ДЕНЬГИ, КРЕДИТ, БАНКИ

УДК 378.018.44: 004 doi 10.29039/2312-5330-2025-1-105-114

Бойченко Олег Валериевич,
доктор технических наук, профессор,
профессор кафедры бизнес-информатики и математического моделирования,
Физико-технический институт,
ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского»,
г. Симферополь, Российская Федерация

Boychenko Oleg Valeriyevich,
Doctor of Technical Sciences, Professor,
Professor of the Department of Business Informatics and Mathematical Modeling,
Institute of Physics and Technology,
V.I. Vernadsky Crimean Federal University,
Simferopol, Russian Federation.

КИБЕРУСТОЙЧИВОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

CYBER RESILIENCE OF FINANCIAL ORGANIZATIONS

В статье проведено исследование современного состояния проблематики киберустойчивости в управления кибербезопасностью данных в финансовых организациях. Установлены современные аспекты кратного повышения киберактивности мошенников во всех сферах экономики РФ, особенно в деятельности финансовых организаций. Определено, что для защиты данных в этом секторе необходимостью становится разработка и внедрение концепции киберустойчивости, включающей в себя не только методики предотвращения атак, но и подготовку к ним, наряду с тщательным и всесторонним анализом допущенных промахов, а также восстановлением системы автоматизированного управления деятельностью финансовой организации.

Отдельно установлено, что для исключения негативных последствий, целесообразно сосредоточиться на разработке постоянного цикла обеспечения киберустойчивости, наряду с совершенствованием целостной системы управления рисками кибербезопасности финансовой организации. Установлено обстоятельство противоречивого взаимодействия во многих финансовых организациях систем управления качеством IT, управления кибербезопасностью и непрерывностью бизнеса по общим процессам управления рисками, проблемами, инцидентами, обучением и повышением осведомленности, что приводит к возникновению проблемы своевременного реагирования на кросс-блочные инциденты, оказывающие ключевое воздействие на конфиденциальность, целостность и доступность информации.

Предложено использование разработанной концепции достижения киберустойчивости как целевого состояния организации в составе пяти шагов, в основе которой стоит синхронизация действий и синергии ИТ- и ИБ-экспертов при разработке надежной ИТ-инфраструктуры с высоким уровнем безопасности и отказоустойчивости системы управления кибербезопасностью финансовой организации.

Ключевые слова: финансовая сфера, кибератаки, киберинцидент, концепция, киберустойчивость, конфиденциальность, риск-менеджмент, оценка.

The article studies the current state of cyber resilience issues in data cybersecurity management in financial organizations. The modern aspects of the multiple increase in the cyber activity of fraudsters in all spheres of the Russian economy, especially in the activities of financial organizations, have been established. It is determined that for data protection in this sector it is necessary to develop and implement the concept of cyber resilience, which includes not only methods of preventing attacks, but also preparation for them, along with a thorough and comprehensive analysis of the blunders made, as well as the restoration of the automated management system of the financial organization.

Separately, it was found that in order to avoid negative consequences, it is advisable to focus on the development of a continuous cycle of cyber resilience, along with improving the holistic cybersecurity risk management system of the financial organization. The circumstance of contradictory interaction of IT quality management, cybersecurity management and business continuity management systems in many financial organizations on common processes of risk management, problems, incidents, training and awareness raising has been established, which leads to the problem of timely response to cross-block incidents that have a key impact on confidentiality, integrity and availability of information.

It is proposed to use the developed concept of achieving cyber resilience as a target state of the organization in five steps, which is based on synchronization of actions and synergy of IT and IS experts in the development of a reliable IT infrastructure with a high level of security and fault tolerance of the cyber security management system of a financial organization.

Keywords: financial sector, cyber-attacks, cyber incident, concept, cyber resilience, privacy, risk management, assessment.

ВВЕДЕНИЕ

На фоне роста числа кибератак ужесточается ответственность за нарушение требований цифровой безопасности, что не может не повлиять на скорость и продуктивность инфраструктуры, а ИТ-специалисты, ее поддерживающие, — не вступить в конфронтацию с коллегами из службы информационной безопасности (ИБ). Но рассогласованность действий ИТ- и ИБ-специалистов только усугубляет положение.

Для решения указанной проблемы многие финансовые организации вводят в свою стратегию развития термин «киберустойчивость», разрабатывают и внедряют концепции киберустойчивости, которые включают в себя не только методики предотвращения атак, но и подготовку к ним, а также порядок анализа допущенных ошибок и восстановления после инцидента в случае, если превентивные меры не дали ожидаемого результата.

Следует отметить, что кибератаки становятся все более сложными и тщательно спланированными, а их последствия — максимально разрушительными. Анализируя их возможные последствия, а зачастую испытав их на себе, бизнес все четче формулирует свой внутренний запрос на киберустойчивость.

Кроме того, многие регуляторные требования и стандарты обязывают финансовые организации тщательно защищать данные и часто влекут штрафы за нарушения. Следовательно, обеспечение киберустойчивости становится вопросом не только ИБ, но и соответствия бизнес-операций законодательным нормам и ожиданиям клиентов [1].

Исследованию проблемных вопросов киберустойчивости финансовой деятельности посвящены работы Садыковой Л.М., Коробейниковой Е.В., Фадейкиной Н. В., Зырянова В.С., Халниязовой Д. С., Янгульбаевой Л. Ш. и других ученых.

В частности, в работе [2] Садыковой Л.М. и Коробейниковой Е.В. проведен анализ ключевых угроз в области защищенности внутренней банковской сети, изучены уязвимости банковского бизнеса различного уровня риска, а также практики применения технологий обеспечения безопасности банковской деятельности.

Фадейкина Н.В. и Зырянов В.С. в работе [3] особое внимание уделяют совершенствованию системы управления операционным риском и комплексной модернизации корпоративных систем риск-менеджмента в кредитных организациях, учитывающих новые условия обеспечения информационной безопасности и функционирования системы экономической безопасности, от эффективного функционирования которой всецело зависит способность кредитной организации к устойчивому развитию.

В работе [4] Д. С. Халниязовой уделяется внимание использованию искусственного интеллекта для обеспечения кибербезопасности банковских организаций, а также рассматриваются аспекты реализации федерального проекта «Информационная безопасность».

В работе [5] Янгульбаевой Л. Ш. предложена модель механизма обеспечения киберустойчивости финансового сектора, которая предусматривает мониторинг и координацию финансовых учреждений, основанных на принципах теории жизнеспособных систем, а также приведена модель организационного построения системы управления киберрисками финансового учреждения, которая предусматривает защиту от рисков на уровне бизнес-подразделений, уровне управления операционными рисками и уровне подразделения внутреннего аудита.

ПОСТАНОВКА ЗАДАЧИ

Работа посвящена анализу проблем киберустойчивости финансовых организаций для создания инновационной системы управления кибербезопасностью в финансовой сфере.

Цель работы состоит в исследовании проблем, связанных киберустойчивостью деятельности финансовой организации.

Задачи работы определены целью исследования и направлены на изучение основных особенностей киберустойчивости в деятельности финансовых организаций, анализ современных методик управления киберустойчивостью для минимизации деструктивного воздействия на критические информационные ресурсы финансовой организации, а также создание современной концепции киберустойчивости в составе инновационных механизмов управления кибербезопасностью финансовой деятельности.

МЕТОДЫ

В исследовании был использован комплекс методов:

• метод дедукции, используемый для познания общих теоретических положений, сущности кибербезопасности данных финансовой организации, современных аспектов деструктивного воздействия, наряду с методологическими основами создания модели угроз финансовой организации;

• метод анализа был использован для раскрытия теоретических и практических положений по управлению кибербезопасностью финансовой организации, а также оценки ее киберустойчивости;

• метод синтеза применяется с целью получения обобщенных результатов исследования, формулировки выводов и общих заключений по проблемам оценки киберустойчивости финансовой организации и создания концепции киберустойчивости финансовой организации;

• метод сравнения используется с целью раскрытия и обоснования тенденций, особенностей, направлений, факторов и условий, влияющих на функционирование системы управления кибербезопасностью финансовой организации.

РЕЗУЛЬТАТЫ

Киберустойчивость — это способность организации обеспечить развитие деятельности (устойчивость предприятия) за счет готовности к кибер-угрозам, возможности реагирования на них, средств восстановления после кибератак [6].

Еще несколько лет назад использование ряда инновационных технологий могло казаться невозможным, но уже сегодня виртуальная реальность доступна конечному потребителю, IoT-устройства используются для контроля температуры в домах, а нейронные сети — для обработки фотографий.

Так, согласно отчету Gartner Top Trends in the Gartner Hype Cycle for Emerging Technologies, главными трендами в области развития технологий являются:

• искусственный интеллект — везде (Deep learning, машинное обучение, умные роботы);

• дополненная реальность (4D-печать, AR, VR);

• цифровые платформы (5G, цифровые двойники, блокчейн, IoT, квантовые вычисления).

Следует отметить, что каждая из этих сфер порождает свое множество угроз. Например, при использовании IoT-устройств могут возникать угрозы создания ботнетов, наряду с угрозами нанесения ущерба здоровью.

Кроме того, использование больших данных также создает новые вызовы в области кибербезопасности, такие как:

• непригодность существующих средств защиты для обеспечения безопасности данных такого объема;

• трудоемкость проверки аутентичности источников данных и контроля целостности данных;

• возрастание критичности процессов управления доступом к средам Big Data — получив нелегитимный доступ, нарушитель получает доступ к огромному массиву информации;

• возрастание рисков недоступности и потери данных.

Отдельно отметим, что вектор развития технологий также может говорить о следующих изменениях в области кибербезопасности, а именно:

• скорость появления новых технологий возрастает, ландшафт угроз расширяется с возрастающей скоростью, а угрозы, как и сами технологии, усложняются;

• количество атак (как и их сложность) увеличивается экспоненциально;

• количество уязвимостей не уменьшается, а напротив, растет из-за усложнения технологий и средств разработки;

• появляется тренд со стороны вендоров на обнаружение и реагирование вместо предотвращения и нейтрализации, как это было ранее.

Собственно, само понятие «киберустойчивость» возникло в ответ на повышающуюся скорость появления новых технологий и киберугроз в результате эволюционного развития системы защиты информации от «непрерывности IT» к «информационной безопасности» и далее к «кибербезопасности» (рис. 1). Так, если раньше цель информационной безопасности определялась обеспечением защиты критических данных финансовой организации превентивными мерами, то сейчас цель

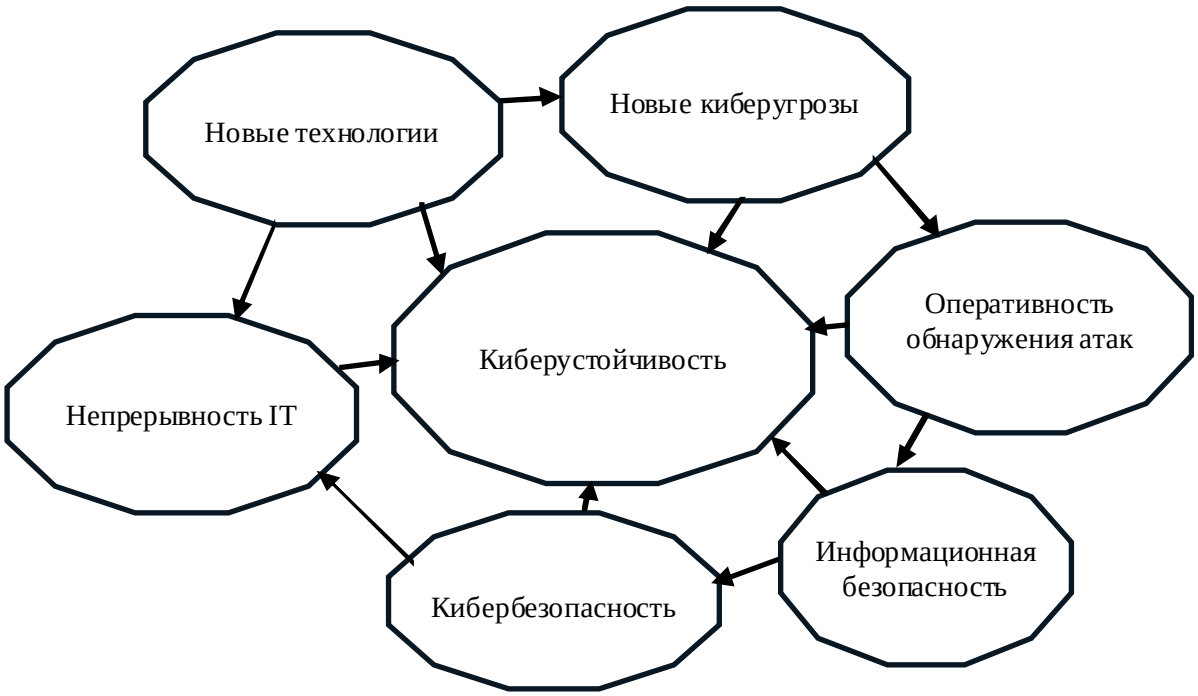

Рис. 1. Ландшафт современных угроз кибербезопасности (Составлено автором)

определяется, прежде всего, оперативным выявлением атак и их последствий. Современное состояние проблемы кибербезопасности определяет для организации перечень условий, когда бизнес должен находиться в готовности нанесения ущерба в условиях постоянного воздействия кибервлияний. Как следствие, возникают задачи, связанные с минимизацией ущерба для бизнеса в случае возникновения инцидента, а также с необходимостью обеспечения определённого уровня функционирования финансовой организации, наряду с сокращением времени восстановления АСУ и бизнес-процессов.

В этой связи, основываясь на решении задач исследования в предметной области киберустойчивости финансовых организаций, следует подчеркнуть важность формирования методологии построения киберустойчивости. Так, одним из первых упоминаний термина «Resilience» можно считать документ правительства Австралии «Стратегия устойчивости критической инфраструктуры» от 2010 года. Позже к этому вопросу подключились и другие организации, такие как компании Big4 (PWC, EY), аналитические агентства (Gartner), вендоры (IBM, Symantec) и NIST, Центральный банк РФ и Европейский центральный банк. Для решения исследуемой проблемы киберустойчивости некоторые организации (EY, Gartner, NIST) сосредоточены на создании собственно цикла обеспечения киберустойчивости, и, напротив, другие достигают ее путем развертывания и доработки самой системы управления рисками кибербезопасности (PWC) [7].

Кроме того, при анализе существующей методологии следует обратить внимание на Руководство по устойчивости финансового рынка к угрозам кибербезопасности (Guidance on cyber resilience for financial market infrastructures), разработанное IOSCO (International Organization of Securities Commissions) в июне 2016 года. IOSCO в своем документе определяет киберустойчивость, как способность прогнозировать, противостоять, сдерживать и восстанавливаться после кибератак. Это руководство представляет интерес по причине наиболее зрелого цикла обеспечения киберустойчивости. Он состоит из основных (идентификация, защита, обнаружение, восстановление) и поддерживающих (тестирование, ситуационная осведомленность, обучение и развитие) процессов [8].

Анализ свидетельствует, что для оценки уровня состоятельности киберустойчивости в организациях используются методики от US Department of Homeland Security (Cyber Resilience Self-Assessment), US-CERT (Assessments: Cyber Resilience Review), а также MITRE Corporation (Cyber Resiliency Metrics), AXELOS (RESILIA) [9].

Таким образом, с учетом количества приведенных выше подходов можно сделать вывод, что единая устоявшаяся методология построения киберустойчивости финансовых организаций не сформирована, наряду с отсутствием методики измерения и оценки эталонной киберустойчивости.

Для решения анализируемой проблемы во многих финансовых организациях отдельно используются системы управления качеством IT, управления кибербезопасностью и непрерывностью бизнеса, которых характеризуются общими процессами, такими, например, как управление рисками, проблемами, инцидентами, обучением и повышением осведомленности. Исследования показывают, что зачастую эти процессы либо находятся в зоне ответственности разных подразделений, либо существуют параллельно и дублируют друг друга. Более того, выходы одного процесса не всегда являются входными данными для работы другого (например, статистика инцидентов кибербезопасности должна поступать на вход процесса управления рисками кибербезопасности), наряду с тем, что сами процессы несогласованны, так, что следствием этого является несвоевременное реагирование на кросс-блочные инциденты, влияющие как на конфиденциальность, целостность, так и доступность информации.

В такой ситуации оптимальным решением проблемы может стать разработка единой методология на уровне всей организации, базис которой составляют следующие элементы:

- Guide on cyber resilience for financial market infrastructures (за авторством IOSCO, июнь 2016 года) [10];
- NIST Special Publication 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, 2018 год [11];
- Международный стандарт ISO/IEC 27001:2013 (Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования) [12];
- Международный стандарт ISO 22301:2012 (Социальная безопасность — Системы управления непрерывностью бизнеса — Требования) [13].

Данный подход предполагает создание кросс-блочной группы под условным названием Центр киберустойчивости финансовой организации. Предположительно, в эту группу должны входить представители подразделений, отвечающих за непрерывность бизнеса, кибербезопасность и качество IT (рис. 2), что позволит создать условия синергетического эффекта при взаимодействии различных направлений и функционировании смежных процессов за счет создания единой взаимосвязанной процессной модели, включая метрики и KPI, а также автоматизированные инструменты мониторинга, анализа эффективности и состоятельности процессов.

В связи с указанным, целесообразно определить перечень задач Центра киберустойчивости:

- интеграция процессов непрерывности бизнеса, надежности IT и кибербезопасности в единый процесс обеспечения киберустойчивости (в том числе выявление пробелов во взаимодействии) и его документирование;
- разработка кросс-блочных сценариев реагирования на инциденты;
- проведение учений, отработка сценариев реагирования на инциденты;
- координация реагирования на инциденты, принятие решения об эскалации руководству;
- сопровождение АС сбора и управления знаниями (единая система управления инцидентами);
- разработка планов развития системы обеспечения киберустойчивости и мониторинг их выполнения [14].

Итак, с одной стороны, к киберустойчивости подталкивает регулятор, с другой — бизнес и сам готов двигаться в этом направлении, чтобы не ставить под угрозу непрерывность технологических процессов, не рисковать финансами, данными и репутацией. Анализ свидетельствует, что наиболее универсальную методику оценки уровня состоятельности киберустойчивости предлагает AXELOS, которая содержит 145 вопросов из 5 доменов, при чем финансовая организация может использовать как вопросы, предлагаемые AXELOS, так и разработанные самостоятельно [15].

Следует подчеркнуть, что для разработки методики оценки киберустойчивости финансовой организации, прежде всего, необходимо определиться с доменами, по которым проводится оценка, начиная от модели киберустойчивости (Cyber Resilience Design), перехода к киберустойчивости (Cyber

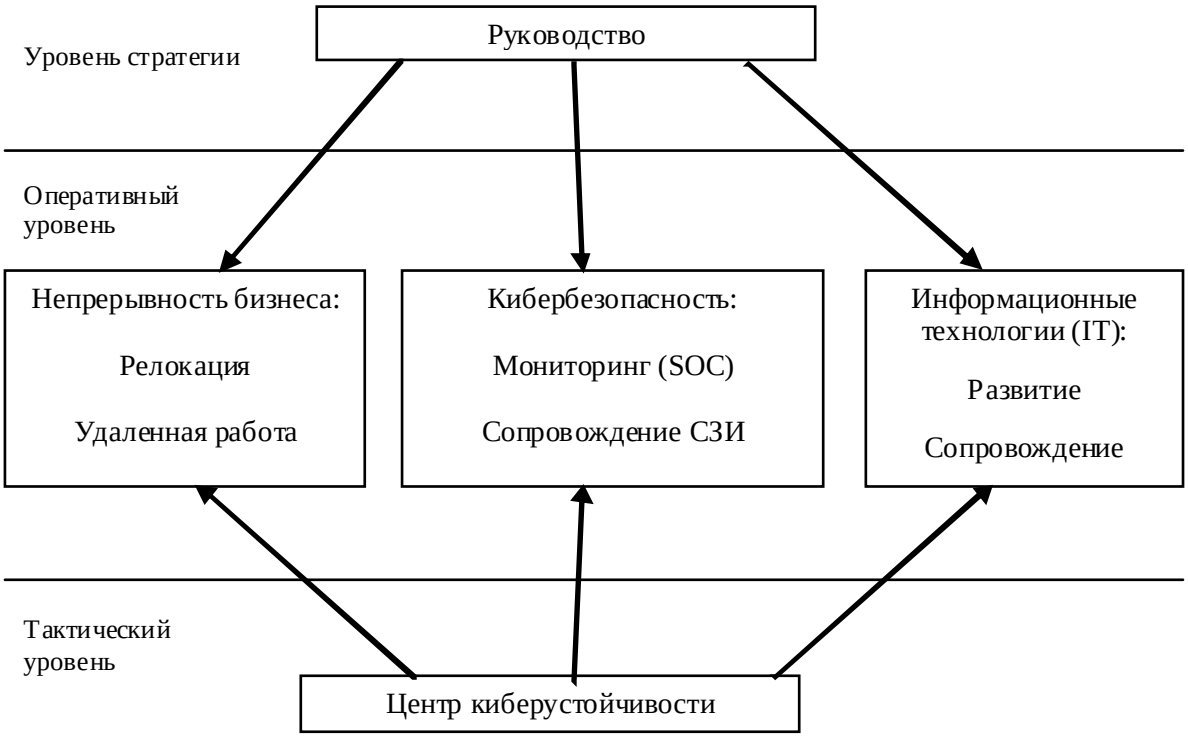

Рис. 2. Центр киберустойчивости (Составлено автором)

Resilience Transition), операционной деятельности (Cyber Resilience Operation), непрерывного улучшения (Cyber Resilience Continual Improvement) до стратегии (Cyber Resilience Strategy) [16].

По результатам оценки получим инструментальную шкалу, состоящую из пяти итоговых уровней киберустойчивости, начиная от (Initial) до оптимального (Optimized).

Целесообразным в указанной ситуации является разработка концепции достижения киберустойчивости как целевого состояния организации, состоящую из пяти шагов, основанную на синх-

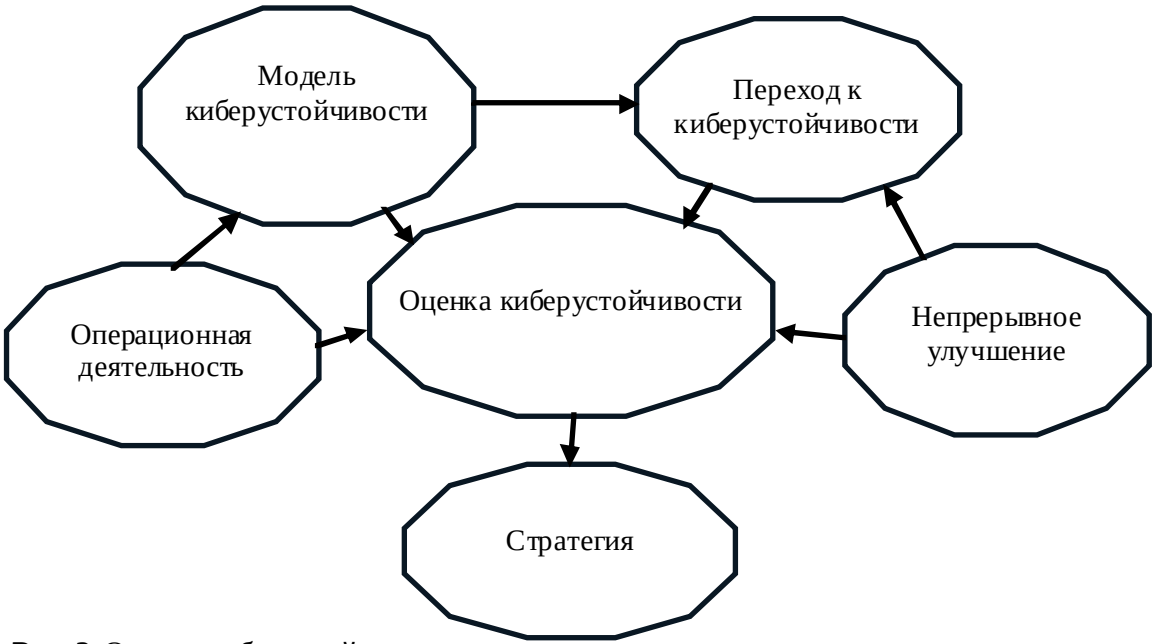

Рис. 3. Оценка киберустойчивости (Составлено автором)

ронизации действий и синергии ИТ- и ИБ-экспертов при создании надежной и эффективной для бизнеса ИТ-инфраструктуры. Для этого, прежде всего, определимся с последовательностью и сущностью шагов указанной концепции, пройдя которые компания получит инфраструктуру с высоким уровнем безопасности и отказоустойчивости систем управления кибербезопасностью финансовой организации [17].

Первым шагом и ключевым элементом в обеспечении киберустойчивости организации является гигиена ИБ, под которогй подразумевается базовый набор мер, направленных на создание прозрачности и непрерывности работы основных элементов ИТ-инфраструктуры.

Цель ИБ-гигиены состоит в обеспечении безопасности известных «точек входа» в инфраструктуру путем реализации базовых защитных мер и контроля взаимодействия инфраструктуры с внешней средой. Кроме того, ИТ- и ИБ-специалистам придется общими усилиями внедрить четкие организационные стандарты и политики управления ИТ-активами в сочетании с обеспечением безопасности, наряду с созданием условий для обеспечения регулярного обучения сотрудников основам кибербезопасности для минимизации влияния человеческого фактора и снижении шансов успешной реализации методов социальной инженерии.

Киберустойчивость ключевых ИТ-систем и сервисов является критическим аспектом общей безопасности организации, которая достигается путем обеспечения полной прозрачности работы компонентов ключевых систем, видимости их и параметров их работы для всех ответственных специалистов. Для этого систематически проводится мониторинг состояния оборудования, производительности систем и потоков данных. Наряду с этим, высокая видимость работы ИТ-сервисов позволяет оперативно выявлять и устранять проблемы, предотвращая их эскалацию. Кроме того, на этом этапе проводится инвентаризация ИТ-активов, относящихся к таким ключевым системам, как оборудование, ПО, сетевая составляющая и другие ресурсы корпоративной сети.

Наряду с этим, необходимостью является использование не только технологии ИТ-мониторинга, а также SIEM-технологий, с помощью которых можно в реальном времени отслеживать и анализировать события безопасности инфраструктуре, обеспечивая оперативное реагирование на инциденты. Безопасность ключевых систем предлагается обеспечивать в первую очередь за счет имеющихся встроенных механизмов защиты. Уровень отказоустойчивости также повысит оптимизация работы базовых ИТ-сервисов организации. Процесс может включать в себя редизайн систем, использование облачных технологий для повышения гибкости и масштабируемости, а также доработка необходимых компонентов средств защиты, наряду с регулярным тестированием систем, сотрудников и процессов на предмет эффективности взаимодействия и устойчивости к различным видам сбоев и атак.

На третьем этапе (устойчивость критичных систем) следует переходить к обеспечению киберустойчивости на уровне информационных систем (ИС) для защиты не только технического обеспечения работы компании, но и бизнес-процессов, поддерживаемых этими системами. Данный этап включает в себя инвентаризацию ИТ-активов, относящихся к критичным системам, использование их встроенных функций обеспечения безопасности, реализацию всестороннего мониторинга и внедрение дополнительных средств защиты в случае необходимости.

Задача повышения киберустойчивости критичных ИС решается в том числе такими методами, как кластеризация серверов, балансировка нагрузки и георапределенное резервное копирование. В современных условиях для увеличения катастрофоустойчивости резервное копирование и восстановление данных играют ключевую роль, равно как и использование решений для виртуализации и облачных технологий. Сюда же можно отнести различные механизмы быстрого обнаружения сбоев и атак, а также методы реагирования, включая аварийное восстановление и планы по борьбе с инцидентами.

Шаг №4 — способность технологических процессов противостоять ИБ-угрозам и обеспечивать непрерывность критически важных операций. На данном этапе видимость подразумевает в том числе осведомленность обо всех зависимостях ИС и о том, как изменения в одних частях цифрового ландшафта могут повлиять на другие. Потребуется наладить регулярное отслеживание потоков данных, используемых в различных бизнес-приложениях, и проводить тестирования

на устойчивость и восстановление после сбоев для гарантии непрерывности работы ИС. Все это поможет минимизировать простои и обеспечить быстрое восстановление критически важных приложений.

С этой целью производится маппинг бизнес-функций на конкретные активы ИТ-инфраструктуры, собираются метрики их работоспособности, подготавливаются источники данных, внедряется и настраивается единая система автоматического сбора и визуализации необходимых данных о состоянии бизнес-процессов, призванная помочь детально рассмотреть «узкие места» в их функционировании.

Обеспечение видимости процессов помогает в оперативном управлении и контроле, что позволяет быстро адаптироваться к изменениям. Необходимо также поддерживать непрерывный мониторинг клиентских сервисов и ИТ-услуг для обеспечения SLA, поскольку киберустойчивость ИТ-инфраструктуры и завязанного на ней комплекса прикладных ИС, технологических и бизнес-процессов является динамическим процессом, направленным на достижение и поддержание оптимального уровня защиты и производительности, в котором ИТ- и ИБ-действия циклично повторяются [18].

Для комплексного понимания текущего статуса ИТ-ландшафта и четкого ориентира дальнейшего развития предприятия, критически важно установить стандарты и бенчмарки оценки эффективности и безопасности работы корпоративных ИТ, поскольку поддержание достигнутых результатов потребует непрерывного управления изменениями, постоянного развития навыков команды ИТ-безопасности, регулярного обновления политик и процедур безопасности.

В такой ситуации, периодическая инвентаризация активов станет ключом к пониманию и защите ИТ в части обнаружения несанкционированных изменений и уязвимостей, а также обеспечении актуальности данных в планировании защиты. При этом, систематический контроль за изменениями с помощью автоматизированных систем управления конфигурацией обеспечит стабильность работы ИТ-систем на протяжении всего жизненного цикла путем предотвращения внедрения уязвимостей, а мониторинг событий в реальном времени позволит оперативно выявлять и реагировать на инциденты, обеспечивая непрерывность бизнес-процессов.

На пятом шаге огромную роль играют регулярные аудиты и тестирования, поскольку такие проверки включают в себя оценку уязвимостей и тестирование на проникновение (пентесты), что позволяет усилить защиту от внешних и внутренних угроз. При этом, успешность определяется наличием четкого плана реагирования на инциденты, который включает в себя коммуникацию с заинтересованными сторонами и управление последствиями инцидентов, поскольку киберустойчивость требует слаженной работы экспертов, обеспечивающей быструю адаптацию к новым угрозам и технологическим изменениям [19].

Чтобы быть конкурентным, бизнесу необходимо перевести ИТ-инфраструктуру в состояние непрерывного совершенствования, где каждый элемент — от инвентаризации до мониторинга и реагирования на инциденты — критически важен для обеспечения общей безопасности и надежности системы.

ВЫВОДЫ

Таким образом, обеспечить киберустойчивость финансовой организации можно только при высоком уровне состоятельности кибербезопасности, а работы по достижению киберустойчивости следует начать с поддержки концепции киберустойчивости со стороны высшего руководства — закрепление на уровне организационно-распорядительной документации организации (приказы или распоряжения); создания структурного подразделения по киберустойчивости; внедрения системы риск-менеджмента в отношении рисков кибербезопасности, непрерывности бизнеса и IT; разработки мероприятий по всестороннему мониторингу и обнаружению угроз, своевременному реагированию и восстановлению в случае их реализации; разработки системы оценки уровня зрелости и независимого аудита состояния киберустойчивости, а также непрерывного улучшения системы менеджмента в области киберустойчивости.

Подводя итоги, следует отметить, что для успешного функционирования в условиях постоянного воздействия киберугроз организация должна своевременно предвидеть, противостоять и вос-

станавливаться при наступлении инцидентов, которые затрагивают интересы всех подразделений и все бизнес-процессы организации. Внедрение системы менеджмента в области киберустойчивости позволит решить данные задачи и при этом соблюсти баланс риска и доходности от использования новых цифровых технологий и нивелировать последствия сопутствующих киберрисков.

СПИСОК ЛИТЕРАТУРЫ

1. Киберустойчивость — комплексный подход // Эксперт ONLINE. — URL: expertnw.com/ekspertnoe-mnenie/kiber-ustoychivost-kompleksnyy-podkhod/ (дата обращения: 27.02.2025).

2. Садыкова, Л. М. Формирование технологии обеспечения безопасности банковской деятельности в современных условиях / Л. М. Садыкова, Е. В. Коробейникова // Азимут научных исследований: экономика и управление. — 2021. — Т. 10, № 3(36). — С. 319-323. — DOI 10.26140/anie-2021-1003-0074. — EDN RWGPWD.

3. Фадейкина, Н. В. Информационная и экономическая безопасность кредитной организации как факторы обеспечения ее устойчивого развития / Н. В. Фадейкина, В. С. Зырянов // Сибирская финансовая школа. — 2024. — № 2(154). — С. 50-60. — DOI 10.34020/1993-4386-2024-2-50-60. — EDN ILXLTX.

4. Халниязова, Д. С. Проблемы обеспечения кибербезопасности при осуществлении банковской деятельности / Д. С. Халниязова // Теория права и межгосударственных отношений. — 2022. — Т. 1, № 5(25). — С. 233-239. — EDN DWZDRZ.

5. Янгульбаева, Л. Ш. Обеспечение устойчивости финансового киберпространства / Л. Ш. Янгульбаева // Вестник Чеченского государственного университета им. А.А. Кадырова. — 2021. — № 2(42). — С. 62-67. — DOI 10.36684/chesu-2021-42-2-62-67. — EDN DXSGFE.

6. Киберустойчивость — что это такое и как ее достичь? — URL: bosfera.ru/bo/kiberustoychivost-chto-eto-takoe-i-kak-ee-dostich (дата обращения: 02.08.2024).

7. Управление безопасностью // PWC. — URL: www.pwc.com/kz/ru/services/risk-assurance-services/cybersecurity.html (дата обращения: 27.02.2025).

8. Servais, J. P. The International Organization of Securities Commissions (IOSCO) and the New International Financial Architecture: What Role for IOSCO in the Development and Implementation of Cross-Border Regulation and Equivalence? / J. P. Servais // European Company and Financial Law Review. — 2020. — Vol. 17, No. 1. — P. 3-10. — DOI 10.1515/ecfr-2020-0001. — EDN KQYPWQ.

9. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs / J. F. Carias, S. Arrizabalaga, L. Labaka, J. Hernantes // IEEE Access. — 2021. — Vol. 9. — P. 80741-80762. — DOI 10.1109/ACCESS.2021.3085530. — EDN WFQQBY.

10. Банк России публикует рекомендации IOSCO для содействия в обеспечении качества внешнего аудита // Аудит. — 2019. — № 2. — С. 27. — EDN YXUJYL.

11. Design Guidelines and a Prototype Implementation for Cyber-Resiliency in IT/OT Scenarios Based on Blockchain and Edge Computing / E. Balistri, F. Casellato, S. Collura [et al.] // IEEE Internet of Things Journal. — 2022. — Vol. 9, No. 7. — P. 4816-4832. — DOI 10.1109/jiot.2021.3104624. — EDN NSYBSS.

12. Международный стандарт ISO/IEC 27001:2013 (Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования) // PQM-online. — URL: pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (дата обращения: 02.08.2024).

13. Международный стандарт ISO 22301:2012 (Социальная безопасность — Системы управления непрерывностью бизнеса — Требования) // Learn. — URL: learn.microsoft.com/ru-ru/compliance/regulatory/offering-iso-22301 (дата обращения: 02.08.2024).

14. Карелова, О. Л. SOC как инструмент повышения уровня кибербезопасности организации / О. Л. Карелова, А. В. Дробышев // Журнал высоких гуманитарных технологий. — 2023. — № 1(1). — С. 17-23. — EDN IKZWWI.

15. Воробьева, Д. Е. Модели оценки киберустойчивости транзакций в СУБД / Д. Е. Воробьева, Е. Г. Воробьев // Защита информации. Инсайд. — 2022. — № 6(108). — С. 67-70. — EDN PFPUXA.

16. Resilience-oriented planning strategy for the cyber-physical ADN under malicious attacks / X. Jing, W. Qin, H. Yao [et al.] // Applied Energy. — 2024. — Vol. 353. — P. 122052. — DOI 10.1016/j.apenergy.2023.122052. — EDN REHDRH.

17. Пять шагов к киберустойчивости. — URL: innostage-group.ru/press/media/pyat-shagov-k-kiberustoychivosti/ (дата обращения: 21.02.2025).

18. Балябин, А. А. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ / А. А. Балябин, С. А. Петренко, А. Д. Костюков // Защита информации. Инсайд. — 2024. — № 5(119). — С. 26-34. — EDN NHCKPS.

SPISOK LITERATURY

1. Kiberustoychivost' — kompleksnyy podkhod // Ekspert ONLINE. — URL: expertnw.com/ekspertnoe-mnenie/kiber-ustoychivost-kompleksnyy-podkhod/ (data obrashcheniya: 27.02.2025).

2. Sadykova, L. M. Formirovaniye tekhnologii obespecheniya bezopasnosti bankovskoy deyatel'nosti v sovremennykh usloviyakh / L. M. Sadykova, Ye. V. Korobeynikova // Azimut nauchnykh issledovaniy: ekonomika i upravleniye. — 2021. — T. 10, № 3(36). — S. 319-323. — DOI 10.26140/anie-2021-1003-0074. — EDN RWGPWD.

3. Fadeykina, N. V. Informatsionnaya i ekonomicheskaya bezopasnost' kreditnoy organizatsii kak faktory obespecheniya yeye ustoychivogo razvitiya / N. V. Fadeykina, V. S. Zyryanov // Sibirskaya finansovaya shkola. — 2024. — № 2(154). — S. 50-60. — DOI 10.34020/1993-4386-2024-2-50-60. — EDN ILXLTX.

4. Khalniyazova, D. S. Problemy obespecheniya kiberbezopasnosti pri osushchestvlenii bankovskoy deyatel'nosti / D. S. Khalniyazova // Teoriya prava i mezhgosudarstvennykh otnosheniy. — 2022. — T. 1, № 5(25). — S. 233-239. — EDN DWZDRZ.

5. Yangul'bayeva, L. Sh. Obespecheniye ustoychivosti finansovogo kiberprostranstva / L. Sh. Yangul'bayeva / / Vestnik Chechenskogo gosudarstvennogo universiteta im. A.A. Kadyrova. — 2021. — № 2(42). — S. 62-67. — DOI 10.36684/chesu-2021-42-2-62-67. — EDN DXSGFE.

6. Kiberustoychivost' — chto eto takoye i kak yeye dostich'? — URL: bosfera.ru/bo/kiberustoychivost-chto-eto-takoe-i-kak-ee-dostich (data obrashcheniya: 02.08.2024). 7. Upravleniye bezopasnost'yu // PWC. — URL: www.pwc.com/kz/ru/services/risk-assurance-services/cybersecurity.html (data obrashcheniya: 27.02.2025).

8. Servais, J. P. The International Organization of Securities Commissions (IOSCO) and the New International Financial Architecture: What Role for IOSCO in the Development and Implementation of Cross-Border Regulation and Equivalence? / J. P. Servais // European Company and Financial Law Review. — 2020. — Vol. 17, No. 1. — P. 3-10. — DOI 10.1515/ecfr-2020-0001. — EDN KQYPWQ.

9. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs / J. F. Carias, S. Arrizabalaga, L. Labaka, J. Hernantes // IEEE Access. — 2021. — Vol. 9. — P. 80741-80762. — DOI 10.1109/ACCESS.2021.3085530. — EDN WFQQBY.

10. Bank Rossii publikuyet rekomendatsii IOSCO dlya sodeystviya v obespechenii kachestva vneshnego audita // Audit. — 2019. — № 2. — S. 27. — EDN YXUJYL.

11. Design Guidelines and a Prototype Implementation for Cyber-Resiliency in IT/OT Scenarios Based on Blockchain and Edge Computing / E. Balistri, F. Casellato, S. Collura [et al.] // IEEE Internet of Things Journal. — 2022. — Vol. 9, No. 7. — P. 4816-4832. — DOI 10.1109/jiot.2021.3104624. — EDN NSYBSS.

12. Mezhdunarodnyy standart ISO/IEC 27001:2013 (Informatsionnyye tekhnologii — Metody obespecheniya bezopasnosti — Sistemy upravleniya informatsionnoy bezopasnost'yu — Trebovaniya) // PQM-online. — URL: pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (data obrashcheniya: 02.08.2024).

13. Mezhdunarodnyy standart ISO 22301:2012 (Sotsial'naya bezopasnost' — Sistemy upravleniya nepreryvnost'yu biznesa — Trebovaniya) // Learn. — URL: learn.microsoft.com/ru-ru/compliance/regulatory/offering-iso-22301 (data obrashcheniya: 02.08.2024).

14. Karelova, O. L. SOC kak instrument povysheniya urovnya kiberbezopasnosti organizatsii / O. L. Karelova, A. V. Drobyshev // Zhurnal vysokikh gumanitarnykh tekhnologiy. — 2023. — № 1(1). — S. 17-23. — EDN IKZWWI.

15. Vorob'yeva, D. Ye. Modeli otsenki kiberustoychivosti tranzaktsiy v SUBD / D. Ye. Vorob'yeva, Ye. G. Vorob'yev // Zashchita informatsii. Insayd. — 2022. — № 6(108). — S. 67-70. — EDN PFPUXA.

16. Resilience-oriented planning strategy for the cyber-physical ADN under malicious attacks / X. Jing, W. Qin, H. Yao [et al.] // Applied Energy. — 2024. — Vol. 353. — P. 122052. — DOI 10.1016/j.apenergy.2023.122052. — EDN REHDRH.

17. Pyat' shagov k kiberustoychivosti. — URL: innostage-group.ru/press/media/pyat-shagov-k-kiberustoychivosti/ (data obrashcheniya: 21.02.2025).

18. Balyabin, A. A. Model' ugroz bezopasnosti i kiberustoychivosti oblachnykh platform KII RF / A. A. Balyabin, S. A. Petrenko, A. D. Kostyukov // Zashchita informatsii. Insayd. — 2024. — № 5(119). — S. 26-34. — EDN NHCKPS.

Статья поступила в редакцию 3 марта 2025 года

Статья одобрена к печати 6 июня 2025 года