ФИНАНСЫ

УДК 378.018.44: 004 doi 10.29039/2312-5330-2024-4-5-14

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.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ДАННЫХ В ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

DATA SECURITY MANAGEMENT IN FINANCIAL ORGANIZATIONS

В статье проведено исследование современного состояния проблематики угроз и уязвимостей управления кибербезопасностью данных в финансовых организациях. Установлена уязвимость финансовой сферы к кибератакам, что указывает на особую ее привлекательность для мошенников. Определено, что для защиты данных в этом секторе система кибербезопасности должна быть комплексной, наряду с гибкостью, простотой и возможностью наращивания инструментов и методов безопасности. Отдельно установлено, что для исключения негативных последствий, денежных и репутационных потерь, важно определить и внедрить комплекс защитных мероприятий по созданию условий по эффективной безопасности финансовых данных. Для реализации указанной направленности системы обеспечения киберзащиты обосновано планирование политики безопасности финансовой организации на основе стандарта банка России СТО БР БФБО-1.8-2024 с целью дифференцирования состава и содержания мер защиты в зависимости от вида операции, ее критичности и рисков. Определено, что современная политика информационной безопасности финансовой организации наряду с действиями по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации, предусматривает процедуру делегирования идентификации или аутентификации в процессе передачи поставщиком услуг обязанности или права проведения идентификации или аутентификации получателя услуг доверенной третьей стороне, что усиливает возможности системы обеспечения киберзащиты в дистанционном предоставлении финансовых продуктов и услуг финансовой организацией.

Предложено внедрение DLP-системы для защиты данных финансовой организации в момент их использования, передачи и хранения, наряду с созданием условий для выявления подозрительной активности сотрудников, а также выявлением угроз и принятия мер противодействия на ранней стадии.

Ключевые слова: финансовая сфера, кибератаки, киберинцидент, политика безопасности, идентификация, аутентификация, кибербезопасность.

The article studies the current state of the problems of threats and vulnerabilities of data cybersecurity management in financial organizations. The vulnerability of the financial sector to cyberattacks has been established, which indicates that it is particularly attractive to fraudsters. It is determined that to protect data in this sector, cybersecurity must be comprehensive, along with flexible, simple, and scalable security tools and techniques. It is separately established that in order to exclude negative consequences, monetary and reputational losses, it is important to define and implement a set of protective measures to create conditions for effective security of financial data. In order to implement the abovementioned orientation of the cyber protection system, the planning of security policy of a financial organization based on the Bank of Russia standard STO BR BFBO-1.8-2024 is justified in order to differentiate the composition and content of protection measures depending on the type of operation, its criticality and risks. It was determined that the modern information security policy of a financial organization, along with actions to verify the authenticity of the subject of access and/or object of access, as well as to verify the belonging of the access identifier and authentication information presented to the subject of access and/or object of access, provides for the procedure of delegation of identification or authentication in the process of transferring the service provider's obligation or right to carry out identification or authentication of the recipient of services to a trusted third party, which is necessary for the organization's data protection.

The implementation of DLP-system for protection of financial organization's data at the moment of their use, transfer and storage, along with creating conditions for detection of suspicious activity of employees, as well as identifying threats and taking action at an early countermeasures stage is proposed.

Keywords: financial sphere, cyberattacks, cyberincident, security policy, identification, authentication, cybersecurity.

ВВЕДЕНИЕ

Компании, работающие в финансовой отрасли, наиболее подвержены внешним кибератакам и внутренним угрозам. Цифровизация и современные технологии создают не только возможности развития, но и определенные риски. Для злоумышленников сведения о сотрудниках, клиентах финансовой организации, их финансовые данные являются ликвидным активом, и зачастую становятся главной мишенью утечки. Финансовая сфера — уязвима к кибератакам и привлекательна для мошенников. Защита данных в этом секторе должна быть комплексной и при этом понятной. Чтобы избежать негативных последствий, денежных и репутационных потерь, важно позаботиться о защите финансовых данных.

Речь идет о сведениях, связанных с движением денежных средств, использованием ресурсов компании, производством, обращением товаров, инвестициями, а также персональными данными клиентов и контрагентов, в которых может содержаться конфиденциальная информация в отношении нормативной базы; результатов предпринимательской деятельности; платежных данных и кассовых ордерах; стратегии и цели в виде планируемых показателей; сведения о финансах предприятий-поставщиков; состоянии покупательского спроса, а также инсайдерских данных о рынке товаров или услуг в условиях цифровизации экономики страны [1].

Исследованию проблемных вопросов управления безопасностью данных в финансовой деятельности посвящены работы Едемского А.В., Бартошко Т.В., Стерхова А.П., Горбуновой В.Б. и других ученых.

В частности, в работе [2] Едемский А.В. указывает на использование методов математической статистики для анализа собранных данных и оценки уровня безопасности финансовых данных наряду с рассмотрением существующие практик и политики безопасности данных в финансовых организациях, а также сравнения этих практик с рекомендациями и стандартами безопасности данных.

Бартошко Т.В. и Стерхов А.П. в работе [3] определяют основные меры, которые могут существенно сократить материальные, временные и трудовые затраты на построение системы защиты персональных данных финансовой организации, учитывая требования законодательных актов, регламентирующих защиту персональных данных, таких как организация конфиденциального делопроизводства, принятия работниками банка обязательства строго исполнять его правила и нести персональную ответственность за обеспечение сохранности доверенных конфиденциальных сведений и информационных носителей, содержащих данные сведения.

В работе [4] Горбуновой В.Б. обоснована актуальность своевременного выявления риска финансовой несостоятельности предприятий в целях обеспечения экономической безопасности региона наряду с рассмотрением основных аспектов и факторов, влияющих на финансовую безопасность организаций, а также современные технологии и подходы, используемые для выявления и предотвращения финансовых проблем, среди которых особое внимание уделено анализу традиционных и альтернативных данных, включая использование Big Data, аналитики данных, методов машинного обучения и алгоритмов прогнозирования для улучшения точности прогнозов.

ПОСТАНОВКА ЗАДАЧИ

Работа посвящена анализу проблем управления безопасностью данных финансовых организаций для разработки и создания комплексной системы управления защитой данных в финансовой сфере.

Цель работы состоит в исследовании проблем, связанных с использованием современной системы управления безопасностью данных финансовой деятельности.

Задачи работы определены целью исследования и направлены на изучение основных особенностей угроз и уязвимостей информации в деятельности финансовых организаций, анализ современных методик управления безопасностью данных для минимизации экономического и репутационного ущерба финансовой организации вследствие деструктивного воздействия внешнего и

внутреннего инсайда, а также создание методики упреждения и противодействия кибервлиянию злоумышленников на основе современных инструментов системы обеспечения информационной безопасности финансовой деятельности.

МЕТОДЫ

В исследовании был использован комплекс методов:

- метод дедукции, используемый для познания общих теоретических положений, сущности безопасности данных финансовой организации, современных аспектов воздействия угроз и уязвимостей СОИБ финансовой организации, наряду с методологией моделирования угроз данных финансовой организации;
- метод анализа был использован для раскрытия теоретических и практических положений по управлению безопасностью данных финансовой организации, а также оценки ее эффективности в защите информационных активов;
- метод синтеза применяется с целью получения обобщенных результатов исследования, формулировки выводов и общих заключений по проблемам оценки безопасности данных финансовой организации и создания методики упреждения и противодействия кибервлиянию злоумышленников;
- метод сравнения используется с целью раскрытия и обоснования тенденций, особенностей, направлений, факторов и условий, влияющих на функционирование системы управления безопасностью данных финансовой организации.

РЕЗУЛЬТАТЫ

На сегодняшний день все более четко обосновываются успехи и достижения цифровизации в экономической сфере, которые обоснованы тем, что уже более 85 % населения пользуются цифровыми услугами и сервисами и получают услуги онлайн, особенно в сфере финансового обслуживания.

Однако, оборотная сторона медали (все, что связано с угрозами и уязвимостями коммерческих о пользовательских данных финансовых организаций), формирует понятие среды доверия — состояние среды взаимодействия между поставщиком и получателем услуг, при возможном участии третьей стороны, предоставляющей сервис идентификации и аутентификации, при котором обеспечена необходимая уверенность в том, что получатель услуги соответствует предоставленной идентификационной информации (идентифицирован), а также является тем, за кого себя выдает (аутентифицирован).

В указанной ситуации, прежде всего, целесообразно обратиться к требованиям регулятора, являющегося главным арбитром в сфере информационной и финансовой безопасности государства. Так, в частности, нормативной базой мероприятий по обеспечению безопасности данных финансовых организаций является следующий комплекс документов:

1. Приказ ФСТЭК № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 г. [2] п. 22 — «Организационные меры и технические меры по идентификации и аутентификации», где указано, что в значимых объектах в зависимости от их категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры: идентификация и аутентификация (ИАФ); управление доступом (УПД); ограничение программной среды (ОПС); защита машинных носителей информации (ЗНИ); аудит безопасности (АУД); антивирусная защита (АВЗ); предотвращение вторжений (компьютерных атак) (СОВ); обеспечение целостности (ОЦЛ); обеспечение доступности (ОДТ); защита технических средств и систем (ЗТС); защита информационной (автоматизированной) системы и ее компонентов (ЗИС); планирование мероприятий по обеспечению безопасности (ПЛН); управление конфигурацией (УКФ); управление обновлениями программного обеспечения (ОПО); реагирование на инциденты информационной безопасности (ИНЦ); обеспечение действий в нештатных ситуациях (ДНС); информирование и обучение персонала (ИПО).

В дополнение следует отметить, что при реализации мер по обеспечению безопасности значимых объектов применяются методические документы, разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспорт-

ному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

2. ГОСТ 58833 «Защита информации. Идентификация и аутентификация. Общие положения» от 01.05.2020 г. [3], который устанавливает единообразную организацию процессов идентификации и аутентификации в средствах защиты информации, в том числе реализующих криптографическую защиту, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила применения методов идентификации и аутентификации, обеспечивающих необходимую уверенность в результатах.

Положения стандарта не исключают применение криптографических и биометрических методов (алгоритмов) при идентификации и аутентификации, но не устанавливают требования по их реализации.

Стандарт определяет состав участников и основное содержание процессов идентификации и аутентификации, рекомендуемое к реализации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом.

Положения стандарта могут использоваться при управлении доступом к информационным ресурсам, вычислительным ресурсам средств вычислительной техники, ресурсам автоматизированных (информационных) систем, средствам вычислительной техники и автоматизированным (информационным) системам в целом.

3. ГОСТ 70262 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации» от 01.01.2023 г. [4], который устанавливает единообразную организацию процесса идентификации субъектов и объектов доступа в средствах защиты информации, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила идентификации, обеспечивающие необходимую уверенность в ее результатах.

Стандарт определяет состав участников и основное содержание процесса идентификации, рекомендуемые к реализации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом.

Положения стандарта могут использоваться при управлении доступом к информационным ресурсам, вычислительным ресурсам средств вычислительной техники, ресурсам автоматизированных (информационных) систем, средствам вычислительной техники и автоматизированным (информационным) системам в целом, а также применяются совместно с документами по стандартизации, регламентирующими вопросы идентификации и аутентификации.

4. НПА Банка России (683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» от 17.04.2019 г. [5], 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» от 20.04.2021 г. [6], 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» от 17.08.2023 г. [7]).

5. ГОСТ 57580.1 «Защита информации финансовых организаций. Базовый состав организационных и технических мер» от 08.08.2017 г. [8], который определяет уровни защиты информации и соответствующие им требования к содержанию базового состава мер защиты информации в финансовых организациях для реализации требований к обеспечению защиты информации, установленных нормативными актами Банка России.

Область применения стандарта, определяющая обязанность финансовых организаций применять меры защиты информации, реализующие один из уровней защиты информации для конкретной совокупности объектов информатизации, в том числе АС, используемых финансовыми организациями для предоставления финансовых услуг, устанавливается в нормативных актах Банка

России путем включения нормативной ссылки на стандарт, приводимой на основании статьи 27 Федерального закона «О стандартизации в Российской Федерации» [9].

Данные документы формируют основу формирования нового документа СТО БР БФБО-1.8-2024 «Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации» (вступил в силу 01.07.2024 г.), целью которого является повышение защищенности людей от злоумышленников, которые похищают деньги, используя личные и финансовые данные граждан [10].

Назначение стандарта состоит в том, чтобы сформировать среду доверия при проведении идентификации и аутентификации, дифференцировать состав и содержание мер защиты в зависимости от вида операции, ее критичности и рисков.

В рамках настоящего стандарта процессы идентификации и аутентификации применяются в соответствии с описанием, приведенным в ГОСТ Р 58833-2020, и включают в себя следующие составляющие:

- первичная идентификация (регистрация) — действия по формированию и регистрации информации о субъекте доступа или объекте доступа, а также действия по присвоению идентификатора доступа субъекту доступа или объекту доступа и его регистрации в перечне присвоенных идентификаторов доступа;
- вторичная идентификация — действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа при доступе, в перечне идентификаторов доступа, которые были присвоены субъектам доступа и объектам доступа при первичной идентификации;
- аутентификация — действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации;
- делегирование идентификации или аутентификации — процесс передачи поставщиком услуг обязанности или права проведения идентификации или аутентификации получателя услуг доверенной третьей стороне;
- передача идентификационной или аутентификационной информации и сведений об идентификации или аутентификации.

При этом, процесс аутентификации может быть организован как с участием доверенной третьей стороны, так и без нее.

При односторонней однофакторной аутентификации по паролю услуги доверенной третьей стороны не используются, а регистрирующая, проверяющая и доверяющая стороны объединены в доверяющую сторону и ее функции выполняет объект доступа.

В рамках настоящего стандарта рассматривается только дистанционное предоставление финансовых продуктов и услуг финансовой организацией, в связи с чем идентификация и аутентификация также являются дистанционными, то есть осуществляются без личного присутствия клиента в финансовой организации.

При этом, в документе предписано установление трех уровней доверия идентификации и аутентификации:

1. Состав мер защиты информации, применяемых при идентификации и аутентификации;
2. Состав мер защиты информации, применяемый при делегировании идентификации и (или) аутентификации;
3. Перечни мер для применения при использовании конкретных аутентификаторов, а также в процессах, наиболее распространенных в финансовых организациях.

Примеры приведенных мер представлены в таблицах 1 и 2.

Проведенный анализ нормативно-правовых актов, обеспечивающих выполнение требований регулятора в отношении построения адекватной современным условиям проблематики угроз и уязвимостей данным финансовых организаций, позволяет наиболее полно провести оценку потенциальной опасности и разработать действенную систему противодействия для обеспечения конфиденциальности пользовательских и коммерческих данных организации.

Таблица 1. Применение УДИ к финансовым операциям поставщика услуг *

Реализация процесса верификации	Допустимые УДИ		
	УДИ 1	УДИ 2	УДИ 3
Предоставление информационных сервисов физическим лицам	+	+	+
Предоставление информационных сервисов юридическим лицам	–	+	+
Совершение финансовых операций физических лиц, оценка операционного риска которых не превышает установленных во внутренних документах показателей оценки операционного риска	–	+	+
Совершение высокорисковых (оценка операционного риска превышает установленныево внутренних документах показатели оценки операционного риска) финансовых операций физических лиц	–	–	+
Совершение финансовых операций юридических лиц	–	–	+

* Составлено на основании [10]

Таблица 2. Примеры реализаций процесса верификации в разрезе уровней доверия идентификации *

Реализация процесса верификации	УДИ 1	УДИ 2	УДИ 3
Подтверждение сведений о получателеуслуг через оператора сотовой связи сиспользованием номера мобильного телефона	+	–	–
Подтверждение сведений о получателе услуг с использованием неподтвержденнойучетной записи ЕСИА	+	–	–
Подтверждение сведений о получателе услуг с использованием подтвержденнойучетной записи ЕСИА с установленной двухфакторной аутентификацией	+	+	+

* Составлено на основании [10]

Известно, что основная угроза данным финансовым организациям связана с утечкой конфиденциальной информации, поскольку злоумышленники могут шантажировать полученными данными или неправомерно использовать их с целью извлечения выгоды. В частности, утечки данных из финансовых организаций происходят вследствие реализации различных киберугроз:

- вредоносные программы, наносящие ущерб отдельным компьютерам, серверам или сетям. Такое ПО вредит работе инфраструктуры, предоставляет злоумышленникам доступ к финансовым данным (в 2023 году угрозы составили в среднем 151 со снижением на 34,44 %);
- фишинг путем создания поддельных сайтов и вредоносных сообщений, которые открывают доверчивые сотрудники, в результате чего происходит «слив» данных (в 2023 году угрозы составили в среднем 2015 со снижением на 38,31 %);
- атаки на поставщиков ПО для финансовых организаций.

Обновления программ подменяются или модифицируются злоумышленниками, вследствие чего они получают доступ к конфиденциальным сведениям (в 2023 году угрозы составили в среднем 195 со снижением на 42,56 %). Злоумышленники могут получить несанкционированный доступ и вывести из строя систему — изменить информацию, «слить» ее конкурентам, а в случае получения платежных данных существует риск хищения денежных средств. Банки в 2023 году предотвратили мошеннические хищения на 5,8 трлн рублей, но злоумышленники смогли провести 1,17 млн успешных операций, на 33 % больше, чем в 2022 году, следует из материалов ЦБ РФ. В результате атак кибермошенников потери клиентов банков увеличились на 11,5 %. Примерно на столько же вырос объем переводов по банковским картам, остающимся самым популярным платежным инструментом у мошенников [11].

Исходя из полученных выводов, необходимо заключить, что информационная безопасность должна быть системной, гибкой и обоснованной, в сочетании с требованиями просто-

ты, прозрачности и достаточной эффективности выбранных средств защиты финансовых данных (рис. 1).

Рис. 1. Требования к системе информационной безопасности (Составлено автором)

Приведенный перечень современных атрибутов информационной безопасности финансовых организаций формирует актуальные принципы обеспечения безопасности [12]:

1. Прозрачность данных касательно доступа сотрудников финансовых компаний в части специфики сбора, хранения и обработки информации;

2. Создание регламента в политике безопасности организации в части разработки требований к алгоритмам работы с конфиденциальной финансовой информацией;

3. Контроль устройств и съемных носителей в отношение ограничения кражи данных и заражения вредоносным ПО;

4. Регламентирование доступа к определенным помещениям в части разработки режимных мероприятий политики безопасности организации (использование журналирования фиксации сотрудников, взаимодействующих с серверами);

5. Проверка готовности служб безопасности в разработке планов контроля и развития выбранной системы информационной безопасности организации, в частности, путем симуляции кибератак для проверки используемых программных и технических средств защиты финансовых данных.

Переходя непосредственно к инструментам системы информационной безопасности финансовой организации, следует выделить один из важнейших элементов обеспечения кибербезопасности, которым является внедрение технических средств, позволяющих защитить данные в момент их использования, передачи, хранения, а также зашифровать конфиденциальные сведения и предотвращать мошеннические действия злоумышленников.

В такой ситуации, руководствуясь требованиями Президента и Правительства РФ в отношении технологического суверенитета нашего государства, в условиях широкомасштабных и повсеместных санкций объединенного запада, необходимостью является выбор программно-технических средств отечественной разработки в соответствие с Единым реестром российских программ для электронных вычислительных машин и баз данных (постановление Правительства от 16 ноября 2015 года № 1236) [13].

Так, для решения обозначенных ранее задач обеспечения безопасности данных финансовых организаций, наиболее целесообразным является использование DLP-систем (Data Leak Prevention), которые выявляют признаки корпоративного мошенничества, позволяют проводить полноценное расследование киберинцидентов, анализировать действия пользователей с возможностью составления персонального досье по поведенческим паттернам [14].

DLP-решения — один из эффективных инструментов, позволяющий отслеживать хранение и передачу финансовых данных, предотвращать утечки, выявлять инциденты и оперативно на них реагировать (рис. 2).

Рис. 2. Обобщенная схема DLP-системы (Составлено автором)

Кроме того, решения класса DLP обеспечивают создание условий для защиты конфиденциальных данных даже при отсутствии подключения к интернету, а проведение постоянного контроля за соблюдением правил кибербезопасности, практически сводит к нулю утечку данных и дальнейшее их неправомерное использование.

Таким образом, важность внедрения DLP-систем в финансовой сфере очевидна, поскольку позволяет непрерывно отслеживать движение конфиденциальных данных, выявлять факты их размещения в неположенных файловых хранилищах, поскольку такой мониторинг позволяет определить не только признаки деструктивных действий потенциальных внутренних злоумышленников (в группе риска), но и пользователей финансовой организации, которые пренебрегают правилами и регламентом политики безопасности при работе с данными.

Кроме того, анализируемая DLP-система позволяет создавать условия для выявления подозрительной активности сотрудников, наряду с выявлением угроз и принятия мер на ранней стадии.

Указанные параметры отечественных DLP-систем также обеспечивают выполнение требований 1-го уровня защищенности персональных данных, что отвечает положениям Приказа ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) [15] и дополнительно подтверждает эффективность использования в информационных системах финансовой сферы для обеспечения безопасности коммерческих и пользовательских данных имеющих признаки конфиденциальности.

ВЫВОДЫ

В частности, для защиты данных крупных финансовых компаний наиболее востребованной является DLP-система Solar Dozor (полноценно заменяет зарубежные DLP-системы и полностью соответствует требованиям импортозамещения), которая характеризуется следующими преимуществами:

1. Контроль всех основных каналов передачи данных, в том числе мессенджеров, съемных носителей, облачных и локальных хранилищ.

2. Поведенческая аналитика и сбор доказательной базы для расследования.

3. Формирование наглядных и понятных отчетов по мониторингу.

4. Возможность функционирования в географически распределенном режиме с централизованным управлением филиалами.

5. Быстрый поиск сообщений, событий и инцидентов безопасности, а также построение карты сети для выявления файловых хранилищ, содержащих конфиденциальные сведения.

6. Совместимость с любой операционной системой, легкость управления и настройки.

СПИСОК ЛИТЕРАТУРЫ

1. Защита данных в финансовой сфере // Solar Dozor. — URL: rt-solar.ru/products/solar_dozor/blog/3587/ (дата обращения: 29.07.2024).

2. Едемский, А. В. Безопасность данных в финансовой сфере: тенденции и вызовы / А. В. Едемский // Вестник науки. — 2023. — Т. 2, № 8(65). — С. 6-19. — EDN LBOTBS.

3. Бартошко, Т. В. Защита персональных данных как важная составляющая общей безопасности банка / Т. В. Бартошко, А. П. Стерхов // Вестник Иркутского государственного технического университета. — 2015. — № 5(100). — С. 177-182. — EDN RWCCZK.

4. Горбунова, В. Б. Финансовая несостоятельность предприятий как угроза экономической безопасности региона / В. Б. Горбунова // Балтийский экономический журнал. — 2024. — № 1(45). — С. 17-27. — DOI 10.46845/2073-3364-2024-0-1-17-27. — EDN GGVRED.

5. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК от 25.12.2017 г. № 239 // Solar Dozor. — URL: www.consultant.ru/document/cons_doc_LAW_294287/ (дата обращения: 02.08.2024).

6. ГОСТ 58833 «Защита информации. Идентификация и аутентификация. Общие положения» от 01.05.2020 г. // Электронный фонд правовых и нормативно-технических документов. — URL: docs.cntd.ru/document/1200172576/titles (дата обращения: 02.08.2024).

7. ГОСТ 70262 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации» от 01.01.2023 г. // Росстандарт. — URL: protect.gost.ru/default.aspx/document1.aspx?control=31&id=245656 (дата обращения: 02.08.2024).

8. Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента: Положение Банка России от 17.04.2019 г. № 683-П // Гарант. — URL: base.garant.ru/72246408/ (дата обращения: 31.07.2024).

9. Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций: Положение Банка России от 20.04.2021 г. № 757-П // Гарант. — URL: www.garant.ru/products/ipo/prime/doc/400824645/ (дата обращения: 31.07.2024).

10. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств: Положение Банка России от 17.08.2023 г. № 821-П // Гарант. — URL: www.garant.ru/products/ipo/prime/doc/408082189/ (дата обращения: 31.07.2024).

11. ГОСТ 57580.1 «Защита информации финансовых организаций. Базовый состав организационных и технических мер» от 08.08.2017 г. // Гарант. — URL: base.garant.ru/72031046/ (дата обращения: 02.08.2024).

12. О стандартизации в Российской Федерации: Федеральный закон от 29.06.2015 № 162-ФЗ (с изменениями и дополнениями) // Гарант. — URL: base.garant.ru/71108018/ (дата обращения: 02.08.2024).

13. СТО БР БФБО-1.8-2024 «Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации» // Гарант. — URL: www.cbr.ru/Crosscut/LawActs/File/7706 (дата обращения: 02.08.2024).

14. Апатова, Н. В. Управление процессами цифровой трансформации бизнеса / Н. В. Апатова // Ученые записки Крымского федерального университета имени В.И. Вернадского // Экономика и управление. — 2022. — Т. 8, № 2. — С. 3-8. — EDN SCWJEG.

15. Буркальцева, Д. Д. История развития теорий концепции экономической безопасности / Д. Д. Буркальцева // Вопросы истории. — 2023. — № 6-1. — С. 122-127. — DOI 10.31166/VoprosyIstorii202306Statyi18. — EDN FIKIYG.

16. Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд: Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 (с изменениями и дополнениями) // Гарант. — URL: base.garant.ru/71252170/ (дата обращения: 31.07.2024).

17. Апатова, Н. В. Экономическое развитие и экономический рост: основные ориентиры в цифровой экономике / Н. В. Апатова // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. — 2023. — Т. 9, № 3. — С. 3-14. — EDN HUYBZL.

18. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ

ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) // ФСТЭК России. — URL: fstec.ru (дата обращения: 31.07.2024).

SPISOK LITERATURY

1. Zashchita dannykh v finansovoy sfere // Solar Dozor. — URL: rt-solar.ru/products/solar_dozor/blog/3587/ (data obrashcheniya: 29.07.2024).

2. Yedemskiy, A. V. Bezopasnost' dannykh v finansovoy sfere: tendentsii i vyzovy / A. V. Yedemskiy // Vestnik nauki. — 2023. — T. 2, № 8(65). — S. 6-19. — EDN LBOTBS.

3. Bartoshko, T. V. Zashchita personal'nykh dannykh kak vazhnaya sostavlyayushchaya obshchey bezopasnosti banka / T. V. Bartoshko, A. P. Sterkhov // Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta. — 2015. — № 5(100). — S. 177-182. — EDN RWCCZK.

4. Gorbunova, V. B. Finansovaya nesostoyatel'nost' predpriyatiy kak ugroza ekonomicheskoy bezopasnosti regiona / V. B. Gorbunova // Baltiyskiy ekonomicheskiy zhurnal. — 2024. — № 1(45). — S. 17-27. — DOI 10.46845/2073-3364-2024-0-1-17-27. — EDN GGVRED.

5. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob'yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Prikaz FSTEK ot 25.12.2017 g. № 239 // Solar Dozor. — URL: www.consultant.ru/document/cons_doc_LAW_294287/ (data obrashcheniya: 02.08.2024).

6. GOST 58833 «Zashchita informatsii. Identifikatsiya i autentifikatsiya. Obshchiye polozheniya» ot 01.05.2020 g. // Elektronnyy fond pravovykh i normativno-tekhnicheskikh dokumentov. — URL: docs.cntd.ru/document/1200172576/titles (data obrashcheniya: 02.08.2024).

7. GOST 70262 «Zashchita informatsii. Identifikatsiya i autentifikatsiya. Urovni doveriya identifikatsii» ot 01.01.2023 g. // Rosstandart. — URL: protect.gost.ru/default.aspx/document1.aspx?control=31&id=245656 (data obrashcheniya: 02.08.2024).

8. Ob ustanovlenii obyazatel'nykh dlya kreditnykh organizatsiy trebovaniy k obespecheniyu zashchity informatsii pri osushchestvlenii bankovskoy deyatel'nosti v tselyakh protivodeystviya osushchestvleniyu perevodov denezhnykh sredstv bez soglasiya kliyenta: Polozheniye Banka Rossii ot 17.04.2019 g. № 683-P // Garant. — URL: base.garant.ru/72246408/ (data obrashcheniya: 31.07.2024).

9. Ob ustanovlenii obyazatel'nykh dlya nekreditnykh finansovykh organizatsiy trebovaniy k obespecheniyu zashchity informatsii pri osushchestvlenii deyatel'nosti v sfere finansovykh rynkov v tselyakh protivodeystviya osushchestvleniyu nezakonnykh finansovykh operatsiy: Polozheniye Banka Rossii ot 20.04.2021 g. № 757-P // Garant. — URL: www.garant.ru/products/ipo/prime/doc/400824645/ (data obrashcheniya: 31.07.2024).

10. O trebovaniyakh k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv i o poryadke osushchestvleniya Bankom Rossii kontrolya za soblyudeniyem trebovaniy k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv: Polozheniye Banka Rossii ot 17.08.2023 g. № 821-P // Garant. — URL: www.garant.ru/products/ipo/prime/doc/408082189/ (data obrashcheniya: 31.07.2024).

11. GOST 57580.1 «Zashchita informatsii finansovykh organizatsiy. Bazovyy sostav organizatsionnykh i tekhnicheskikh mer» ot 08.08.2017 g. // Garant. — URL: base.garant.ru/72031046/ (data obrashcheniya: 02.08.2024).

12. O standartizatsii v Rossiyskoy Federatsii: Federal'nyy zakon ot 29.06.2015 № 162-FZ (s izmeneniyami i dopolneniyami) // Garant. — URL: base.garant.ru/71108018/ (data obrashcheniya: 02.08.2024).

13. STO BR BFBO-1.8-2024 «Obespecheniye bezopasnosti finansovykh servisov pri provedenii distantsionnoy identifikatsii i autentifikatsii. Sostav mer zashchity informatsii» // Garant. — URL: www.cbr.ru/Crosscut/LawActs/File/7706 (data obrashcheniya: 02.08.2024).

14. Apatova, N. V. Upravleniye protsessami tsifrovoy transformatsii biznesa / N. V. Apatova // Uchenyye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo // Ekonomika i upravleniye. — 2022. — T. 8, № 2. — S. 3-8. — EDN SCWJEG.

15. Burkaltseva, D. D. Istoriya razvitiya teoriy kontseptsii ekonomicheskoy bezopasnosti / D. D. Burkaltseva // Voprosy istorii. — 2023. — № 6-1. — S. 122-127. — DOI 10.31166/VoprosyIstorii202306Statyi18. — EDN FIKIYG.

16. Ob ustanovlenii zapreta na dopusk programmnogo obespecheniya, proiskhodyashchego iz inostrannykh gosudarstv, dlya tseley osushchestvleniya zakupok dlya obespecheniya gosudarstvennykh i munitsipal'nykh nuzhd: Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 16 noyabrya 2015 g. № 1236 (s izmeneniyami i dopolneniyami) // Garant. — URL: base.garant.ru/71252170/ (data obrashcheniya: 31.07.2024).

17. Apatova, N. V. Ekonomicheskoye razvitiye i ekonomicheskiy rost: osnovnyye oriyentiry v tsifrovoy ekonomike / N. V. Apatova // Uchenyye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. Ekonomika i upravleniye. — 2023. — T. 9, № 3. — S. 3-14. — EDN HUYBZL.

18. Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Prikaz FSTEK Rossii ot 18.02.2013 № 21 (red. ot 14.05.2020) // FSTEK Rossii. — URL: fstec.ru (data obrashcheniya: 31.07.2024).

Статья поступила в редакцию 22 октября 2024 года

Статья одобрена к печати 18 ноября 2024 года