасность. Лучшие инструменты для исследования пользователей и тестирования пользователей используют программное обеспечение для совместного использования экрана, которое фиксирует отзывы на сайте. Меры безопасности должны быть встроены в дизайн на начальном этапе и на протяжении всего жизненного цикла продукта [4].

Для достижения этих целей необходимо:

1) Убедиться, что имена пользователей не являются электронными письмами. Хакеры могут получить доступ к любой системе, использующей ту же электронную почту.
2) Убедиться, что обработка ошибок не ставит под угрозу безопасность сайта. Если пароли введены неправильно, не надо указывать адрес электронной почты, на который отправляется пароль.
3) Требование от пользователей создания надежных паролей.
4) Необходимо использовать двухфакторную аутентификацию каждый раз, когда банк участвует в финансовой транзакции. Это помогает защитить данные для входа и информацию о кредитной карте.
5) Найти альтернативы паролям для безопасной аутентификации, например, биометрической аутентификации.
6) Настроить параметры, чтобы администраторы и пользователи могли выбирать, кто может делиться контентом.
7) Ограничить доступ к данным, чтобы пользователи могли просматривать и делиться только тем, что им нужно.
8) Использовать сквозное шифрование автоматически. Примером может служить Skype, который шифрует ваши разговоры, только если вы выберете функцию «Приватный разговор».

5. Информирование пользователей о фишинговых атаках. Фишинг — это онлайн-мошенничество, при котором преступники выдают себя за законные организации с помощью электронной почты, текстовых сообщений, рекламы или других средств для кражи конфиденциальной информации. Для защиты от фишинга разработчики UX могут создавать всплывающие окна, которые предупреждают пользователей таким образом, чтобы не нарушать их работу в Интернете. Дизайнеры также могут создавать форумы по безопасности и инструменты совместной работы в команде, где пользователи могут сообщать о спаме и помогать другим пользователям. Они также могут использовать всплывающие окна или сообщения в своих приложениях для предупреждения пользователей о попытках фишинга.

6. Дизайн для прозрачности. Пользователю необходимо убедиться, что намерения компании прозрачны путем информирования пользователей о том, как используются их данные, и заранее знаете, какие действия повлекут за собой действия пользователя. Пользователи должны иметь право голоса в том, какие данные собираются, и иметь возможность давать свое согласие на каждый бит обработки данных. Они также должны иметь право отозвать это согласие, когда им этого захочется. Дизайнеры должны убедиться, что пользователи также знают о третьих сторонах, которые могут использовать их данные.

Необходимо избегать хранения конфиденциальной информации, чтобы активно защищать свои данные от взломов. Всегда спрашивать разрешения, прежде чем хранить это. Отличный UX-дизайн предполагает хорошо структурированную и легко усваиваемую политику конфиденциальности, которая сообщает пользователям все, что им нужно знать об их данных и их использовании.

7. Сбор допустимо минимального количества данных и файлов cookie. Необходимо свести к минимуму собираемые персональные данные и работать над их сохранением. Кроме того, необходимо убедиться, что отслеживается тот факт, какие данные собирают третьи стороны, и, если возможно, анонимизировать личные данные.

Дизайнеры должны убедиться, что закрыть учетную запись легко. Удобство является ключевым, даже если клиент уходит. Хотя считается, что сбор как можно большего количества данных создает более персонализированный интерфейс, в компромиссе между большим количеством информации и проблемами безопасности, необходимо отдавать предпочтение последним.

Пользовательский дизайн обращает внимание на то, как собираются данные и как формулируются вопросы. Уведомления, формы и запросы разрешений отправляются пользователю только тогда, когда вы уверены, что клиент их примет.

Также играет тот факт, что больше шансов, что форма будет заполнена, если в ней меньше полей. Например, Imagescape сократила свою контактную форму с 11 до четырех полей и увеличила конверсию на 120% [1]. Или, например, для веб-сайта для бронирования встреч бесполезно указывать поля в форме бронирования, запрашивающие адрес пользователя. Для завершения транзакции вам нужно только их имя и кредитную карту.

Из множества способов улучшить пользовательский интерфейс, сокращение количества файлов cookie является отличным. Кроме того, необходимо убедиться, что баннер с файлами cookie не бросается в глаза и не мешает работе пользователя. Хороший UX может изменить судьбу компании, но продукт, в котором легко ориентироваться и которым приятно пользоваться, не должен идти на компромисс с безопасностью. Без этого пользователи уязвимы.

К счастью, UX и безопасность могут работать рука об руку. Можно создать продукт, который будет одновременно удобным и высокозащищенным. Вам не нужно решать, что важнее — повышение безопасности или улучшение взаимодействия. Безопасность продукта не противоречит дизайну. Последний фактически может быть использован для повышения безопасности в Интернете.

Литература

1. Bufe, Annemarie. 20+ Powerful UX Statistics To Impress Stakeholders 2022. [Электронный ресурс] / Uxcam, 2022. – URL: https://uxcam.com/blog/ux-statistics/ (дата обращения: 05.02.2023).
2. Lawrence, Cate. How to Bring UX Designers and Developers Together. [Электронный ресурс] / Codemotion, 2020. – URL: https://www.codemotion.com/magazine/frontend/design-ux/ux-designers-developers-together/?_ga=2.208666066.1596962621.1675533920-1572303993.1675533920 (дата обращения: 05.02.2023).
3. Shah, Rushit. Why Has Web App Security Become a Major Concern in Recent Times? [Электронный ресурс] / Codemotion, 2021. – URL: https://www.codemotion.com/magazine/backend/cybersecurity/web-app-security-tools/?_ga=2.208666066.1596962621.1675533920-1572303993.1675533920 (дата обращения: 05.02.2023).
4. Conn, Richard. How to optimize web-design to convert better than competitors [Электронный ресурс] / JEG DESIGN, 2020. – URL: https://www.jegdesign.com/design-chat/how-to-optimize-web-design-to-convert-better-than-competitors/ (дата обращения: 05.02.2023).

УДК 340: 004.056.5

Тутова Ольга Васильевна
к.педагог.н., доцент
старший преподаватель кафедры гуманитарных
и социально-экономических дисциплин
Черкасова Надежда Сергеевна
слушатель 6 курса
Крымский филиал Краснодарского университета МВД России
Республика Крым, Россия

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И НЕКОТОРЫЕ АСПЕКТЫ ЕГО ЗАЩИТЫ

Активное внедрение информационно-коммуникационных технологий (ИКТ) во все сферы жизни человека, в частности, внедрение искусственного интеллекта, технологий биометрической идентификации, обработка больших объемов информационных данных, широкое распространение удаленных систем обслуживания банковской сферы, облачное хранение данных открывают новые возможности для совершения преступлений в сфере экономики, против общественного порядка и общественной безопасности.

Цифровизация коснулась и следственной деятельности органов внутренних дел. В современных условиях информационное обеспечение следственной деятельности осуществляется на основе использования ИКТ с применением возможностей телекоммуникационных сетей, а также сети Интернет.

Согласно Федеральному закону от 7 февраля 2011 г. № 3-ФЗ «О полиции» (ст. 11, гл. 1) полиция обязуется использовать достижения науки и техники в своей деятельности, новейшие технологии и информационные системы, а также телекоммуникационные сети и актуальную информационно-коммуникационную инфраструктуру (ст. 1, 12, гл. 1) [1].

Полиция использует аудио-, фото- и видеофиксацию для документирования обстоятельств совершения преступлений. Эти же методы применяются для фиксирования действий сотрудников полиции при исполнении ими своих обязанностей (п. 3 ст. 12 гл. 1). Кроме того, полицейский имеет право использовать в своей работе сеть Интернет, автоматизированные информационные системы, интегрированные банки данных (п. 4 ст. 12. гл. 1) [1].

Проанализировав определения авторов [2, 3], можно отметить основные характеристики информационного обеспечения следственной деятельности, в частности:

- аккумулятивную, так как информационное обеспечение деятельности следователя является единой системой, которая аккумулирует информационные данные из внутренних и внешних источников, информации, которая возникает в ходе расследования преступлений;
- деятельностную, так как следователь осуществляет определенную деятельность по разработке, организации, совершенствованию и обслуживанию информационных систем;
- информационную, в связи с тем, что работа с информационным обеспечением следственной деятельности направлена на обеспечение сотрудников конкретными

информационными данными, которые позволяют выполнять возложенные на следователя задания и функции.

Информационное обеспечение следственной деятельности позволяет решить многие проблемы, возникающие в работе следователя. Сотрудник может осуществить тщательный отбор тех информационных данных, которые позволят ему проанализировать информацию в рамках конкретного расследуемого дела, произвести конкретные процедуры, используя стандартные методы, а также привлекая соответствующих специалистов. Кроме того, информационное обеспечение может помочь следователю с определением сроков и порядка получения информации, ее фиксации, обработки, а также систематизации полученных информационных данных. Помимо этого, информационное обеспечение следственной деятельности позволяет эффективно организовать использование результатов анализа данных в практической деятельности органов предварительного следствия [4].

Таким образом, информация, которую получает следователь - это данные о лицах, фактах, предметах, событиях и процессах, предоставляемые в соответствии с действующим законодательством, специально зафиксированные материально и систематизированные [3].

Информационные потребности следственной деятельности обеспечиваются криминалистическими, оперативно-розыскными и оперативно-справочными учетами, которые можно обобщить, назвав «криминальными учетами». Учеты - это сформированные в определенном виде наборы информационных данных о лицах, событиях, фактах, предметах по их признакам, которые предопределяют эффективное информационное обеспечение деятельности следователя.

Составными элементами криминальных учетов выступают различные автоматизированные информационные системы и банки данных.

В настоящее время МВД России использует в своей деятельности большое количество автоматизированных информационных систем, которые, в основном, входят в состав ИСОД МВД России (Единую систему информационно-аналитического обеспечения деятельности МВД России) и обслуживают различные направления деятельности МВД. Сюда относятся автоматизированные информационные системы, обеспечивающие деятельность следователей, сотрудников оперативно-розыскных подразделений, кроме того, данные системы позволяют получить информацию правового характера, справочную и статистическую информацию и т.д.

Защита информации от негативного воздействия и несанкционированного доступа правонарушителей обеспечивается использованием различных методов, которые постоянно модернизируются и видоизменяются. К ним относят дробление информации, ее учёт, шифрование, кодирование, ранжирование скрываемых информационных данных, дезинформация, сокрытие, а также морально-нравственные и иные меры [5].

Важным элементом контроля обеспечения защиты информационных данных является учет и регистрация электронных носителей и бумажных источников с защищаемой информацией. Выделяют несколько принципов использования учётов для обеспечения сохранности информационных данных в следственных подразделениях органов внутренних дел:

- обязанность уполномоченных лиц регистрировать все носители информации и не допускать её копирование на незащищенные источники;
- запрет повторной регистрации нескольких носителей по одному номеру, то есть запрет их дублирования;
- контроль за местонахождением каждого носителя информации, предотвращение их утери, принятие мер по поиску утерянных носителей и по устранению угроз, возникших в результате их утери;
- личная ответственность каждого сотрудника за утрату или копирование вверенной ему защищаемой информации.

Для обеспечения защиты информации в ИСОД МВД России создана подсистема обеспечения информационной безопасности, которая включает в себя средства защиты инфраструктуры, средства защиты сервисов и средства защиты автоматизированных рабочих мест.

Защита информации в ИСОД МВД России осуществляется благодаря защите от несанкционированного доступа, антивирусным механизмы защиты, криптографической защите и механизмам защиты межсетевого взаимодействия.

Защита информации от несанкционированного доступа реализуется за счет идентификации и аутентификации при попытках осуществления доступа в ИСОД МВД России, разграничения доступа к ресурсам и сервисам, а также протоколирования событий безопасности. Кроме того, осуществление защиты информационных данных от несанкционированного доступа обеспечивается за счет контроля целостности программных средств и информационных ресурсов.

Механизм антивирусной защиты предполагает установку антивирусной программы Kaspersky Anti-Virus, ее регулярное автоматическое обновление, а также централизованное управление антивирусной политикой и контроля за параметрами антивирусного программного средства на рабочих местах сотрудников.

Криптографическая защита информационных данных в ИСОД МВД России осуществляется за счет шифрования информационных данных, использования сотрудниками правоохранительных органов электронной подписи и контроля целостности защищаемой информации средствами криптографической защиты.

Защита межсетевого взаимодействия осуществляется обязательной установкой на служебные компьютеры межсетевых экранов, регулярным и тщательным анализом сетевого трафика на обнаружение атак и реализацией постоянной фильтрации сетевого трафика.

Однако сфера защиты информации в ИСОД МВД России имеет свои недочеты. В частности, как отмечают А.В. Шапкин и И.А. Кубасов в [6], в части сервисов Единой системы информационно-аналитического обеспечения деятельности МВД России используются разнообразные технологические решения, которые чаще всего являются слишком сложными и достаточно дорогими как в процессе разработки, так и в дальнейшем их обслуживании. Кроме того, авторы считают, что до сих пор не настроена надлежащим образом функциональность некоторых платформ (например, аналитической, биометрической, геоинформационной и внешнего взаимодействия). Эти платформы могли бы обеспечить возможность проводить оперативный комплексный анализ накопленной защищаемой информации различных типов.

Тем не менее, единая технологическая платформа, на которой осуществляется функционирование информационных систем МВД России, ее текущее реформирование дают основания надеяться на последующее решение указанных проблем.

Таким образом, одним из основных пунктов обеспечения информационной безопасности следственной деятельности является систематическая защита информационных данных от несанкционированного доступа, а также от негативного воздействия. Кроме того, мы считаем, что регулярное повышение квалификации сотрудников органов внутренних дел в вопросах защиты служебной информации и персональных данных позволит частично решить проблему защиты информации, циркулирующей в информационном обеспечении следственной деятельности.

Литература

1. Федеральный закон «О полиции» от 07.02.2011 № 3-ФЗ. // Гарант: комп. справ. правовая система [Электронный ресурс]. – http://www.garant.ru.

2. Муленков Д.В., Горшков М.М. Использование учетных информационных данных в работе полиции, исходя из типовых следственных ситуаций // Вестник Уральского юридического института МВД России. 2018. № 3. С. 17.

3. Долгинов С.Д. Информационное обеспечение следственной деятельности: возможности и реальность // Труды Академии МВД Республики Таджикистан. 2018. № 2 (38). С. 58.

4. Цимбал В.Н. Технологическое обеспечение процесса внеэкспертного использования специальных криминалистических знаний в ходе предварительного расследования / А.В. Гусев, В.Н. Цимбал // Общество и право. - 2018. - № 1 (63). - С. 69-73.

5. Клименко И.С. Информационная безопасность и защита информации. Модели и методы управления / И.С. Клименко. – М: ИНФРА-М, 2020. – 180 с.

6. Шапкин А.В., Кубасов И.А. Основные направления дальнейшего развития ИСОД МВД России на период с 2020 по 2024 годы // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: Сб. статей Междунар. научно-практ. конф. - М., 2019. - С. 256.

УДК 332.143

Чепорова Галина Евгеньевна
к.п.н., доцент
Институт педагогического образования и менеджмента
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

БАЛАНС МЕЖДУ РАСКРЫТИЕМ ИНФОРМАЦИИ И ЗАЩИТОЙ КОНФИДЕНЦИАЛЬНОСТИ В УСЛОВИЯХ ПАНДЕМИИ

Право на доступ к информации, находящейся в распоряжении органов государственной власти или право на информацию признано международным правом в качестве основного права человека. Доступ к информации важен сам по себе и как средство защиты других прав, включая принципы демократии и поддержку устойчивого развития. Его важность была признана в качестве целей в области устойчивого развития, которая призывает государства «обеспечить доступ общественности к информации». ЮНЕСКО является уполномоченным агентством ООН

по мониторингу и отчетности для этой цели в отношении гарантий и реализации права на информацию во всем мире.

Пандемия COVID-19 подчеркнула повышенную важность информации во времена кризиса. Доступ к точной и своевременной информации помогает людям делать безопасный выбор для себя и своих семей, при этом правительства обязаны широко распространять информацию, представляющую общественный интерес, и бороться с дезинформацией. Доступ к информации также способствует подотчетности в отношении важных решений, принимаемых правительствами во время чрезвычайных ситуаций. В то же время пандемия нарушила обычные административные процедуры, в том числе связанные с информацией, такие как обработка запросов на информацию или обеспечение регистрации соответствующей информации.

Право на информацию признается в качестве основного права в соответствии с международным правом, право «распространять», а также «искать» и «получать» информацию и идеи. Это право налагает на государства позитивное обязательство признавать это право и разрабатывать удобные для пользователя системы, обеспечивающие практический доступ к информации, как путем ответа на запросы о предоставлении информации, так и путем упреждающего раскрытия информации. С 1990-х годов произошло резкое увеличение числа государств, принявших законы о праве на информацию для институционализации этих систем.

Государствам следует создать удобные для пользователя системы предоставления информации. С этой целью в законах о праве на информацию должны излагаться такие детали, как порядок подачи запроса, сроки предоставления ответов, а также взимаемые сборы за информацию. В то время как реагирование на запросы информации остается ключевым для реализации права, особое внимание можно уделить роли упреждающего раскрытия информации в текущий исторический момент. Чем эффективнее раскрытие информации, тем меньше общественности приходится прибегать к запросам. И чем официальнее раскрытие информации, тем меньше места остается для дезинформации и слухов. Однако, право на информацию не является абсолютным правом. В доступе к определенной информации, такой как частная информация о третьих сторонах или конфиденциальная информация о национальной безопасности, может быть отказано. В соответствии с международным правом ограничения права на информацию должны быть оправданы одним из двух способов. Во-первых, допускаются ограничения этих прав как в обычное время, так и в чрезвычайных ситуациях в соответствии со строгим трехэтапным тестом: предусмотрено законом; защищает законный интерес и является необходимым для этой защиты (Комитет ООН по правам человека). Во-вторых, особые отступления от этих прав могут быть разрешены во время чрезвычайной ситуации.

Одним из интересов, который может противоречить праву на информацию во время чрезвычайной ситуации в области здравоохранения, является право на неприкосновенность частной жизни, которое также защищается как право человека в соответствии с международным правом. Право на информацию поддерживает неприкосновенность частной жизни, предоставляя людям доступ к информации о себе, хранящейся у правительства, в то время как неприкосновенность частной жизни также общепризнано как исключение из права на информацию. Интересы конфиденциальности особенно высоки в отношении медицинской информации, которая представляет собой «один из основных элементов частной жизни человека и человеческого достоинства»

В результате, как правило, медицинские данные должны публиковаться только после того, как они будут анонимизированы, чтобы нельзя было установить личность отдельных лиц, даже если эти данные объединены с другими наборами данных. Это остается верным во время чрезвычайной ситуации в области общественного здравоохранения, несмотря на высокий общественный интерес к быстрому доступу к медицинской информации. Согласно международному праву, любой конфликт между правом на информацию и неприкосновенностью частной жизни должен разрешаться с учетом того, что лучше всего отвечает общим общественным интересам. В связи с этим может потребоваться раскрытие определенной частной информацию для защиты более широкого общественного блага.

Упреждающее раскрытие информации является важно функцией государств во время пандемии. Государства использовали широкий спектр стратегий для передачи информации о пандемии COVID-19. Многие страны создали доступные центральные веб-сайты для обмена ключевой информацией о пандемии, такой как количество случаев, смертей, тестов и выздоровлений. Это обеспечивало согласованный обмен сообщениями, а также регулярное расположение и формат для публичного доступа к информации. Важным было дезагрегация этих данных, в том числе по полу и возрасту.

С другой стороны, в ряде стран возникли проблемы с достоверностью, точностью и полнотой информации о пандемии. Например, специальный механизм мониторинга

Межамериканской комиссии по правам человека для Никарагуа обнаружил, что данные, предоставленные о случаях, смертях и выздоровлениях

С другой стороны, в ряде стран возникли проблемы с достоверностью, точностью и полнотой информации о пандемии. Например, мониторинг Межамериканской комиссии по правам человека для Никарагуа обнаружил, что данные, предоставленные о случаях, смертях и выздоровлениях была ненадежными, и что информация о данных тестирования, распространении болезни и протоколах мониторинга случаев не была доступна. Некоторые страны стремились централизовать официальные сообщения о пандемии, запретив другим официальным лицам говорить о ней. Важно следить за тем, чтобы официальная информация была максимально точной и актуальной, но чрезмерная централизация препятствует потоку информации и дает возможности для политического контроля. Так, Сербия приняла указ, требующий централизованного обнародования всей информации, связанной с COVID-19, что не позволило местным кризисным штабам напрямую общаться с местными сообществами, в которых они работали. Постановление было отменено всего через несколько дней после общественного протеста. Как в Зимбабве, так и в Бразилии юридические проблемы, инициированные гражданским обществом, успешно заставили правительство улучшить свою работу. Подобные проблемы возникали в Черногории, Индонезии, Перу, Индии и других странах.

Таким образом, баланс между упреждающим раскрытием информации и защитой конфиденциальности иногда представлял собой определенную проблему. В большинстве случаев надлежащий баланс может быть достигнут путем публикации информации в достаточно агрегированных формах, чтобы было невозможно выделить конкретных лиц, но достаточным для понимания общей картины.

УДК 004.056.33

Бойченко Олег Валериевич
д.т.н., профессор
Белей Алла Петровна
обучающаяся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КИБЕРБЕЗОПАСНОСТЬ ДЛЯ САЙТОВ СОЦИАЛЬНЫХ СЕТЕЙ

Актуальность исследования. В современной социально-экономической среде одной из наиболее быстро развивающихся областей развития технической инфраструктуры является Интернет. Участившиеся за последнее десятилетие кибер-атаки представляют серьезную угрозу для цифрового мира, что определяет актуальность изучения проблем кибербезопасности для сайтов социальных сетей (SNS), поскольку распространение социальных сетей среди частных лиц и предприятий стремительно растет. Сайты социальных сетей имеют множество сфер применения, таких как цифровой маркетинг, социальная электронная коммерция и брендинг. Тот факт, что максимальное количество пользователей не знают о рисках, а их незнание приводит к дальнейшему росту киберпреступлений, является серьезной проблемой. Все эти вопросы станут частью данной работы. Отдельно следует также отметить проблемы и вызовы безопасности SNS, такие как неправомерное использование личных данных, вредоносные программы, фишинговые атаки и угрозы со стороны сторонних приложений [1].

Цель работы состоит в исследовании проблем, связанных с обеспечением кибербезопасности цифровых технологий в Российской Федерации для создания условий реализации решений, которые могут быть приняты как отдельными пользователями, так и правительством в сотрудничестве с частным сектором для создания кибербезопасного цифрового мира.

Методы исследования. В сегодняшнюю эпоху смартфонов и компьютеров Интернет изменил представление о коммуникации. Из-за отсутствия безопасности в последнее десятилетие появились различные киберпреступления. Кибербезопасность играет важную роль в современном развитии информационных технологий и услуг. Таким образом, кибербезопасность — это попытка пользователей сохранить свою личную и профессиональную информацию в целости и сохранности от атак в Интернете. Основной функцией кибербезопасности является защита сетей, компьютеров, программ от несанкционированного доступа и потери. Максимальное количество пользователей не знают о рисках и делятся своей информацией неосознанно, а отсутствие знаний делает их уязвимыми для кибер-атак. Поэтому кибербезопасность является главной проблемой в современном мире компьютерных технологий [2].

Основной целью сайтов социальных сетей является объединение людей и организаций. Они также открывают множество возможностей для бизнеса компаний и фирм. Социальные сети внесли значительные изменения в способ общения людей. Сайты социальных сетей вызывают особую озабоченность, связанную с конфиденциальностью и безопасностью пользователей. Безопасность и конфиденциальность этих сайтов в основном сосредоточена на обнаружении вредоносных программ, поскольку кажется, что сообщение исходит от доверенного лица, пользователи с большей вероятностью нажмут на ссылку. Сайты социальных сетей нашли применение во многих областях, таких как социальная электронная коммерция: Сайты социальных сетей могут использоваться для промо-акций и рекламы для владельцев порталов электронной коммерции. Брендинг: Социальные сети предоставляют компаниям лучшую платформу для привлечения клиентов для расширения возможностей бизнеса [3].

Поскольку рост социальных сетей принес различные преимущества, он также принес различные проблемы безопасности. Они также предоставляют уязвимую платформу для злоумышленников, формируя некоторые проблемы, связанные с этим. Например, использование личности не по назначению, когда злоумышленник выдает себя за личность любого пользователя, что приводит к злоупотреблению идентификацией [4]. Кроме того, злоумышленники атакуют через приложения, в которых они запрашивают разрешение на доступ к информации, предоставленной на сайтах социальных сетей. Когда пользователь разрешает это сделать, он получает доступ ко всей информации, и эта информация может быть использована не по назначению без ведома пользователя.

Результаты исследования. С ростом популярности сайтов социальных сетей они стали главной мишенью для киберпреступлений и атак. Киберпреступность становится широко распространенной и представляет собой серьезную угрозу национальной и экономической безопасности. Под угрозой находятся как государственные, так и частные учреждения в таких секторах, как здравоохранение, информация и телекоммуникации, оборона, банковское дело и

финансы. Поэтому организации должны принимать надлежащие меры безопасности, чтобы обезопасить себя от киберпреступлений, а пользователи должны защищать свою личную информацию, чтобы избежать кражи персональных данных или злоупотреблений.

Выводы. Киберпространство становится важной областью для киберпреступлений и атак террористов на важную информацию. Поэтому необходимо всеобщее сотрудничество стран для совместной работы по снижению постоянно растущей киберугрозы.

Литература

1. Rituparna D., Mayank P. Cyber Security for Social Networking Sites: Issues, Challenges and Solutions/ International Journal for Research in Applied Science & Engineering Technology (IJRASET). 5 Issue IV, April 2017// [Электронный ресурс]. – Режим доступа: www.ijraset.com. (дата обращения: 20.01.2023).

2. Sukhov M. I., Gnedina O. A. Metody zashchity informatsii v sotsial'nykh setyakh [Methods of protecting information on social networks]. Molodoy issledovatel' Dona - Young researcher Don, 2017, no. 2 (5), pp. 32-35.

3. Киберпреступность и киберконфликты: Россия [Электронный ресурс] // - Российский интернет-портал и аналитическое агентство Tadviser по теме корпоративной информатизации - Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения: 20.01.2023).

4. Kovtun D. Assessment of Congruence of Unstructured Data Using Text Mining Technology // Proceedings – 2021 IEEE 23rd Conference on Business Informatics, CBI 2021 – Main Papers: 23 (Virtual, Online, 2021, Sept. 1–3). P. 163−166. DOI: 10.1109/CBI52690.2021.10067.

УДК 004.056.33.21

Бойченко Олег Валериевич
д.т.н., профессор
Собаленко Милена Сергеевна
обучающаяся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КИБЕРБЕЗОПАСНОСТЬ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Актуальность исследования. Кибербезопасность – состояние защищенности инфокоммуникационной системы и содержащейся в ней информации от внешних и внутренних угроз. Состояние защищенности нарушается посредством кибератак. Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на инфокоммуникационную систему в целях нарушения и (или) прекращения ее функционирования и (или) создания угрозы безопасности обрабатываемой такой системой информации. Таким образом, понятие кибербезопасности включает в себя защищенность информации, которая обрабатывается инфокоммуникационной системой (информационная безопасность), так и защищенность процесса функционирования самой инфокоммуникационной системы (функциональная безопасность).

Цель работы состоит в исследовании проблем, связанных с обеспечением кибербезопасности объектов информатизации для создания условий реализации решений, обеспечивающих снижение и минимизацию кибер рисков.

Методы исследования. В реальной среде функционирования любой инфокоммуникационной системы независимо от нее существует множество угроз ее безопасности. Угроза безопасности инфокоммуникационной системе – возможное воздействие на нее, которое прямо или косвенно может нанести ущерб ее безопасности. Следует разделять угрозы функциональной и информационной безопасности исходя из функций, на которые они нацелены. Совокупность всех угроз T = {1, 2, , ..., m} (от англ. threat), которые в той или иной степени могут нанести ущерб безопасности инфокоммуникационной системы, формируют реальную среду ее функционирования [1].

Именно на такое функционирование следует рассчитывать при эксплуатации инфокоммуникационных систем. Любая угроза не может существовать сама по себе – у нее должен быть источник. Источники угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Таким образом, источником угрозы могут являться [2]:

− субъекты, потенциальные неумышленные или преднамеренные действия, которых могут нанести ущерб функциональной или информационной безопасности инфокоммуникационной системы;

− технические средства – аппаратные, программные или аппаратно-программные средства и комплексы, отказы которых или наличие в их реализации логических ошибок может привести к нарушению безопасности инфокоммуникационной системы;

− стихийные явления – стихийные бедствия, частично или полностью препятствующие функционированию инфокоммуникационной системы.

Оптимальным методом оценки угроз является метод экспертных оценок, при котором экспертам предлагается оценить возможность реализации некоторого перечня угроз. В качестве критериев оценки опасности конкретной угрозы, согласно [3], следует выбрать возможность возникновения источника угрозы (К1), степень его готовности произвести атаку (К2), а также фатальность для инфокоммуникационной системы от реализации угрозы (К3). Коэффициент опасности угрозы вычисляется на основании баллов (дискретно от 1 до 10), выставленных экспертом по трем критериям, по следующей формуле:

$$K_{\text{опуг}} = \frac{K_1 K_2 K_3}{10^3}$$

При таком расчете максимальное значение коэффициента опасности угрозы при выставлении экспертами максимальных баллов по всем критериям будет равно единице. Анализируя коэффициенты опасности совокупности угроз, можно произвести их ранжирование и определить для конкретной инфокоммуникационной системы перечень наиболее опасных из них. Сами по себе угрозы не представляют опасности инфокоммуникационных систем. Сосуществуя совместно с ним, угрозы могут вовсе не причинять ущерба их безопасности. Опасность для инфокоммуникационной системы представляют только те угрозы, для которых она является уязвимой, или, иными словами, обладает определенными уязвимостями, через которые источники угроз могут реализовать свои угрозы и нанести ущерб данному объекту. Уязвимость инфокоммуникационной системы – это присущие инфокоммуникационной системе причины, приводящие к нарушению безопасности ее функционирования или безопасности информации, которая в ней обрабатывается.

Результаты исследования. В связи с тем, что неуклонно растет количество киберпреступлений, инфокоммуникационные системы становятся как предметом таких преступлений, так и средством их совершения, в перспективе намечается формирование тотальной зависимости транспортной отрасли от защищенности инфокоммуникационных систем, построить абсолютно адекватную систему защиты не представляется возможным. Особенно, если затраты на ее организацию и сопровождение не должны превышать предполагаемый ущерб от ее нарушения в результате реализации угроз. Таким образом, необходимо выбрать методику, которая позволит определить опасность угроз для инфокоммуникационной системы, сравнить угрозы между собой и провести ранжирование.

Выводы. Для оценки рисков кибербезопасности инфокоммуникационной системы необходимо в первую очередь выделить ее активы. Совокупность активов инфокоммуникационной системы – это все то, что необходимо для ее штатного функционирования и находится в ее распоряжении (аппаратные средства, программное обеспечение, хранимая и (или) обрабатываемая информация. Процесс оценки рисков для каждого из активов должен учитывать стоимость самого актива и вероятностную характеристику возможности нарушения его кибербезопасности. Процесс изменения совокупности угроз в процессе функционирования инфокоммуникационной системы является гораздо более динамичным по сравнению с процессом изменения совокупности ее уязвимостей. В связи с этим для оценки рисков целесообразно первостепенное внимание уделять именно угрозам кибербезопасности инфокоммуникационных систем.

Литература

1. Буй П.М. Оценка рисков кибербезопасности инфокоммуникационных систем // Кодирование и цифровая обработка сигналов в инфокоммуникациях. – Минск, 2020. – 68-73.
2. Вихорев С.В., Кобцев Р.Ю. // Защита информации. Конфидент. 2002. № 2. С. 44–49.
3. Вихорев С.В., Кобцев Р.Ю. // Защита информации. Конфидент. 2002. № 3. С. 80–84.

УДК 004.056

Закирьяева Эвелина Серверовна
обучающаяся Э-б-о-221
Институт экономики и управления
Усенко Роман Станиславович
старший преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ФИШИНГ КАК РАСПРОСТРАНЁННАЯ МОДЕЛЬ КИБЕРМОШЕННИЧЕСТВА

Кибермошеничество – серьёзная проблема современного общества. В настоящее время мошенников на просторах сети Интернет появляется всё больше и больше, и хищения денежных средств с банковских карт и электронных кошельков происходит намного чаще. Киберпреступники прибегают к всякого рода уловкам, чтобы заманить и обмануть пользователя. Они используют довольно заманчивые предложения, которые должны настораживать людей, но никак не подталкивать совершить то или иное действие, которое потребовал от него мошенник. Одним из самых распространённых видов интернет-мошеничества является фишинг.

Согласно энциклопедии Касперского под фишингом понимается вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать или обновить личные данные [1].

Компания Group-IB, один из мировых экспертов в сфере кибербезопасности сообщила о том, что в 2022 году в российском сегменте интернета было около 18000 фишинговых сайтов, что составляет на 15% больше, чем в 2021 году [2].

В первом полугодии 2022 года произошел рост случаев онлайн-мошенничества с использованием известных брендов — на 579% по сравнению с аналогичным периодом 2021 года. По оценкам Group-IB, для привлечения внимания жертв злоумышленники используют уже более 2100 мировых брендов и торговых марок компаний из сферы телекоммуникаций, сферы услуг, банковского сектора и т.д. Для сравнения: в конце 2021 их было всего 120. Чаще всего за прохождение опроса мошенники обещают пользователям крупное вознаграждение или ценный приз, но в итоге жертва сама лишается денег и данных банковских карт. Ежемесячные потери пользователей от таргетированного мошенничества в мире Group-IB оценивает по минимальным подсчетам в 5,9 млрд руб. [3].

Атаки с использованием фишинговых сайтов показывают свою эффективность из года в год. Фишинговые рассылки влекут за собой существенные финансовые убытки для компании. По статистике вредоносные письма открывают до 85 % сотрудников, чаще всего это специалисты, напрямую не связанные с IT. Однако у них может не быть интересующих злоумышленников прав доступа, поэтому ущерб компании от похищения таких учетных записей редко бывает существенным [4].

Неподготовленным пользователям трудно отличить фишинговые письма от настоящих. Эксперты советуют не открывать подозрительные электронные письма. На 2020 год бесплатные почтовые сервисы, которые использовали злоумышленники для отправки украденных данных, составляли 61% об общего числа используемых email-адресов.

Обычно киберпреступники используют одноразовые адреса электронной почты, только 23% email-адресов, встречавшихся на базе фишинг-китов Group-IB, были использованы повторно [5].

Для того чтобы избежать фишинговой атаки необходимо знать следующие правила безопасности:

1. Подключить двухфакторную аутентификацию везде, где это возможно. Двойная защита на сервисах, запрашивающих проверку захода в личный кабинет по двум параметрам: через логин, пароль и, например, по коду СМС.

2.Установить надежный антивирус — он поможет не только отсканировать скачиваемые программы на вредоносный код, но и определить фишинговые страницы.

3.Использовать браузеры Chrome, Safari, Firefox. Они уже имеют антифишинговую защиту.

4.С осторожностью открывать письма или сообщения от неизвестных отправителей.

5.Подключить почтовые фильтры. Фишинговые мошенники часто делают массовые рассылки, поэтому хороший почтовый фильтр пометит их как спам-рассылку. Попробовать настроить почтовый клиент или антивирус, чтобы сервис проверял и вложения.

6.Не переходить по странным ссылкам.

7.Оформить виртуальную карту для покупок онлайн. Такая карта не имеет физического носителя и выпускается только в цифровом виде. Привязана она к вашему основному счёту, но имеет другие реквизиты. Используя такую карту, вы не «светите» свои личные данные [6].

В настоящее время ничто не указывает на уменьшение числа кибератак [7]. Необходимо дальнейшее повышение грамотности населения в вопросах информационной безопасности.

Литература

1. Что такое «фишинг». [Электронный ресурс]. - URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/ (дата обращения: 03.02.2023).
2. Статья Фишинг в России. [Электронный ресурс]. - URL: https://www.tadviser.ru/index.php/Статья:Фишинг_в_России (дата обращения: 03.02.2023).
3. Статья компании Group-IB. [Электронный ресурс] . - URL: https://www.group-ib.ru/media-center/press-releases/brands/ (дата обращения: 03.02.2023).
4. Trust Technologies [Электронный ресурс] . - URL: https://www.trusttech.ru/expert-materials/za-god-kolichestvo-fishingovykh-atak-vyroslo-v-2-raza/ (дата обращения: 04.02.2023).
5. Статья компании Group-IB. [Электронный ресурс] . - URL: https://blog.group-ib.ru/kit (дата обращения: 04.02.2023).
6. Что такое фишинг: способы защиты и безопасности. [Электронный ресурс] . - URL: https://www.reg.ru/blog/kak-opredelit-fishing-i-ne-popastsya-na-kryuchok/ (дата обращения: 04.02.2023).
7. Плотникова, П. В. Киберпреступность как угроза обществу / П. В. Плотникова, Р. С. Усенко // Проблемы информационной безопасности : Труды VI Всероссийской с международным участием научно-практической конференции, Симферополь-Гурзуф, 13–15 февраля 2020 года. – Симферополь-Гурзуф: ИП Зуева Т.В., 2020. – С. 105-107.

УДК 330.341.11

Иваненко Ирина Анатольевна
к. э. н., доцент кафедры
мировой экономики и экономической теории
Горячих Сергей Игоревич
студент 1 курса направления
подготовки 38.03.01 Экономика
направленность «Цифровая экономика»
ГБОУ ВО РК «КИПУ имени Февзи Якубова»
Республика Крым, Россия

КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВА ЦИФРОВОЙ ЭКОНОМИКИ ГОСУДАРСТВА

С увеличением числа пользователей, устройств и программ в сочетании с растущим потоком сведений, большая часть которых является конфиденциальной информацией, выросла и потребность в защите персональных данных от интернет-атак злоумышленников. Целью подобных кибератак может стать подделка, уничтожение или хищение данных для их перепродажи на подпольных цифровых рынках или дальнейшего вымогательства денежных средств. Киберпреступники выбирают личную информацию: имена, адреса, паспортные данные, номера и коды кредитных карт. В последнее время особенно остро стоит вопрос кибербезопасности. Ей все большее внимание уделяют как отдельные лица, так и предприятия, которые выстраивают целую защиту от возможных ловушек и несанкционированного доступа к центрам обработки данных и другим компьютеризированным системам. Стремительное увеличение числа персональных компьютеров, свободный доступ к Интернету привлекает к виртуальному общению всё больше и больше людей. Социологические опросы показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые беспокоят людей сегодня.

Актуальность рассматриваемого материала заключается в том, что в последнее десятилетие киберпреступность особенно сильно ударила по передовым, современным государствам. Исследователи полагают, что каждый житель таких стран должен ожидать, что все его личные данные могут быть похищены без его согласия в любое время. Компании, которые не смогли защитить персональные данные сотрудников и пользователей, рискуют сильно подорвать свою репутацию в рыночной сфере. Согласно исследованиям, 59% российских компаний в 2019 году столкнулись с утечками информации. Однако 63% из пострадавших от кибератак организаций скрыли данный инцидент от своих сотрудников, клиентов.

Аналитики полагают, что глобальные расходы на киберпреступность будут расти на 15% в год в течение следующих пяти лет, достигнув примерно 10,5 триллионов долларов в год к 2025 году по сравнению с 3 триллионами в 2015 году. Последствия от кибератак значительно превышают ущерб, нанесенный стихийными бедствиями за год, и могут быть более

прибыльными для преступников, чем глобальная торговля всеми основными незаконными наркотиками вместе взятыми [2].

Цифровые данные и операции уже лежат в основе большинства современных организаций, и эта тенденция только усиливается. Но с такой зависимостью от компьютерных систем возникает множество киберугроз. Эти риски могут быть внутренними, исходящими от сотрудников и подрядчиков. Они могут быть внешними, результатом деятельности киберпреступников или даже ваших собственных клиентов. Они могут быть преднамеренными актами кражи или нарушения данных, или просто вызваны человеческой ошибкой и небрежностью.

Кибербезопасность - краеугольный камень цифровой экономики государства, где киберландшафт быстро растет и с каждым днем становится все более сложным. Большая интеграция и зависимость от технологий в сочетании с увеличением векторов угроз и уязвимостей в системе безопасности заставляют как правительство, так и граждан осознать важность кибербезопасности. Информация часто является самым ценным активом организации; следовательно, кибербезопасность – защита этого ценного актива – должна быть интегрирована в основные операционные и бизнес-процессы.

Кибербезопасность обладает рядом преимуществ:

- непосредственная защита от атак сети;
- повышение уверенности клиентов и других заинтересованных лиц;
- повышенная гарантия непрерывности бизнеса и доступности;
- предотвращение несанкционированного доступа к данным и информации.

Соблюдение юридических требований по защите персональных данных. Критически важные секторы инфраструктуры взаимосвязаны и зависят от защищенных киберсистем, а киберсбои в критически важной инфраструктуре могут иметь серьезные экономические последствия, способствуя значительным убыткам для бизнеса и негативно влияя на местную, национальную и глобальную экономику.

Кроме того, косвенные издержки кибератаки могут привести к производственным потерям, перебоям в продажах и подрыву доверия потребителей. Подобные косвенные экономические издержки могут быть такими же значительными, как и ущерб оборудованию и инфраструктуре, с потенциально далеко идущими и долгосрочными последствиями для занятости, инноваций и экономического роста.

Кибербезопасность не должна стоить огромных денег или требовать много времени для своего внедрения. Независимо от размера коммерческой компании повышение кибербезопасности помогает защитить как собственные данные, так и данные клиентов, что обычно способствует улучшению деловых отношений и открывает новые возможности в ведении бизнеса. Кибербезопасность становится важным компонентом успеха в бизнесе и важнейшей защитой от угроз информационной эпохи [1].

Сейчас положение дел касательно концепции информационной безопасности не совсем определены, так как не имеют четкой грани в полном представлении и понятии, хотя и сформированы на государственном уровне, как и во многих других государствах информационного (современного) типа. Чтобы защититься и избежать проблем с мошенничеством, достаточно окунуться в финансовую грамотность. Именно она должна помочь людям в защите от любых схем. Зная простые базовые вещи, можно с легкостью распознать мошенников.

В завершение можно сделать вывод о том, что нужно принимать меры для борьбы с киберпреступностью, а также вводить все возможные наказания, различные меры ответственности. Должны быть усилены меры по защите личной информации, чтобы свести до минимума неблагоприятные последствия. Однако стоит помнить о том, что высокотехнологичные открытия и технические средства требуют большого финансового обеспечения. В соответствии с этим, необходимо грамотно вести процесс регулирования себестоимости выпускаемых продуктов путем использования информационных платформ и систем. Цифровая экономика, как и все выходящие из нее перспективные проекты, являются главным ориентиром страны для становления новой экономической среды.

Литература

1. Козлова Н. Ш. Кибербезопасность и информационная безопасность: сходства и отличия / Н. Ш. Козлова, В. А. Довгаль // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2021. – № 3(286). – С. 88-97.

2. Эриашвили Н.Д. Теоретико-правовые основы противодействия международной преступности/ Н.Д. Эриашвили, Г.М. Сарбаев, Ю.А. Иванова // Социально-гуманитарное обозрение. – 2021. – № 1. – С. 43-50.

УДК 004.056

Карамова Марианна Валерьевна
Зуйкова Елизавета Андреевна
обучающиеся 1 курса направления
подготовки 38.03.01 Экономика
Институт экономики и управления
Научный руководитель:
Усенко Роман Станиславович
старший преподаватель
Физико-технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

СОВРЕМЕННЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Основной задачей национального государства является защита национальной безопасности, которая включает в себя защиту его граждан, экономики и институтов. Первоначально национальная безопасность защищала нацию от военных угроз, но в настоящее время ее масштабы стали шире, и включают в себя безопасность от терроризма и преступности, безопасность экономики, энергетики, окружающей среды, продовольствия, критически важной инфраструктуры и, наконец, кибербезопасность [1].

Согласно отчету о глобальных рисках в сфере IT от лаборатории Касперского за 2016 г., основные причины наиболее дорогостоящих утечек данных связаны со старыми атаками, которые развиваются с течением времени в следующем порядке [2]:

- вирусы, вредоносные и троянские программы;
- недостаток усердия и неподготовленность сотрудников;
- фишинг и социальная инженерия;
- целевая атака;
- программы-вымогатели.

Первые три причины в этом списке - хорошо известны в сообществе кибербезопасности, они все еще актуальны. Настоящая проблема состоит в том, что обычно они связаны с человеческими ошибками. Все может начинаться с фишингового сообщения по электронной почте, использующего социальную инженерию, чтобы заставить сотрудника щелкнуть ссылку, которая может загрузить вирус, вредоносное программное обеспечение или троянскую программу.

Термин целевая атака (или продвинутая постоянная угроза) иногда не слишком понятен отдельным лицам, но есть некоторые ключевые атрибуты, которые могут помочь определить этот тип атаки. Первый и самый важный атрибут заключается в том, что у злоумышленника есть конкретная цель, когда он или она начинает составлять план атаки. Во время этой начальной фазы злоумышленник потратит много времени и ресурсов на проведение исследований для получения информации, необходимой для осуществления атаки. Мотивом для этой атаки обычно является несанкционированная передача данных с компьютера, иными словами, их кража.

Еще один атрибут этого типа атаки – это срок службы или период времени, в течение которого они поддерживают постоянный доступ к сети цели. Намерение злоумышленника состоит в том, чтобы продолжать дальнейшее распространение по сети, взламывая различные системы, пока цель не будет достигнута [2].

Основные статистические данные по киберпреступности в 2022 году говорят, что 95% всех киберпреступлений и нарушений безопасности происходят из-за человеческой ошибки. 95% всех записей, взломанных в 2016 году, относились только к трем секторам: к розничной торговле, технологиям и государственному управлению. 10% утечек данных были связаны и мотивированы шпионажем, а 86% были мотивированы деньгами.

ФБР сообщило, что после пандемии COVID-19 количество сообщений о киберпреступлениях увеличилось на 300%. По прогнозам экспертов, к 2025 году ущерб от киберпреступлений достигнет 10,5 триллионов долларов в год [3].

Согласно статистике киберпреступлений, лишь 5% всех папок компании эффективно защищены. Самым вредоносным из всех типов файлов вредоносных программ, отправляемых по электронной почте, является .exe. По данным на май 2022 года, 64% американцев никогда не проверяли свою систему, чтобы выяснить, не подвергалась ли она атаке. В 2020 году 48% всех вредоносных вложений в электронную почту были отправлены в виде файлов Microsoft Office.

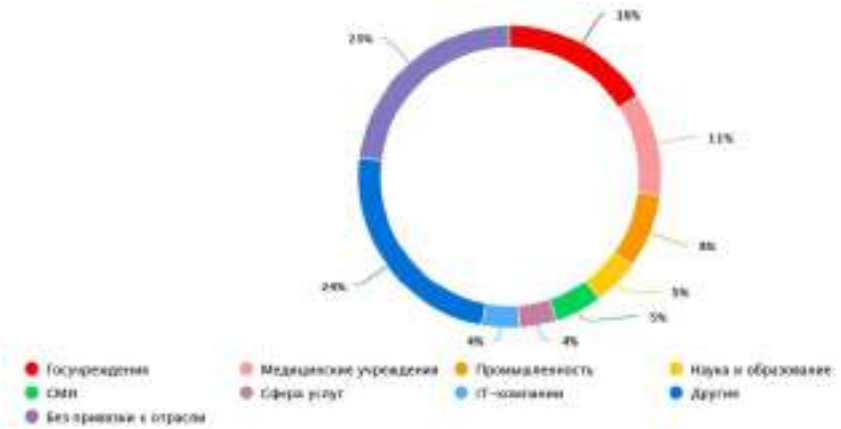

Рисунок 1 – Категории жертв кибербезопасности среди организаций [4]

В настоящее время ничто не указывает на уменьшение числа кибератак. Более того, чем больше точек входа для атак, тем больше требуется усилий для защиты сетей и устройств [5].

Один из наиболее проблемных элементов кибербезопасности – это постоянно меняющийся характер рисков безопасности. По мере появления новых технологий и их использования появляются и новые способы атак.

Литература

1. Хлопов О. А. Проблемы кибербезопасности и защиты критической инфраструктуры: // The scientific heritage. No 45. (2020). URL: https://cyberleninka.ru/article/n/problemykiberbezopasnosti-i-zaschity-kriticheskoy infrastruktury/viewer (дата обращения: 22.01.2023).
2. Кибербезопасность: стратегии атак и обороны: учебное пособие / пер. с англ. Д. А. Беликова/ Диогенес Ю., Озкайа Э. – Москва: ДМК Пресс, 2020. – 326 с.
3. Статистика киберпреступлений 2022 [Электронный ресурс]. – Режим доступа: https://clickfraud-ru.turbopages.org/clickfraud.ru/s/statistika-kiberprestuplenij-2022/ (дата обращения: 22.01.2023).
4. Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 22.01.2023).
5. Плотникова, П. В. Киберпреступность как угроза обществу / П. В. Плотникова, Р. С. Усенко // Проблемы информационной безопасности : Труды VI Всероссийской с международным участием научно-практической конференции, Симферополь-Гурзуф, 13–15 февраля 2020 года. – Симферополь-Гурзуф: ИП Зуева Т.В., 2020. – С. 105-107.

УДК 004.056

Корец Александр Олегович
студент 1-го курса
Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Байракова Ирина Викторовна
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

КИБЕРБЕЗОПАСНОСТЬ

В наши дни сфера кибербезопасности развивается быстро, динамично, поэтому системе защиты коммерческой компании необходимо совершенствоваться постоянно. Крупные и малые организации подвергаются атакам каждый день, от простых фишинговых писем до сложных, подробных операций, организованных преступными группировками, и для каждой исправленной уязвимости всплывает новая, готовая к эксплуатации. Кибербезопасность не должна стоить огромных денег или требовать много времени для своего внедрения. Независимо от размера коммерческой компании повышение кибербезопасности помогает защитить как собственные данные, так и данные клиентов, что обычно способствует улучшению деловых отношений и открывает новые возможности в ведении бизнеса. Кибербезопасность становится важным компонентом успеха в бизнесе и важнейшей защитой от угроз информационной эпохи.

Внедрение цифровых технологий в современную жизнь оказалось стремительным и колоссальным по своим последствиям. Риск для промышленных коммуникационных сетей, особенно тех, которые поддерживают критически важные инфраструктуры (местные,

региональные или национальные), в последние годы неуклонно возрастает, поэтому происходит увеличение исследований в области кибербезопасности. Современный мир ориентирован на цифровизацию и оптимизацию деятельности, и эта тенденция затрагивает все сферы жизнедеятельности человека. Вся наша жизнь «в онлайне»: проверка почты, оплата коммунальных услуг, работа и досуг, запись на прием к врачу. Государственные структуры понимают и принимают потребности современного человека и, с каждым годом ближе к цифровизации и отказу от излишнего бюрократизма. Уже сейчас, с помощью единого портала государственных услуг можно получить огромное количество услуг, не выходя из дома, например: оформление паспортов разного типа, представление пособий и государственной поддержки, регистрация по месту жительства, регистрация предпринимателей и юридических лиц, постановка на учет авто в ГИБДД, смена места жительства, изготовление гражданских документов (полис, СНИЛС и так далее) представление ИНН, регистрация прав собственности, выдача документов о правах на то или иное имущество [1]. Огромное количество наших личных данных находятся на разных сайтах, и тут уже встает вопрос о том, насколько это безопасно. Информационная безопасность, или кибербезопасность - это совокупность методов защиты для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от атак злоумышленников. Инциденты, связанные со взломом, фишингом и вредоносным программным обеспечением (ПО), в настоящее время становятся главными причинами нарушения безопасности. Кроме того, на попытки взлома оказывают влияние человеческие ошибки. В борьбе с киберпреступниками и предотвращении нарушений безопасности критически важными являются образование и осведомленность.

Кибербезопасность связана с атаками изнутри или за пределами организации. Это структура защиты всего, что уязвимо для взлома, атак или несанкционированного доступа, что в основном состоит из компьютеров, устройств, сетей, серверов и программ. Кибербезопасность также относится исключительно к защите данных, исходящих в цифровой форме – она характерна для цифровых файлов, когда говорим о кибербезопасности, то автоматически обсуждаем цифровую информацию, системы и сети.

Кибербезопасность – это область информационных технологий, ориентированная на защиту систем, включающих в себя электронные записи, устройства для отслеживания информации, оборудование и программное обеспечение, используемое для оказания услуг и управления ими. Кибербезопасность направлена на предотвращение атак путем защиты систем от несанкционированного доступа, использования и раскрытия данных. Основная цель – обеспечить доступность, конфиденциальность и целостность критически важных данных, которые в случае компрометации могут поставить под угрозу жизнь. Кибератаки могут принимать разные формы – от программ-вымогателей до кражи личной информации. Воздействие атаки может варьироваться в зависимости от размера объекта. Несколько проблем являются общими для всех отраслей промышленности и производства: защита конфиденциальной информации персональных данных, уязвимости устаревших систем, проблемы ИТ и нарушения безопасности. Кибербезопасность – это защита данных в электронной форме (например, компьютеров, серверов, сетей, мобильных устройств и т.д.) от компрометации или атак. Частично это определение критических данных, их местонахождения, подверженности рискам и технологии, которую необходимо внедрить для их защиты.

Кибербезопасность представляет собой практику защиты данных извне ресурса в Интернете, предназначена для защиты киберпространства от кибератак и для защиты всего периметра в киберсфере, устраняет опасность для киберпространства, предотвращает киберпреступления, кибермошенничество и применяется правоохранительными органами, оказывает помощь специалистам при постоянной угрозе взлома данных, занимается проблемами угроз, возникающими в киберпространстве.

Киберугрозы - действия, направленные на кражу данных, внедрения вредоносного программного обеспечения, нарушение работы компьютерных систем [2, с. 634]. Выделяют несколько источников киберугроз: враждебные страны, террористические организации, преступные группы, хакеры и вредоносные инсайдеры. Причиной может быть что угодно, шпионаж, шантаж, угроза национальной безопасности, а также личная выгода.

Специалисты по кибербезопасности традиционно понимают, какие технологии, брандмауэры и системы защиты от вторжений необходимы, но не обязательно были связаны с бизнесом по оценке данных. Поскольку эта тема становится все более важной для бизнеса, роль экспертов по управлению рисками кибербезопасностью меняется для должной защиты данных. Деловые партнеры и инвесторы все больше осознают важность этой темы, и компании заинтересованы в регулярной и эффективной защите данных и управлении как физическими рисками, так и киберрисками. Кибербезопасность – это особый тип информационной безопасности, относящийся к способам, которыми организации защищают цифровую информацию, такую как сети, программы, устройства, серверы и другие цифровые активы. Они

принимают активное участие в защите серверов, конечных точек, баз данных и сетей, обнаруживая дыры и неправильные конфигурации, которые создают уязвимости. Другими словами, они несут ответственность за предотвращение нарушений. Самые талантливые думают, как хакеры и, возможно, даже были таковыми в прошлом.

Информационная безопасность государства достигается целым комплексом организационных и технических мер, направленных на защиту личных данных граждан. Организационные меры включают: документированные процедуры и правила работы с разными видами информации, IT-сервисами, средствами защиты и т. д [3]. Государственные учреждения Российской Федерации в значительной степени полагаются на информационные технологии для повышения эффективности работы организаций, и для них кибербезопасность играет немаловажную роль.

К вопросу кибербезопасности подходят очень ответственно, ведь взлом информации в государственном секторе может поставить под угрозу не только выполнение критически важных задач, конфиденциальность данных граждан, но и безопасность страны в целом. Так, 1 мая 2022 года Президент Российской Федерации издал указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Из указа следует, что госструктурам необходимо будет создавать подразделения по обеспечению информационной безопасности. Кроме того, запрещается использование средств защиты информации от компаний из недружественных стран [4]. Основная часть документа посвящена структурным подразделениям, которые осуществляют функции по обеспечению информационной безопасности. Их назвали киберотделами. Такие подразделения должны появиться в каждом российском ведомстве, государственном фонде, государственной корпорации и на стратегическом или системообразующем предприятии, а также в юридических лицах, являющихся объектами критической информационной инфраструктуры России. Функции киберотделов описаны лаконично: «обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты» [5].

Трудно переоценить важность кибербезопасности в современном мире. Кибербезопасность является необходимым условием развития информационного общества. По мере того, как мир становится все более взаимосвязанным, исследования в области кибербезопасности будут оставаться одним из самых эффективных и незаменимых инструментов в глобальной борьбе с злоумышленниками, желающими вызвать хаос и разрушение, поэтому невозможно полностью исключить риск киберугроз, но нужно стремиться свести их к минимуму.

Литература

1. Единый портал государственных услуг: [официальный сайт]. - URL: https://www.gosuslugi.ru/ (дата обращения: 18.08.2022).

2. Кодацкий Н.М., Мотуз А.С. Угрозы кибербезопасности в информационной среде // StudNet. 2022. №1. URL: https://cyberleninka.ru/article/n/ugrozy-kiberbezopasnosti-vinformatsionnoy-srede (дата обращения: 18.08.2022).

3. Басшыкызы Д. Обеспечение кибербезопасности в современном мире // Наука, техника и образование. 2022. №3 (86). URL: https://cyberleninka.ru/article/n/obespecheniekiberbezopasnosti-v-sovremennom-mire (дата обращения: 18.08.2022).

4. Новости России и мира за сегодня BFM.RU: [официальный сайт]. - https://www.bfm.ru/news/499063 (дата обращения: 18.08.2022).

5. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». - URL: http://publication.pravo.gov.ru/Document/View/0001202205010023

УДК 004.056:69

Норец Надежда Константиновна
к.э.н., ассистент кафедры бизнес-информатики
и математического моделирования
Физико-технический институт
ФГАОУ ВО «КФУ имени В. И. Вернадского»
Республика Крым, Россия

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В СТРОИТЕЛЬНОЙ ОТРАСЛИ

Управление зданиями и сооружениями с каждым годом становится все более простым, более эффективным и инновационным благодаря внедрению Интернета вещей (IoT). Предполагается, что в течение следующих 10 лет в зданиях будут установлены миллиарды считывающих устройств. При этом крайне важно, чтобы программное обеспечение для управления зданиями могло обеспечить кибербезопасность и стандартизацию, используя при этом преимущества сервиса Интернет вещей.

При принятии управленческих решений и формировании безопасного функционирования систем обеспечивается хранение коммерческой тайны и другой конфиденциальной информации. Как правило, речь идет не только о физической безопасности пользователей объекта во время эксплуатации. Трудно представить масштаб последствий, если особенности конструкций зданий общественного пользования попадут в руки террористов. Именно поэтому многие строительные организации задаются вопросом о необходимости получения специальных лицензий ФСБ. На самом деле такая лицензия нужна только определённому виду компаний, которые занимаются специфическими разработками, в частности - создают ключи шифрования и криптосистемы, то есть системы шифрования. В привязке к отрасли это может быть некая база российских данных, которую можно купить и передать третьим лицам. Вот в этом случае придется получать разрешение ФСБ. В большинстве же случаев можно опираться на классификатор средств защиты информационных систем ФСТЭК. В Федеральной службе по техническому и экспортному контролю принято 5 уровней, где 5 - минимальный, а 1 - максимальный. В последнем случае речь идет о государственной тайне. Как правило, в строительной отрасли достаточно первых трех уровней, с которыми работает большинство поставщиков ИТ-оборудования. Однако встречаются и более секретные данные. К примеру, для применения программного комплекса на объектах нефтегазового сектора компании “Мобильные решения для строительства” необходимо было подтвердить 4 класс секретности, и это скорее исключение, чем правило.

Угроза кибератак на системы управления зданиями (BMS) вызывает растущую озабоченность как внутри строительной отрасли, так и за ее пределами. Ежегодно увеличивается число нападений на различные объекты инфраструктуры государственной и частной собственности. Как и при большинстве возникающих цифровых рисков львиная их доля – это риски утечки информации и в большей степени утечки эти происходят из-за человеческого фактора. Это могут быть некомпетентные служащие или банальная кража персональных данных.

Итак, что могут сделать владельцы зданий и другие заинтересованные стороны перед лицом этих растущих угроз? В области систем управления зданиями ответственность за безопасность несут не только владельцы зданий, но и производители и частично партнеры, которые предоставляют продукты конечным пользователям.

Со стороны производителя требуется обеспечение безопасного жизненного цикла разработки. Это означает, что продукты разрабатываются с учетом требований безопасности и “обкатываются” к тому времени, когда они попадают потребителю.

Что касается конечного пользователя (компании, обслуживающей здание или сооружение), то соблюдение надлежащих процессов и процедур поможет свести к минимуму уровень риска. Процессы должны быть налажены таким образом, чтобы ограничить вероятность человеческой ошибки, открывающей дверь для уязвимостей кибератак. Незащищенные ноутбуки, рабочие станции, рабочие зоны и небрежное управление паролями (включая отказ от отзыва учетных данных и доступа, когда сотрудник покидает компанию) - все эти факторы могут увеличить риск разоблачения. Бизнес-процедуры также должны быть разработаны таким образом, чтобы предотвращать потенциальные угрозы со стороны инсайдеров, такие как саботаж, мошенничество, кража или утечка интеллектуальной собственности или секретной/ конфиденциальной информации.

Традиционные решения в области ИТ-безопасности должны быть включены в сети систем управления зданиями. Обучение людей, которые управляют сетями BMS, является важнейшим фактором успеха. Бдительность и должная осмотрительность должны включать в себя дисциплинированное обслуживание систем BMS с последними обновлениями.

Литература

1. Апатова Н. В. Интернет и бизнес / Н. В. Апатова, О. В. Бойченко, О. Л. Королев. – Симферополь : ИП Зуева Т. В., 2022. – 190 с.
2. Апатова Н. В. Кибербезопасность: проблемы бизнеса / Н. В. Апатова // Проблемы информационной безопасности социально-экономических систем: VIII Всероссийская с международным участием научно-практическая конференция, Симферополь - Гурзуф, 17–19 февраля 2022 года. – С. 3.
3. Бакуменко М. А. О преимуществах применения технологий искусственного интеллекта в промышленности / М. А. Бакуменко, В. А. Васильева // Тенденции развития Интернет и цифровой экономики: Труды V Всероссийской с международным участием научно-практической конференции, Симферополь-Алушта, 02–04 июня 2022 года. – С. 126-127.
4. Боркова Е. А., Изотова А. Г., Литвинова Н. А. Цифровая трансформация строительной отрасли в условиях макроэкономического шока COVID-19 // Вопросы инновационной экономики. – 2020. – Том 10. – № 4. – С. 2129-2140.
5. Ветрова Н. М. Об особенностях направлений развития строительной отрасли Республики Крым в рамках концепции биосферной совместимости / Ветрова Н. М., Гайсарова А. А., Пригорская Я. Д. // Экономика строительства и природопользования. - 2021. - № 2 (79). - С. 5-10.
6. Круликовский А. П. Роль процесса цифровизации и информационной безопасности / А. П. Круликовский, В. А. Васильева // Проблемы информационной безопасности социально-экономических

систем: VII Всероссийская с международным участием научно-практическая конференция, Гурзуф, 18–20 февраля 2021 года. – С. 116-117.

7. Насонов Е. И., Макиша Е. В. Киберфизические системы в строительной отрасли // ИВД. – 2019. – №1 (52). – URL: https://cyberleninka.ru/article/n/kiberfizicheskie-sistemy-v-stroitelnoy-otrasli (дата обращения: 12.01.2023).

8. Норец Н. К. Направления цифровизации строительного производства / Н. К. Норец // Экономика строительства и природопользования. – 2022. – № 4(85). – С. 5-12.

9. Норец Н. К. Технологии цифровизации строительной отрасли / Н. К. Норец // Стратегии адаптации ESG модели к меняющейся экономической реальности: Материалы III Всероссийской научно-практической конференции с международным участием, Омск, 05–06 октября 2022 года. – С. 193-198.

10. Стратегическое управление развитием информационной безопасности социально-экономических систем на основе умных технологий: Монография / Л. М. Борщ, С. В. Герасимова, А. Р. Жарова [и др.]. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. – 392 с.

11. Сулимова Е. А., Новицкая Д. А. Развитие цифровой экономики в сфере строительства // Экономика строительства. – 2022. – №10. – URL: https://cyberleninka.ru/article/n/razvitie-tsifrovoy-ekonomiki-v-sfere-stroitelstva (дата обращения: 12.01.2023).

УДК 004.056

Романюк Елена Витальевна
к.э.н., доцент кафедры экономической теории
Османова Алие Махмутовна
студентка 1-го курса
Институт экономики и управления
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

КИБЕРБЕЗОПАСНОСТЬ В РОССИЙСКОЙ БАНКОВСКОЙ СФЕРЕ

В настоящее время все чаще слышатся слова о безопасности в цифровой сфере. Цифровая экономика - это новая основа для развития экономики, бизнеса и всего общества. Формирование цифровой экономики - это вопрос безопасности национальной экономики нашей страны. В каком состоянии находится кибербезопасность в России - этот вопрос будет рассмотрен в статье.

Перед началом изучения данного вопроса, ознакомимся с основными понятими кибербезопасности.

Кибербезопасность - это защита подключенных к Интернету систем от киберугроз. Эта практика используется частными лицами и предприятиями для защиты от несанкционированного доступа к центрам обработки данных и другим компьютеризированным системам.

Правильная стратегия кибербезопасности может обеспечить хорошую защиту от вредоносных атак, предназначенных для доступа, изменения, удаления, уничтожения или вымогательства конфиденциальных данных. Кибербезопасность также играет важную роль в предотвращении атак, направленных на отключение или нарушение работы системы или устройства.

Кибератака - это нежелательная попытка украсть, разоблачить, изменить, отключить или уничтожить информацию путем несанкционированного доступа к компьютерным системам. Обычно злоумышленник ищет какую-то выгоду от нарушения сети жертвы.

Российские банки и другие финансовые организации еще не до конца усвоили способы управления киберрисками: в 2020 году у 75 банков были обнаружены нарушения требований кибербезопасности[2]. Скорее всего, проблема отчасти заключается в том, что руководители банков и компаний скидывают ответственность за киберриски на менеджеров. У тех, в свою очередь, не хватает полномочий для решения этих проблем, так как для защиты всех элементов современных систем нужно не только иметь мощную компетенцию внутри компаний, но и серьезную кооперацию в банковской сфере в общем. Государство старается реагировать на современные реалии, так как ЦБ ужесточил требования по защите средств банков и их клиентов от киберпреступников: если ранее кредитные организации должны были обеспечивать информационную безопасность только при проведении операций по переводу денег, то теперь под это требование подвели еще и процедуры по привлечению вкладов.

Американская компания по киберзащите Cybersecurity Ventures ожидает, что глобальные затраты на киберпреступность будут расти на 15 процентов в год, достигнув 10,5 трлн долларов США в год к 2025 году по сравнению с 3 трлн долларов США в 2015 году. Компания Group IB, провела исследование, которое показало, что 74% российских банков не готовы к атакам хакеров. Причину они видят в низком уровне организации защиты[4].

Кибератаки направлены на многие банки, но атаки на малые и средние, становятся все более частыми, целенаправленными и сложными. Согласно исследованию киберпреступности, 43% кибератак направлены на небольшие банки, но только 14% готовы защитить себя[5].

Кибератака не только нарушает нормальные операции, но и может нанести ущерб важным IT-активам и инфраструктуре, от которых невозможно оправиться без бюджета или ресурсов для этого.

ЦБ требует от банков защищать от киберпреступников операции по открытию вкладов клиентов и ведению их счетов. Особые требования по автоматизации защиты предъявлены крупнейшим банкам.

Также за последние несколько лет в рамках усиления информационной безопасности в кредитной и финансовой сфере:

- –приняты нормативные акты, согласно которым банки и финансовые организации обязаны уведомлять ЦБ РФ о выявленных инцидентах информационной безопасности[1];
- –выпущены стандарты СТО БР БФБО-1.5-2018 об управлении инцидентами информационной безопасности и СТО БР ИББС-1.0-2014, освещающий общие вопросы информационной безопасности в финансовой и кредитной сферах;
- –изданы разъяснения о порядке выполнения нормативных актов.

Это привело к заметному снижению числа инцидентов. ЦБ РФ устанавливает наиболее жесткие требования по информационной безопасности к следующим программным модулям[3]:

- –платформа удаленной идентификации в Единой биометрической системе (не в последнюю очередь из-за обработки биометрических персональных данных);
- –системы быстрых платежей;
- –платформы, обслуживающие маркетплейсы;
- –цифровой профиль клиента.

Центральный Банк и государство глубоко привержены поддержке индустрии финансовых услуг в области кибербезопасности. Они планируют расширить свои процедуры проверки банков, чтобы более полно сосредоточиться на кибербезопасности. Пересмотренные процедуры проверки будут включать дополнительные вопросы в области управления IT. Пересмотренные процедуры призваны дать целостное представление готовности учреждения к противостоянию кибератакам и будут адаптированы с учетом уникального профиля рисков каждого учреждения. Государство считает, что такой подход будет способствовать более разумным и сильным программам кибербезопасности, которые отражают разнообразие индустрии финансовых услуг России.

Литература

1.Федеральный закон от 02.12.1990 №395-1 (ред. от 27.12.2019) «О банках и банковской деятельности» (с изм. и доп., вступ. в силу с 01.01.2020 г.)

2. Звонова, Е. А. Деньги, кредит, банки, безопасность : учебник и практикум для среднего профессионального образования / Е. А. Звонова, В. Д. Топчий ; под общей редакцией Е. А. Звоновой. – Москва : Издательство Юрайт, 2021. – 456 с.

3. Исаев, Р. А. Банковский менеджмент и бизнес-инжиниринг : в 2 томах. Том 1 / Р. А. Исаев. – 2-е изд., перераб. и доп. – Москва : ИНФРА-М, 2020. – 286 с.

4. Исаев, Р. А. Секреты успешных банков: бизнес-процессы и технологии : пособие / Р.А. Исаев. – 2-е изд., перераб. и доп. – Москва : ИНФРА-М, 2021. – 222 с.

5. Ядрышникова Н.Е. Банковская система России и перспективы ее развития / Н.Е. Ядрышева // В книге: Сборник тезисов докладов научно-практической конференции студентов Курганского государственного университета Курганский государственный университет. — 2019. — С. 14-15.

УДК 004.056

Сухой Семён Андреевич
обучающийся 1-го курса направления подготовки 38.03.01
Научный руководитель: Романюк Е. В.
к.э.н., доцент кафедры экономической теории
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация

КИБЕРБЕЗОПАСНОСТЬ. ВИДЫ КИБЕРУГРОЗ

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Статистика свидетельствует: согласно отчету RiskBased Security, только за первые девять месяцев 2019 года было зафиксировано 7,9 миллиардов случаев утечки данных. Эти цифры превышают показатели за тот же период 2018 года более чем в два раза (на 112 %) [1, с. 60].

Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина –действия преступников. Некоторые организации привлекают злоумышленников по понятной причине – у них можно взять финансовые и медицинские данные. Однако мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов.

Компания International Data Corporation прогнозирует, что если количество киберугроз будет расти и дальше, то объем расходов на решения в области кибербезопасности к 2022 году достигнет 133,7 миллиардов долларов США. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности [3, с. 70].

Так, Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) разработал принципы безопасной IT-инфраструктуры. NIST рекомендуют проводить постоянный мониторинг всех электронных ресурсов в реальном времени, чтобы выявить вредоносный код, пока он не нанес вреда, и предотвратить его распространение.

Национальный центр кибербезопасности (National Cyber Security Centre) правительства Великобритании выпустил руководство 10 steps to cyber security (10 шагов к кибербезопасности). В нем говорится о том, насколько важно вести наблюдение за работой систем. В Австралии рекомендации по борьбе с новейшими киберугрозами регулярно публикует Австралийский центр кибербезопасности (Australian Cyber Security Centre, ACSC) [2, с. 45].

Далее рассмотрим виды киберугроз. Кибербезопасность борется с тремя видами угроз.

1. Киберпреступление– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. Кибератака – действия, нацеленные на сбор информации, в основном политического характера.
3. Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы – ниже приводим самые распространенные. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

- вирусы – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- троянцы– вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- шпионское ПО – программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях;
- программы-вымогатели шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные;
- рекламное ПО – программы рекламного характера, с помощью которых может распространяться вредоносное ПО;
- ботнеты – сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях;
- SQL-инъекция. Это вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).
- фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.
- атаки Man-in-the-Middle («человек посередине») – это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

Итак, рассмотрев некоторые варианты усиления защиты операционной системы и персональных данных при работе в сети, мы можем сделать вывод, что у каждого пользователя есть множество способов защиты. Ведь для большинства пользователей основной целью пользования Интернетом является поиск нужной им информации и развлечений. Мало кто задумывается о безопасности, открывая браузер или играя в онлайн-игру. Поэтому перед началом работы в Интернете необходимо принять меры безопасности, чтобы в будущем не подвергаться опасности заражения вирусами, кражи данных, потери файлов и т.п. Если пользователь внимателен и осмотрителен, то пользование Интернетом принесет ему только пользу. Поэтому для достижения оптимальных результатов и безопасного использования Интернета необходимо сочетать все эти методы в соответствии с психологическими и возрастными особенностями пользователей и их потребностями.

Литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / КноРус, 2016.
2. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации, 2016.
3. Авчаров И.В. Борьба с киберпреступностью /Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. - М., 2012.

УДК 33.01

Цхададзе Нелли Викторовна
д.э.н., профессор
Калмыкова Алина Зауровна
студент
ФГОБУ ВО «Финансовый университет при Правительстве РФ»
г. Москва, Россия

КИБЕРБЕЗОПАСНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Термин «кибербезопасность» преимущественно западное понятие, так как применять его там стали уже в 90-х годах. Более того, именно ведущие развитые страны увидели в нем особую важность для развития национальной безопасности, поэтому незамедлительно разработали и ввели в действие ряд основополагающих доктрин национальной безопасности. Одним из таких документов является, например, Стратегия и Политика кибербезопасности.

В Российской же федерации данный термин прошел тернистый путь. Так изначально его и вовсе отрицали, а в настоящее время уделяют особое внимание рынку информационной безопасности.

Цель исследования проанализировать текущее состояние рынка информационной безопасности в Российской Федерации.

Первоначально важно отметить, что термин «кибербезопасность» в нынешнее время все еще известен далеко не каждому гражданину нашей страны, синоним «компьютерная безопасность» более популярен, однако все еще данная тема не так популярна, чем в других странах.

Так под кибербезопасностью понимают набор процессов, передовых методов и технологий, которые помогают защитить критически важные системы и сети от цифровых атак. В ногу с технологическим прогрессом идет и распространение данных, а также происходит увеличение количества людей, работающих и подключающихся к сети из разных мест, в связи с этим злоумышленники разрабатывают изощренные методы получения доступа к вашим ресурсам и кражи данных, саботажа вашего бизнеса или вымогательства денег. С каждым годом количество атак увеличивается, а преступники разрабатывают новые методы, чтобы избежать обнаружения.

Проблема кибербезопасности в России особо остро встала в 2022 году, причиной тому послужило беспрецедентное количество хакерских атак на российские компании в самых разных сферах бизнеса и политика нашего государства, в которой одной из ключевых потребностей и является эффективная, практическая информационная безопасность. Также важно отметить, что спусковым крючком для развития этого рынка является массовый отток иностранных производителей продуктов информационной безопасности.

Здесь важно отметить, что, согласно статистике, на 2021 год российские вендоры в области информационной безопасности доминировали на отечественном рынке: они занимают 61% рынка, в то время как на долю иностранных приходится 39%. Но несмотря на превалирующую долю, изначально считалось, что возможности нашей страны ограничены и

уход зарубежных вендоров в 2022 году приведет к сокращению общего объема рынка на 11 %, однако как показывает предварительная экспертная оценка Positive Technologies, рынок ИБ вырос на 10–20%, что говорит о состоятельности российского рынка как самостоятельной единицы и возможности для дальнейшего развития.

На данном этапе можно обозначить следующий круг проблем, которые встают перед политикой государства в сфере кибербезопасности:

- множество кибероперации иностранных государств против российских информационных систем, в том числе кибершпионаж;
- "монополистическая" деятельность транснациональных ИТ-корпораций;
- распространение политически дестабилизирующей информации, информационно-психологическое воздействие;
- использование современных технологий в военно-политических целях, более того тенденция к милитаризации киберпространства;
- формирование враждебного образа России в информационном пространстве;
- уязвимость российских информационных систем перед недоброжелательным иностранным влиянием в силу зависимости России от импортных технологий и др.

В связи с поставленными задачами можно вывести следующие линии тренда в сфере информационных технологий:

Бесспорно можно говорить о том, что мы Россия стремится адаптироваться к новым условиям, однако некоторые пути развития виднелись еще до сложившейся в 2022 году ситуации на рынке.

- в первую очередь политика в сфере цифровых технологий направленна на импортозамещение. Ни для кого не секрет, что немаловажную роль для российского рынка ИТ играли большую роль такие крупнейшие западные компании, как SAP, Microsoft, IBM и Oracle. Однако это стало шансом для отечественных разработчиков не только занять освободившуюся нишу, но и сделать рывок в развитии российских технологий. И, как мы можем видеть, что уже в марте 2022 года спрос на российское программное обеспечение вырос на 300% по сравнению с аналогичным периодом прошлого года.
- целенаправленная борьба с хакерскими атаками. Данный тренд зародился уже в 2020 году – период пандемии, так как компании массово стали вести дела в удаленном режиме, корпоративные сервисы и деловая информация стали более уязвимы, что повело за собой последствия в виде волны хакерских атак. Причем важно отметить, что нападениям подверглись не только отдельные компании, но и целые отрасли, как, например, в 2021 году пострадал банковский сектор, а навыки хакеров улучшились, так как были выявлены новые виды атак. Соответственная сложившая ситуация, повлекла спрос на ИБ-решения различных классов, эта линия продолжается по сей день и, как говорилось раннее, виден прогресс в становлении российских технологии на данном рынке.

Более того считается, что в 2022 году тенденция, обозначившаяся годом ранее, закрепится: Российские компании и государственные структуры начали комплексно подходить к вопросам кибербезопасности. Заказчики все чаще строят свои системы ИБ на базе решений безопасности одного вендора, что обеспечивает удобное управление всей системой и гарантирует простую и эффективную интеграцию отдельных продуктов. Данный аспект действительно имеет большую роль, поскольку практически все процессы требуют высокого уровня безопасности.

Большую роль в развитии кибербезопасности играет поддержка сферы информационных технологий со стороны государства. Правительство всячески помогает отечественным производителям в сфере информационных технологий стать независимыми от иностранных поставщиков, а также не дает произойти «утечке мозгов». Для осуществления такой политики было предпринято множество мер по поддержке ИТ-специалистов. Так в льготы для организаций входят – мораторий на проверки, отмена налога на прибыль, отмена проверок и налога на прибыль, упрощенная процедура найма иностранцев, гранты и льготные кредиты. Помощь же непосредственно для специалистов заключается в отсрочке от армии и сниженная ставка по ипотеке. Здесь важно отметить, что данные льготы будут действовать до 2024 года, а также для их получения компания должна быть аккредитована Министерством цифровой экономики России и специализироваться на разработке и внедрении ИТ-продуктов.

Также одной из перечисленных проблем являлась тенденция к милитаризации киберпространства. Это одна из основных и самых сложных проблем для любого государства, так как для ее решения необходимо прийти консенсусу обеих сторон. И здесь важно отметить, что в разгар гонки ядерных вооружений "гарантия взаимного уничтожения" обеспечивала мировое равновесие. На сегодняшний же день кибероружие играет ту же роль. Однако его относительно низкая стоимость значительно расширила список стран, обладающих современными средствами кибератак, а это в любой момент может привести к глобальной дестабилизации.

Россия вынуждена принимать меры по сдерживанию других стран в киберпространстве и поэтому участвует в кибервойне. Основным противником в этой области традиционно являются США и их союзники. Однако мы можем видеть, что наша страна неоднократно предпринимала меры по решению данной проблемы. Так, еще в марте 2017 года Россия предложила международную конвенцию по информационной безопасности, она была направлена на киберпреступников, которые нарушают цифровое пространство государств, ведут незаконную деятельность и подрывают суверенитет стран. Также в 2017 году Россия заключила двусторонние межправительственные соглашения по предотвращению эскалации компьютерных инцидентов с такими странами, как Китай, США, Индиея, ЮАР, Белоруссиея, Куба, также были намерения заключить такие договоры с ФРГ, Францией, Израилем, Южной Кореей и Японией.

В 2019 году ГА ООН приняла резолюцию России о разработке международной конвенции по борьбе с киберпреступностью, в поддержку данного документа высказались 79 государств, 60 проголосовали против, 33 страны воздержались. Основной направленностью документа являлось объединение усилий против общей проблемы, которая наносит триллионный ущерб не только отдельным странам или компаниям, но и всей мировой экономике, а также лично гражданам.

В 2021 году была озвучена позиция Российской Федерации касаемо темы кибероперации: «Мы сторонники равенства, порядка и взаимного уважения в информационной сфере, обеспечения её прогрессивного развития». Также важным тезисом выдвинутым нашим государством на Заседании Совета Федерации о том, что победить кибератаки на мировом уровне можно только объединив усилия, необходимо совместными усилиями разрабатывать и согласовывать универсальные и справедливые правила ответственного поведения государств в информационном пространстве с четкими и ясными критериями допустимых и недопустимых действий, а для обязательного характера разработать юридическую базу.

Переходя к 2022 году, важно начать с того, что около 90 процентов инфраструктуры государственного сектора Российской Федерации в той или иной степени подверглись кибератакам.

По данным Positive Technologies, количество кибератак значительно увеличивалось по сравнению с 2021 годом. Такой рост объясняется продолжающимся противостоянием в киберпространстве, появлением новых злоумышленников-шифровальщиков и обновлением существующих. Доля атак на компьютеры, серверы и сетевое оборудование организаций увеличилась на 6 процентных пунктов в результате активности шифровальщиков. Кроме того, отмечается рост числа массовых атак на 4% по сравнению с предыдущим кварталом.

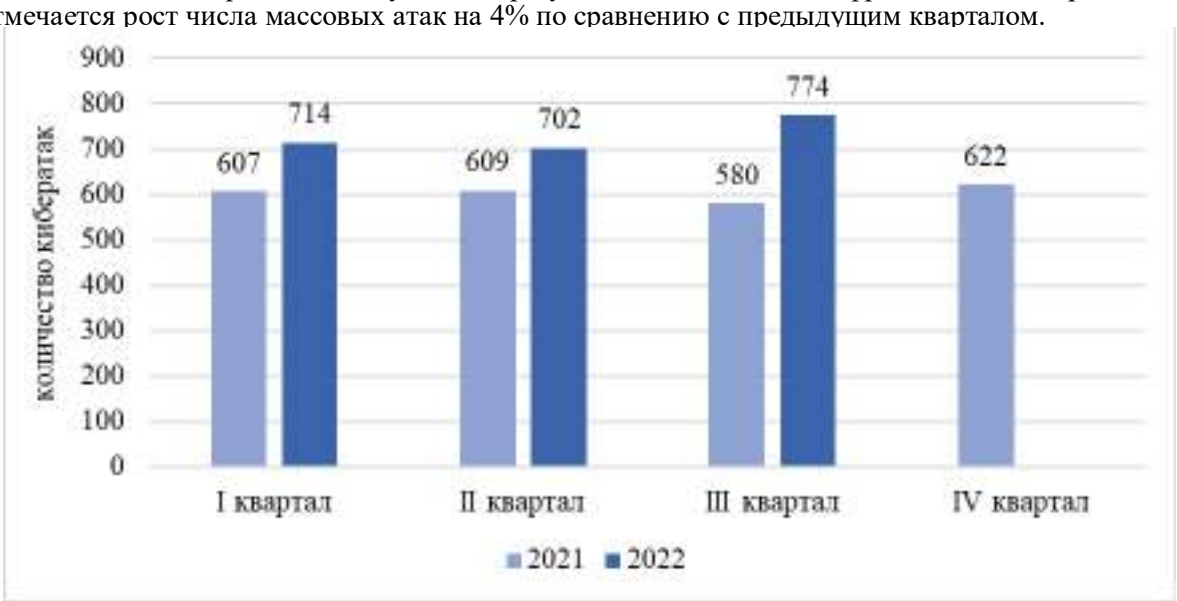

Рисунок 1 – Количество атак в 2021 и 2022 годах (по кварталам)

Несмотря на то, что количество атак заметно увеличилось, невозможно их обозначить иначе, как террористические акции в киберпространстве. Причина заключена в том, что нападавшие лица не изменились, изменения произошли только в их цели, а именно сейчас они работают не ради извлечения материальной выгоды, а на дестабилизацию инфраструктуры органов власти и бизнеса России.

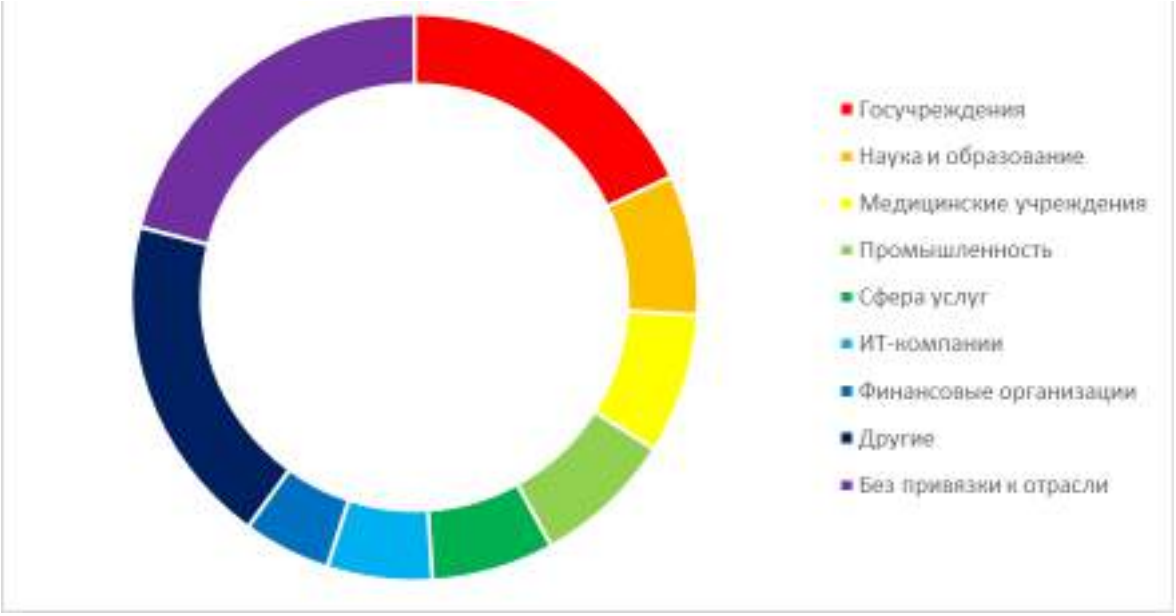

Рисунок 2 – Категории пострадавших организаций

Таким образом мы можем говорить о том, что после событий произошедших в 2022 году наступил момент, когда рынку кибербезопасности необходимо повернуться на 180 градусов и переосмыслить фундаментальные принципы построения защиты и реагирования на угрозы в масштабах бизнеса, отрасли и страны. В 2023 году индустрия информационной безопасности будет переживать период активной пересборки с большим упором на практику эффективной защиты.

В последующих годах экономика Российской федерации будет переживать глобальные изменения, так как приоритетом будет политика протекционизма, а отечественные производители укоренят свои места во всех сферах. Рынок кибербезопасности ждет таже участь, уже сейчас растет спрос на российские технологи, способные предотвратить хакерские атаки до того, как компаниям будет нанесен непоправимый ущерб. На данный момент компании разных направленностей, в том числе и государственные учреждения, уделяют должное внимание практическому кибер-обучению и средствам защиты с максимальной автоматизацией для обнаружения и противодействия хакерским атакам.

Как раннее было сказано, ближайшие годы будут расцветом отечественных технологий, так как именно сейчас появился стимул для развития во всех сферах. По мнению экспертов, мы увидим обновления в линейках продуктов NGFW, контейнерной и облачной защиты.

Литература

1. Указ Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ» // СПС «КонсультантПлюс».
2. Positive Technologies — российская компания, специализирующаяся на разработке решений в сфере информационной безопасности. – URL: https://www.ptsecurity.com/ru-ru/ [Электронный ресурс] (дата обращения: 07.02.2023).
3. Англо-русский словарь Мюллера. - URL: https://gufo.me/dict/enru_muller [Электронный ресурс] (дата обращения: 07.02.2023).
4. TADviser – информационно-новостной портал, специализирующийся в основном на IT-рынке. – URL: https://www.tadviser.ru/?ysclid=le09k8e4px805955215 [Электронный ресурс] (дата обращения: 07.02.2023).
5. Лаборотория Касперского - Международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих киберугроз. - URL: https://www.kaspersky.ru [Электронный ресурс] (дата обращения: 07.02.2023).
6. Заседание совета безопасности. - URL: http://www.kremlin.ru/events/president/news/65231 [Электронный ресурс] (дата обращения: 07.02.2023).

УДК 330

Бакуменко Мария Александровна
к.э.н., доцент
Физико-технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

О ВОЗМОЖНОСТЯХ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Исследование выполнено за счет гранта Российского научного фонда № 23-28-00127, https://rscf.ru/project/23-28-00127/

10 октября 2019 г. Указом Президента Российской Федерации № 490 была утверждена «Национальная стратегия развития искусственного интеллекта на период до 2030 года» [1] (далее Стратегия). Это событие на законодательном уровне закрепило высокую значимость использования технологий искусственного интеллекта для социально-экономического развития Российской Федерации. Отметим, во многих странах подобные документы были разработаны и утверждены ранее, что, в частности, дало им некоторые конкурентные преимущества на современном этапе развития.

Как предполагает Стратегия, к 2024 г. Россия должна существенно улучшить уровень развитости отечественных достижений в сфере искусственного интеллекта, а к 2030 г. – стать лидером в отдельных направлениях, связанных с технологиями искусственного интеллекта.

Существенное внимание Правительства РФ к анализируемым технологиям обусловлено их значительным влиянием на уровень конкурентоспособности национальной экономики. Как отмечено в работе [2], «отставание в сфере развития искусственного интеллекта грозит в перспективе экономическим отставанием» [2, с. 14]. Данные технологии могут найти эффективное применение практически во всех сферах жизнедеятельности человека, в том числе и в сфере здравоохранения.

Система здравоохранения является, с одной стороны, одной из важнейших социально-значимых отраслей экономики РФ, а, с другой стороны, важным поддерживающим звеном отечественной экономики. Здоровье нации оказывает влияние на состояние социально-экономической системы. Как показала недавняя пандемия COVID-19, эпидемии могут наносить существенный ущерб экономическому развитию страны, препятствовать экономическому росту, при этом плохо поддаются прогнозированию. Как показано в работе [3], здоровье населения является одним из факторов, формирующих конкурентоспособность экономики, при этом уровень здравоохранения страны можно рассматривать как один из важнейших показателей экономического развития.

Как отмечают эксперты Организации экономического сотрудничества и развития, в ближайшем будущем можно ожидать расширение применения технологий искусственного интеллекта в системе здравоохранения [4, с. 58].

Можно перечислить ряд технологий искусственного интеллекта, которые уже нашли применение в системах здравоохранения ряда стран, и в дальнейшем, очень может быть, их использование будет расширяться [5, с. 91-93]:

- робототехника (например, проведение операций роботизированными системами, уход роботов за лежачими пациентами);
- автоматизированные диагностические системы (технологии искусственного интеллекта позволяют уточнить диагноз заболеваний);
- системы для прогнозирования событий (например, в процессе планирования выпуска и закупки лекарственных препаратов на государственном уровне);
- системы распознавания речи (например, сервис медицинского писца, который позволяет значительно сэкономить временные ресурсы врача, затрачиваемые на ведение документации);
- системы автоматической классификации и сверки информации (могут быть применены в процессе оценки качества работы системы здравоохранения на уровне определенного региона);
- чат-боты (поддержка пациентов во время реабилитации, уменьшение необходимости в консультационной помощи врача).

Перечисленные выше направления развития технологий искусственного интеллекта могут быть применены и в нашей стране. Желательно, разрабатывать свои системы, а не пользоваться зарубежными разработками. Создание подобных систем требует значительных финансовых затрат, но эти затраты могут окупиться. Как показала мировая практика, реализация инновационных проектов по внедрению технологий искусственного интеллекта в медицине может быть высокоприбыльным бизнесом и, что существенно важнее, может позволить

добиться желаемых изменений в доступности и качестве медицинской помощи. Ведь в нашей стране есть все условия (в том числе высококвалифицированные кадры) для создания подобных систем, а рынок России является достаточно емким. Наконец, созданные интеллектуальные информационные системы можно будет экспортировать за рубеж.

Следует отметить, что применение технологий искусственного интеллекта не должно рассматриваться как полная замена труда врача. Эти технологии должны, в первую очередь, быть направлены на повышение качества функционирования системы здравоохранения, в целом, отдельных медицинских учреждений, а также на облегчение труда врачей и других медицинских работников, на повышение качества диагностики, а также на снижение медицинских ошибок. Всегда следует помнить о возможных рисках и угрозах, связанных с применением технологий искусственного интеллекта, и оставлять принятие решения за человеком-врачом. В настоящее время уровень «здравого смысла» самого мощного в мире суперкомпьютера сопоставим с уровнем интеллектуального развития четырехлетнего ребенка. Поэтому о полной замене труда врача искусственными системами не приходится говорить.

Литература

1. Указ Президента РФ от 10.10.2019 N 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года"). – URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (Дата обращения: 10.02.2023 г.).
2. Бакуменко М. А. О развитии искусственного интеллекта в Российской Федерации / М. А. Бакуменко // Эффективное управление экономикой: проблемы и перспективы: сборник трудов VI Всероссийской научно-практической конференции, г. Симферополь, 15–16 апреля 2021 г. / научн. ред. В. М. Ячменевой; редкол.: И. М. Пожарицкая, Р. А. Тимаев, Т. И. Воробец. – Симферополь: ИТ «АРИАЛ», 2021. – С. 11-15.
3. Sigal A. V. The level of the country's health care as an indicator of its economic development / A. V. Sigal, M. A. Bakumenko // Proceedings of the International scientific conference "FAREASTCON" (ISCFEC 2020). Advances in Economics, Business and Management Research. Val. 128. – Vladivostok, 2020. DOI: 10.2991/aebmr.k.200312.151.
4. Смирнов Е. Н. Формирование и развитие глобального рынка систем искусственного интеллекта / Е. Н. Смирнов, С. А. Лукьянов // Экономика региона. – 2019. – Т. 15, вып. 1. – С. 57–69.
5. Гусев А. В. Искусственный интеллект в медицине и здравоохранении / А. В. Гусев, Добриднюк С. Л. // Информационное общество. – 2017. – № 4-5. – С. 78-93.

УДК 330

Бакуменко Мария Александровна
к.э.н., доцент
Шульман Михаил Станиславович
обучающийся
Физико-технический институт
ФГАОУ ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АГРАРНОМ СЕКТОРЕ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аграрный сектор экономики Российской Федерации (РФ) всегда требовал поддержки со стороны государства и являлся приоритетной отраслью экономики. Российская Федерация должна самостоятельно обеспечивать внутренние потребности страны в качественных и натуральных продуктах питания (без ГМО). В свою очередь, сельское хозяйство не является высокоприбыльной отраслью и зачастую обусловлено существованием многочисленных рисков и неопределенности. Так, например, рентабельность отечественного сельскохозяйственного производства в 2022 г. составила 21 % (с учетом субсидий), или 17,7 % без учета субсидий [1].

Повышение рентабельности аграрного сектора экономики Российской Федерации возможно благодаря применению современных инновационных технологий, в том числе технологий искусственного интеллекта.

Технологии искусственного интеллекта с каждым годом становятся все более востребованными в различных секторах экономики. Развитию данных технологий в настоящее время Правительство РФ уделяет пристальное внимание. Так, в частности, в 2019 г. была утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года. Реализация этой стратегии должна укрепить позиции России в сфере развития и применения технологий искусственного интеллекта в экономической сфере.

Развивая технологии искусственного интеллекта, в первую очередь, необходимо сконцентрировать внимание на реальном секторе экономики, в том числе на аграрном комплексе страны. Поскольку внедрение технологий искусственного интеллекта, как правило, приводит к

снижению издержек и повышению качества продукции, а, следовательно, способствует повышению конкурентоспособности отечественного производителя.

В аграрном секторе экономики можно выделить следующие возможные направления применения технологий искусственного интеллекта [3]:

- робототехнические системы (автоматизация сбора урожая, борьба с сорняками);
- мониторинг урожая и качества почвенного покрова и предоставление фермерам рекомендаций по улучшению ситуации;
- прогнозирование осадков, температур, стихийных бедствий и т.п.;
- автоматизация процесса слежения за животными и контроль состояния их здоровья.

Развитие технологий искусственного интеллекта называют «…одним из значимых факторов повышения конкурентоспособности национальной экономики» [4, с. 14].

Применение технологий искусственного интеллекта в аграрном секторе экономики должно привести к возникновению следующих положительных эффектов:

- снижению издержек производства;
- повышению качества продукции;
- повышению рентабельности производства;
- снижению рисков и уровня неопределенности;
- повышению управляемости и прогнозируемости протекающих экономических процессов;
- росту оплаты труда в аграрном секторе экономики;
- повышению привлекательности сельского труда и, соответственно, уменьшению оттока молодежи из сельской местности.

Разрабатывая интеллектуальные информационные системы для аграрного сектора экономики не стоит забывать и про риски, которые могут быть обусловлены внедрением данных технологий.

Литература

1. Рентабельность сельхозпроизводства в РФ в 2022 г. с учетом субсидий составит 21% против 25,6% в 2021 г. – URL: https://agrarnayanauka.ru (дата обращения: 10.02.2023).
2. Указ Президента РФ от 10.10.2019 N 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года"). – URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 10.02.2023 г.).
3. Бакуменко М. А. О применении технологий искусственного интеллекта в агропромышленном комплексе / М. А. Бакуменко, Д. А. Петрушин // Тенденции развития Интернет и цифровой экономики / Труды V Всероссийской с международным участием научно-практической конференции. Под ред. проф. Н. В. Апатовой. Симферополь-Алушта, 2–4 июня 2022 год. – Симферополь: Издательский дом КФУ, 2022. – С. 127-128.
4. Бакуменко М. А. О развитии искусственного интеллекта в Российской Федерации / М. А. Бакуменко // Эффективное управление экономикой: проблемы и перспективы: сборник трудов VI Всероссийской научно-практической конференции, г. Симферополь, 15–16 апреля 2021 г. / научн. ред. В. М. Ячменевой; редкол.: И. М. Пожарицкая, Р. А. Тимаев, Т. И. Воробец. – Симферополь: ИТ «АРИАЛ», 2021. – С. 11-15.

УДК 658.51

Глухий Екатерина Николаевна
обучающаяся
Научный руководитель:
Штофер Геннадий Аркадьевич
доцент кафедры экономики предприятия, к.э.н., доцент
Институт экономики и управления
ФГАОУ ВО «КФУ им. В.И. Вернадского»
Республика Крым, Россия

ВЛИЯНИЕ ИННОВАЦИЙ НА ЭФФЕКТИВНОСТЬ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Инновации играют ведущую роль в организации эффективной деятельности предприятия, поскольку в современных реалиях без инноваций бизнес не сможет эффективно функционировать и обеспечивать стратегическое развитие. Однако просто ввести инновации в деятельность предприятия недостаточно, они должны быть качественными и грамотными и за счет этого приносить предприятию наибольший полезный эффект (увеличение прибыли, количество клиентов и уровень престижа компании). Это именно то, на что предприятию необходимо выделять материальные средства, чтобы получить выгоду в долгосрочной перспективе.

Инновации в современном мире можно трактовать как что-либо новое, которое принесет полезный эффект. Однако если трактовать понятие инноваций применительно к предприятию,

то это форма проявления научно-технического прогресса на микроуровне, именно инновации помогают обновлению номенклатуры выпускаемой продукции, а также повышению ее качества в целях удовлетворения потребностей клиентов и увеличению прибыли на предприятии.

Рассмотрим виды инноваций и их конкретные характеристики (таблица 1).

Основной стимул ведения инновационной деятельности на современных предприятиях – моральный износ выпускаемых товаров или устаревшие способы оказания услуг. Для того чтобы выявить продукцию, выпуск которой уже не актуален при существующем уровне технического прогресса в мире, на предприятиях следует периодически проводить специальную проверку. На основе проведённой работы руководители организации пытаются найти способы самостоятельно перевести свою продукцию или услуги в разряд устаревших, не дожидаясь момента, когда к этому придут конкуренты. Такой анализ определяет приоритеты компании в области новаторства.

Таблица 1 – Виды инноваций применительно к предприятию

Вид инновации	Характеристика
Инновации на входе в предприятие	Изменения в выборе и использовании сырья, материалов, машин и оборудования, информации и др.
Инновации на выходе с предприятия	Изделия, услуги, технологии, информация и др.
Инновации системной структуры предприятия	Управленческой, производственной, технологической
Радикальные	Создание чего-либо еще не существующего, что-либо новое и запатентованное
Улучшающие	Дополняют и усиливают текущие инновации
Модификационные	Инновации, представляющие собой существенные изменения (усовершенствования) базисных нововведений

Источник: [Составлено авторами].

При поиске и внедрении инноваций предприятию целесообразно оценивать эффективность предлагаемых мер, соотнося выгоды от инновационной деятельности с затратами на ее проведение. В результате, может быть рассчитана социально-экономическая эффективность [1] на уровне предприятия от внедрения инноваций рассчитывается по формуле (1):

$$Э_{абс} = Д_{чп} / К_{нт} \text{ , где} \quad (1)$$

$Э_{абс}$ – абсолютная эффективность;
$Д_{чп}$ – прирост чистой продукции;
$К_{нт}$ – затраты на внедрение инноваций.

При этом срок окупаемости (возврата) капитальных затрат на инновации определяется по формуле (2):

$$Т_{ОК} = \sum \frac{П}{К_{НТ}}, \text{ где} \quad (2)$$

$Т_{ОК}$ - срок окупаемости (возврата) капитальных затрат на инновации;
П – прибыль;
$К_{нт}$ – затраты на внедрение инноваций.

Прирост прибыли в результате внедрения инноваций рассчитывают по формуле:

$$П=(Ц_2-С_2)*А_2-(Ц_1-С_1)*А_1 \text{ , где} \quad (3)$$

$А_1$ – количество изделий;
$Ц_1$ – цена до внедрения инноваций;
С1 – себестоимость;
$А_2$,$Ц_2$,$С_2$ - …после внедрения инновация.

При этом устанавливается влияние различных факторов на прибыль. В свою очередь, инновации обеспечивают прирост прибыли за счёт двух факторов:

— путем снижения себестоимости (снижения удельных расходов заработной платы, материальных затрат, за счёт снижения страховых платежей на единицу продукции, за счёт изменения амортизационных платежей);

— путем повышения качества продукции (надбавки к оптовой цене, и увеличение объёмов продаж).

Реализация инновационного развития фирмы требует от руководителя создания рабочей атмосферы, обеспечивающей выполнение следующих условий:

1. Новаторские проекты требуется воспринимать не как угрозу, а как новые перспективы развития.

2. Создание нового проекта направлено на сохранение и укрепление предприятия.

3. Выделение средств на развитие новых проектов выступает своеобразным гарантом благополучия каждого сотрудника.

Стоит отметить, что инновации на предприятии необходимо не только внедрить, но и затем постоянно совершенствовать. Произвести оценку новизны инноваций можно путем оценивания технологических параметров, а также с учетом рыночных позиций. Очевидно, что, развиваясь на инновационной основе, предприятие будет совершенствовать свою производственную базу, систему материально-технического обеспечения, оптимизировать структуру сбыта продукции, адаптируя их к изменениям во внешней среде. Одновременно с этим неизбежно будет происходить перестройка организационной структуры управления, меняться компетенции работников всех уровней и руководителей, будет модернизирована система взаимодействия с бизнес-партнерами, будет укрепляться деловая репутация предприятия.

Таким образом, что результаты деятельности инновационно-активных компаний способствуют не только экономическому росту, но и социальному развитию. Это влияние происходит через их воздействие на внешнюю среду (потребители, местное сообщество и население в целом, бизнес-партнеры и др.), а также через формирование специфической инновационно-ориентированной организационной культуры, что приводит к изменению понимания целей и инструментов обеспечения социального, инновационного и экономического развития персонала.

Литература

1. Балдин, К. В. Инвестиции в инновации / К.В. Балдин, И.И. Передеряев, Р.С. Голов. – М.: Дашков и Ко, 2016. – 238 с.
2. Вилисов, В.Я. Инфраструктура инноваций и малые предприятия: состояние, оценки, моделирование: Монография / В.Я. Вилисов. – М.: РИОР, 2017. – 587 с.
3. Волкова, В. Н. Информационные модели и автоматизированные процедуры для управления инновациями / В.Н. Волкова. – М.: Синергия, 2015. – 762 с.
4. Кермадек, Ян. Инновации на предприятии – это общее дело! / Ян Кермадек. – М.: Претекст, 2018. – 434 с.
5. Курчеева, Г. И. Инновационный маркетинг и маркетинг инноваций в системе конкурентных преимуществ фирмы / Г.И. Курчеева. – М.: Синергия, 2019. – 786 с.
6. Философова, Т. Г. Конкуренция. Инновации. Конкурентоспособность / Т.Г. Философова, В.А. Быков. – М.: Юнити-Дана, 2014. – 296 с.
7. Штофер, Г. А. Определение инновационной активности предприятий России при прогнозировании стратегических изменений / Г. А. Штофер, А. А. Гайсарова, А. О. Юдина // Экономика строительства и природопользования. – 2021. – № 3(80). – С. 88-95. – DOI 10.37279/2519-4453-2021-3-88-95. – EDN ERGDPB.
8. Штофер, Г. А. Система показателей и порядок оценки эффективности инвестиционной деятельности предприятия / Г. А. Штофер // Экономика строительства и природопользования. – 2019. – № 1(70). – С. 75-82. – EDN SRIGIB.

УДК 004.62

Гончаров Артём Максимович
обучающийся
Научный руководитель:
Гончарова О. Н.
д.п.н., профессор
Физико-технический институт
ФГАО ВО «КФУ имени В.И. Вернадского»
Республика Крым, Россия

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ МЕНЕДЖМЕНТА ПОЛЬЗОВАТЕЛЬСКИХ КЛЮЧЕЙ И ПАРОЛЕЙ

В настоящее время наблюдается тенденция к цифровизации услуг и сервисов. В облачные системы уже перенесены или находятся в процессе переноса ключевые и жизненно необходимые сервисы. Такими сервисами являются, например, приложения хранения и управления юридическими документами и банковские личные кабинеты. В этих условиях механизм аутентификации пользователя получает особую важность, так как необходимо обеспечить его максимальную, асимптотически близкую к абсолютной, надёжность и предотвратить допуск злоумышленников к этапу авторизации в системе сервиса. Потенциальными последствиями некорректного прохождения аутентификации могут быть потеря средств или имущества.

Исторически, при разработке первых электронных приложений, поддерживающих пользовательские аккаунты, за основной способ аутентификации был принят пароль. С течением времени для предотвращения атак по подбору паролей требования по сложности новосоздаваемых паролей постоянно повышались. Однако, пользователи склонны к созданию паролей минимально возможной сложности, их одновременному использованию в различных сервисах и забыванию. Системы менеджмента паролей решают проблему, обеспечивая генерацию, хранение и, обычно, шифрование паролей. Тем не менее, злоумышленник, получивший доступ к устройству пользователя, может извлечь все пароли, хранящиеся в менеджере. Для этого необходимо будет пройти системную аутентификацию или аутентификацию менеджера. Это, в свою очередь, ведёт к возвращению к исходной проблеме. Вышесказанное также справедливо для хранения закрытых криптографических ключей.

Частичное решение проблемы добавлением двухфакторной аутентификации недостаточно, так как потеря, например, смартфона, даёт злоумышленнику доступ к её основным методам. Перспективным развитием системы менеджмента паролей и ключей являются аппаратные ключи безопасности. Они выполняют те же функции, но при этом физически отделены от устройств пользователя, автономны, переносимы и не подвержены программным атакам через пользовательские устройства. Тем не менее, ключ может быть утерян или украден, что даст злоумышленнику возможность свободно использовать его. Эта проблема не входит конкретно в сферу компьютерной безопасности, но всё же требует внимания.

Биометрические данные человека являются его составляющей, а, следовательно, не могут быть утеряны. Более того, каждый ввод таких данных отличается от любого другого, так как производится биологическим генератором случайных значений. Это исключает возможность повторного использования перехваченных данных. Результат валидации данных получается не проверкой на совпадение с конкретным оригиналом, а с помощью программной модели. Таким образом, централизированный облачный сервис аутентификации с помощью биометрических данных, получающий ввод с клиентских устройств, является перспективным и надёжным методом, исключающий необходимость в менеджерах паролей и ключей в целом.

УДК 331.108 : 004

Круликовский Анатолий Петрович
к.ф.-м.н., доцент
Буренин Иван Семенович
обучающийся
Физико-технический институт
ФГАОУ ВО «КФУ им. В. И. Вернадского»
Республика Крым, Россия

ПЕРСПЕКТИВЫ РАЗВИТИЯ HR В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Цифровая экономика формирует новую общественную полезность, новое мышление, новые ценности, новую структуру мировой экономики и новые перспективы развития деятельности менеджеров по управлению персоналом.

Технологии искусственного интеллекта будут играть важную роль в помощи HR-менеджерам по управлению персоналом в отборе и подборе персонала в удаленном режиме, осуществлении тщательной проверки кандидатов, проведении собеседования, найме и управлении работниками в процессе трудовой деятельности, в оказании помощи сотрудникам при повышении их квалификации. Цифровые технологии могут помочь проанализировать резюме и выполнить оценку кандидатов на вакантную должность, обнаружив наиболее подходящих кандидатов, используя методы машинного обучения, которые выходят далеко за рамки простого сопоставления ключевых слов.

Будущее рабочих мест будет различаться по отраслям и секторам под влиянием начальных исходных условий, связанных с распределением задач, различными инвестициями во внедрении технологий, а также наличием навыков и возможностью адаптироваться к изменяющимся условиям. Быстрое внедрение новых технологий потребителями, а также достижения в области облачных технологий стимулировали рост отрасли информационных и коммуникационных технологий. Доступность больших данных, как ожидалось, оказало еще более широкое влияние на финансовые услуги и инвесторов, а также на энергетику, коммунальные услуги и технологии. Разные отрасли испытывают различия в составе и характере новых профессий, спрос на которые должен снижаться.

По словам Дэна Шавбела, директора по исследованиям в FutureWorkplace: «Лучшие таланты не хотят работать в компании, которая не является современной и ориентированной на

инновации. Талантливым людям, даже если они не занимаются техническими вопросами, нужен доступ к передовым инструментам» [1].

Среди тенденций, определивших рост в различных отраслях в период 2018–2022 годов, достижения в области мобильного интернета, оказали заметное влияние на индустрию авиации, путешествий и туризма, финансовых услуг и инвесторов, а также на потребительскую промышленность. Новые источники энергии и технологии в сочетании с достижениями в области вычислительной мощности должны способствовать росту сектора энергетических коммунальных услуг и технологий. Среди нетехнологических факторов роста бизнеса увеличение благосостояния в развивающихся странах может стимулировать рост в авиации, путешествиях и туризме.

После распространения в 2020 году вируса по всему миру и глобальной рецессии в мировой экономике, продажи Apple выросли на 11%. Это произошло благодаря лояльным пользователям продукции компании, которые были готовы покупать гаджеты через интернет. Общая сумма капитализации четырех главных высокотехнологичных компаний США, включая Apple, Amazon , Microsoft и Alphabet, к концу 2020 года уже превысила 6 трлн. Долларов [1].

Анализируя бизнес-процессы современных предприятий, была выявлена потребность в цифровизации процессов путем внедрения искусственного интеллекта, для улучшения эффективности работы предприятия, а именно имплементации искусственного интеллекта (Al - Artificial intelligence) для поиска и отбора персонала, анализа деятельности персонала и прогнозирования возможных рисков.

Технологии искусственного интеллекта дают значительные возможности для улучшения всех функций HR. Использование технологии с элементами искусственного интеллекта в системе управления персоналом возможно с позиций: создание виртуальных отделов по управлению персоналом, рекрутеров-ботов; анализ показателей деятельности работников с указанием его производительности для каждого работника; рост ценности развития «мягких» навыков работников (лидерство, эмоциональный интеллект, работа в команде, креативность и т.п.). Искусственный интеллект позволит быстро анализировать данные и показатели деятельности работников компании, создавая отчет об использовании труда персонала на предприятии [2]. В случае, когда показатели будут отклоняться от нормы, система автоматически предупредит возможные угрозы, их причины и пути преодоления. Таким образом, будет уменьшена нагрузка на управляющее звено, а также значительно снизится риск человеческого фактора.

В управлении персоналом искусственный интеллект позволит значительно снизить время на поиск новых работников и проверку их профессионального соответствия требованиям на предприятии. Сокращение времени на анализ информации и контроля деятельности персонала с помощью цифровизации и Al позволит сократить затраты на оплату труда, оптимизировать рабочую площадь, сократить расходы на оплату коммунальных услуг. Таким образом, цифровизация бизнес-процессов управления персоналом и анализа информации приведет к увеличению рентабельности и прибыли. Целью усовершенствования бизнес-процессов является цифровизация управления персонала посредством создания ценности от использования новых, прогрессивных технологий с помощью цифровой сетевой динамики и гигантского цифрового потока информации, в частности с использованием искусственного интеллекта. В работе Позмогова А.И. [3] показано, что Искусственный Интеллект позволяет компьютерам учиться на собственном опыте, адаптироваться к заданным параметрам, анализировать большие объемы информации и выявлять закономерности, обрабатывать естественный язык. Благодаря этому, технологическую линию производства можно «научить» выполнять определенные задачи по алгоритмам, которые будут самосовершенствоваться с помощью нейронной сети. Реализация идеи обеспечит большую экономию времени по сравнению с существующими процедурами и гарантирует высокую точность контроля всего персонала предприятия.

Таким образом, цифровая эра открыла радикально новые возможности для развития новых видов бизнеса, создала условия для творческого развития человеческого капитала. Влияние современных цифровых технологий существенно меняет трудовую деятельность людей, условия организации, оплаты, социальной защиты труда, которые трансформируются и приобретают индивидуальный характер. Уменьшается зависимость работников от работодателей, их труд перемещается в цифровое пространство, что требует постоянного обновления знаний и навыков работы с современными технологиями. Знания, креативность, интеллект и инновации становятся ценными ресурсами цифровой эпохи. Основными средствами труда становятся цифровые устройства, предметом труда - информация.

Литература

1. Бодяко, А.В. Проблемы развития методологии учета и контроля в условиях институциональной экономики инновационного типа. Том 3. О перспективах «цифрового формата» учета, контроля и отчетности / А.В. Бодяко. - М.: Русайнс, 2020. - 609 с.

2. Быков, А.Ю. Система нормативно-правовой базы цифровой экономики в Российской Федерации / А.Ю. Быков. - М.: Проспект, 2022. - 724 с.

3. Цифровая трансформация российского бизнеса: монография / под ред. А.И. Позмогова. - Москва: Русайнс, 2019. - 456 с.

Остапенко Ирина Николаевна
к.э.н., доцент
Шульман Михаил Станиславович
обучающийся
ФТИ ФГАОУ ВО "КФУ им. В.И. Вернадского"
Республика Крым, Россия

К ВОПРОСУ АВТОМАТИЗАЦИИ ДЕЯТЕЛЬНОСТИ ВУЗА

Приоритет современного вуза – цифровизация внутренних и внешних процессов для оптимизации использования электронной продукции [1]. Интересен опыт Санкт-Петербургского государственного института психологии и социальной работы по созданию учебного портала на базе «1С-БИТРИКС: КОРПОРАТИВНЫЙ ПОРТАЛ».

Выбор образовательной траектории.
Студенты создают заявку в личном кабинете на Учебном портале. Запускаемый при этом бизнес-процесс помогает согласовать индивидуальные программы обучения с учетом возможностей преподавателей: максимального количества студентов, которых они могут взять к себе в группу.

Модуль расписания предметов, зачетов, экзаменов и практики.
У студентов индивидуальные расписания, любые изменения сообщаются своевременной email- и СМС - рассылки.

Загрузка и проверка самостоятельных, научно-практических и выпускных квалификационных работ.
Студенты согласовывают с преподавателями темы контрольных, курсовых, дипломных работ, отправляют готовые работы на проверку, обсуждают замечания преподавателей, получают оценки и допуски к следующим этапам обучения.
Преподаватель может оставить комментарий, информация о котором поступает студенту через уведомления на портале и СМС.

Функционал «Мои оценки».
Позволяет каждому обучающемуся увидеть результаты его учебной деятельности.

Коммуникации. Рабочие области дисциплин.
Для каждой дисциплины и практики на Учебном портале создаются специальные виртуальные группы - Рабочие области дисциплин, в которых можно для всех участников группы: написать вопрос или сообщение; обсудить учебный материал или разместить файлы по дисциплине; просмотреть размещенную преподавателем учебную документацию, задания для самостоятельной работы, слайды и др.

Чат для общения.
Однокурсники, преподаватели или методисты могут использовать встроенный чат для общения.

Система нотификаций.
Через email, портал и СМС происходят напоминания по выбору и сдаче дисциплин, проверке работ, изменениях в расписании.

Интеграции.
Интеграция с Active Directory. Личные данные новых студентов заносятся в Active Directory. В соответствии с выбранной траекторией обучения аккаунты распределяются по учебным группам, которые автоматически генерирует система.
Интеграция с ERP-системой «Галактика» обеспечивает отображение на портале данные об оценках, действующих договорах, персональных приказах, предоставляет возможность оформлять заявки различных категорий в администрацию ВУЗа.
Интеграция с системой «Антиплагиат».
Когда студент загружает свою работу на портал, выполняется автоматическая проверка обнаружения текстовых заимствований благодаря интеграции через API с российской интернет-системой «Антиплагиат». В личном кабинете преподавателя рядом с каждой работой отображается % уникальности сданной работы.

Рисунок 1 – Учебный портал на базе «1С-БИТРИКС: КОРПОРАТИВНЫЙ ПОРТАЛ»

Удобная и функциональная система, внедрённая в СпбГИПСР - официальный инструмент коммуникаций, формирования ряда важных документов, развивается и постоянно совершенствуется, оптимизирует работу всех участников учебного процесса, устраняет рутинные формы работы, освобождая время сотрудников и студентов для научного творчества. По мнению ректора СпбГИПСР Юрия Петровича Платонова, процесс внедрения очень сложный и требует много усилий, однако им удалось автоматизировать большое количество рабочих процессов.

Литература

1. Цифровизация образовательных процессов в ВУЗах/ Н.М. Тюкавкин/ ЭКСПЕРТ: ТЕОРИЯ И ПРАКТИКА 2019. № 1 (1). - URL: file:///C:/Users/Пользователь/Downloads/tsifrovizatsiya-obrazovatelnyh-protsessov-v-vuzah.pdf
2. Внедрение Битрикс24 в СПбГИПСР. - URL: https://club.cnews.ru/blogs/entry/vnedrenie_ bitriks24_v_spbgipsr

УДК 004 : 330

Попов В. Б.
к.ф.-м.н., доцент
Ляшко А. А.
обучающийся
Физико-технический институт
КФУ им. В.И. Вернадского
Симферополь, Россия

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ WEB-РЕСУРСОВ

Актуальность и цель исследования. Одной из важнейших составляющих современного цифрового мира является информационная безопасность. Исследование касается вопросов архитектуры и классификации существующих приложений по информационной безопасности и устойчивости, использующих технологии глубокого машинного обучения, предиктивной аналитики и поведенческого анализа, которые в настоящее время обозначают общим термином «Технологии Искусственного Интеллекта (AI)». IT-специалисты в области защиты информации, отмечают что трендом наступившего года является увеличение атак на организации со стороны мотивированных хакеров. Данная тенденция будет продолжаться пока международная обстановка остается нестабильной. Единственное изменение, которое заметно уже сейчас, заключается в том, что сложность таких атак начинает расти. Если все начиналось с простейших ddos-атак, в которых участвовали и обычные пользователи, то сейчас активность хакеров приобретает более сложный интеллектуальный характер.

Информационная безопасность – это одна из важнейших составляющих современного цифрового мира. Технологии искусственного интеллекта (AI) и машинного обучения (ML) дают возможность создавать новые методы надежной защиты, при этом вся кибербезопасность становится безрисковой [1, 2, 3].

Основные методы улучшения кибербезопасности при помощи машинного обучения и искусственного интеллекта следующие.

- Искусственный интеллект используется для классификации, обработки, кластеризации и фильтрации поступающей информации, поскольку существует достаточное число информационных данных в данной предметной области.
- Машинное обучение дает возможность анализировать прошлую информацию, предоставлять оптимальные методы решения для будущего и настоящего. При помощи прошлых данных алгоритмы обеспечивают инструкциями, позволяющие найти угрозы или вредоносные приложения. Технологии искусственного интеллекта (AI) и Машинного обучения (ML) помогают нарушать работу любого, кто захочет проникнуть в систему.
- Внедрение технологий систематизирует информацию по заданным параметрам, позволяя сопоставлять разную информацию, отслеживать любые угрозы.
- Искусственный интеллект упрощает ведение аудита способов защиты информации, что дает возможность быстро узнать об эффективности внедрения ограничений. Это защищает пользователей компании.
- Технологии искусственного интеллекта (AI) и Машинного обучения (ML) быстро находит угрозы, вредоносное программное обеспечение создавая платформу безопасности для сканирования крупных информационных объемов.

При помощи искусственного интеллекта предприятия усиливают методы миграции в облако, улучшается производительность при большом количестве данных.

Тенденции развития информационных технологий говорят о том, что в 2023 году сохранится уверенный рост интеллектуальных приложений. Об этом свидетельствуют результаты исследований ведущих аналитических компаний, таких как IDC, Gartner и TrendForce.

Еще одним современным трендом является дальнейшее совершенствование глубокого обучения технологий искусственного интеллекта. В настоящее время глубокое обучение используется в различных отраслях для таких задач, как прогнозирование будущего экономических объектов, прогнозирование погодных условий, выявление ложных страховых случаев, в медицинских приложениях и др. Широко используется в том числе и для обеспечения кибербезопасности. В этой области работают, например, компании Deep Instinct и Alotros, которые используют глубокое обучение не только для выявления новых, но и для ранее не обнаруженных угроз. Они собирают данные и запускают тестирование для классификации файлов как вредоносных. На основе этого ИИ делает прогнозы. Deep Instinct показывает наиболее точный прогноз в 99,8%.

Выводы. Анализ состояния приложений на основе технологий искусственного интеллекта в информационной безопасности позволяет сделать следующие выводы.

- Искусственный интеллект вносит заметный вклад в борьбу с современными информационными угрозами. В частности, в большинстве случаев внедрение технологий искусственного интеллекта в поддержку информационной безопасности организации сокращает время выявления проблем и реагирования на инциденты, а также уменьшает расходы на управление персоналом.
- Пользователи отмечают значительный рост эффективности в детектировании вредоносных неизвестных угроз.
- Использование рассматриваемых технологий влияет также на скорость анализа и обнаружения вредоносной активности на конечных точках и в приложениях.
- Суммарные инвестиции в компаниях, которые создают продукты по информационной безопасности с применением технологий искусственного интеллекта, составляют $4000 млн на конец 2022 года (данные из Интернет). При этом мировой рынок продуктов по информационной безопасности с применением технологий искусственного интеллекта достигнет $30 млрд в 2025 году с ежегодным ростом на 23%.

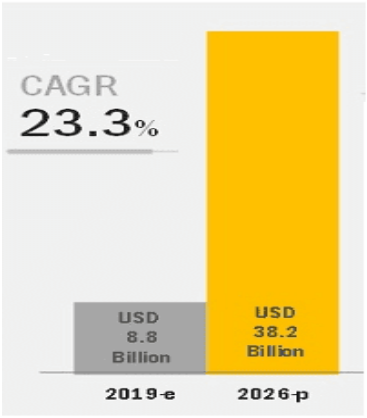

Рисунок 1 – Прогноз объёма мирового рынка технологий искусственного интеллекта в информационной безопасности на 2019-2025 годы, по данным MarketsandMarkets

Источник: [4].

Литература

1. Ван Хайтао. Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности. – 2018. (3).
2. https://www.oracle.com/ru/artificial-intelligence/what-is-ai/
3. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity
4. https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

СЕКЦИЯ 2.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ МЕЖДУНАРОДНОЙ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

СЕКЦИЯ 3.
МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРУПНЫХ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

СЕКЦИЯ 7.
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В МОБИЛЬНЫХ СИСТЕМАХ

СЕКЦИЯ 8.
ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР, ПОЛЬЗОВАТЕЛЕЙ, ИХ ДАННЫХ И ИНТЕРЕСОВ

СЕКЦИЯ 10.
МЕНЕДЖМЕНТ ИННОВАЦИЙ В СФЕРЕ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В ЭКОНОМИЧЕСКОЙ СФЕРЕ

Научное издание

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМ

Труды IX Международной
научно-практической конференции
2-4 марта 2023, Симферополь —Гурзуф

Печатается в авторской редакции

Подписано в печать 21.02.2023 г.
Формат 60х90 $^{1}/_{8}$. Бумага офсетная. Печать цифровая.
Гарнитура Times New Roman.
Усл. п.л. 22,75. Тираж 300 экз. Заказ № НИ/122.

Издательский дом ФГАОУ ВО «КФУ имени В. И. Вернадского».
295051, Республика Крым, г. Симферополь, бул. Ленина, 5/7,
тел.: +7 978 823 14 29, e-mail: print@cfuv.ru

Отпечатано с готового оригинал-макета ИП Зуева Т. В.
297565, Республика Крым, Симферопольский р-он,
с. Кизиловое, ул. Верхне-Кизиловая, д. 2, кв. 61.