DOI: 10.17747/2618-947X-2026-1-73-83
УДК 332

Стратегия обеспечения информационной безопасности предприятия: мониторинг и управление

Т.А. Рудакова[1, 2]
О.Ю. Рудакова[2]
[1] Алтайский государственный технический университет им. И.И. Ползунова (Барнаул, Россия)
[2] Алтайский государственный университет (Барнаул, Россия)

Аннотация

Защищенность информации экономического субъекта и инфраструктуры, которая ее обеспечивает, остается одним из вызовов на современном этапе экономических отношений. Несанкционированный доступ к информации, случайные или злонамеренные воздействия на информацию, вторжение третьих лиц в работу поддерживающей инфраструктуры грозят уменьшением экономических выгод и нанесением ущерба экономическим субъектам – как юридическим, так и физическим лицам. В этих условиях одной из задач службы экономической безопасности организации становится предотвращение угроз и купирование рисков несанкционированного доступа к чувствительной и финансовой информации о предприятии и персональным данным сотрудников. Цель исследования – разработка методических рекомендаций по организации процесса управления рисками информационной безопасности предприятия. В ходе исследования авторами получены следующие научные результаты: в сравнительном аспекте рассмотрены элементы информационной безопасности (защита информации, ограничение доступа к информации, шифрование, система безопасности, двухфакторная аутентификация, передача информации, подделка документов, проверка уязвимости источника информации, подлинность информации) – современное состояние и в ретроспективе; систематизирована информация о хищениях информации и способах несанкционированного доступа к ней; проведен анализ факторов, ограничивающих соблюдение принципов защиты персональных данных, систематизированы риски информационной безопасности в контексте объект – уязвимость – угроза. Практическое применение результатов исследования заключается в возможности их интеграции в систему менеджмента организации и построения системы внутреннего контроля для минимизации угроз и купирования рисков несанкционированного доступа к чувствительной и финансовой информации и персональным данным сотрудников.

Ключевые слова: персональные данные, чувствительная и финансовая информация, риск несанкционированного доступа

Для цитирования:
Рудакова Т.А., Рудакова О.Ю. (2026). Стратегия обеспечения информационной безопасности предприятия: мониторинг и управление. *Стратегические решения и риск-менеджмент*, 17(1): 73–83. DOI: 10.17747/2618-947X-2026-1-73-83.

Enterprise Information Security Strategy: Monitoring and Management

T.A. Rudakova[1, 2]
O.Yu. Rudakova[2]
[1] Altai State Technical University named after I.I. Polzunov (Barnaul, Russia)
[2] Altai State University (Barnaul, Russia)

Abstract

The security of an economic entity's information and the infrastructure that supports it remains one of the key challenges at the current stage of economic relations. Unauthorized access to information, accidental or malicious impacts on information, and third-party intrusion into the operation of the supporting infrastructure threaten to reduce economic benefits and cause damage to economic entities, both legal entities and individuals. Under these conditions, one of the tasks of an organization's economic security service is to prevent threats and mitigate risks related to unauthorized access to sensitive and financial information about the enterprise and to employees' personal data. The objective of the study is to develop methodological recommendations for organizing the process of managing enterprise information security risks. In the course of the study, the authors obtained the following scientific results: the elements of information security (information protection, access restriction, encryption, security system, two-factor authentication, information transfer, document forgery, verification of the vulnerability of the information source, and information authenticity) were examined comparatively, considering both their current state and their historical development; information on participants involved in information theft and methods of unauthorized access was systematized; factors limiting compliance with personal data protection principles were analyzed; and information security risks were systematized in the context of object-vulnerability-threat. The practical significance of the research results lies in the possibility of integrating them into an organization's management system and developing an internal control system to minimize threats and mitigate the risks of unauthorized access to sensitive and financial information and employees' personal data.

Keywords: personal data, sensitive and financial information, risks of unauthorized access

For citation:

Rudakova T.A., Rudakova O.Yu. (2026). Enterprise Information Security Strategy: Monitoring and Management. *Strategic Decisions and Risk Management*, 17(1): 73-83. DOI: 10.17747/2618-947X-2026-1-73-83. (In Russ.)

企业信息安全保障战略：监测与管理

T.A. Rudakova[1, 2]
O.Yu. Rudakova[2]
[1] 波尔祖诺夫阿尔泰国立技术大学（巴尔瑙尔，俄罗斯）
[2] 阿尔泰国立大学（巴尔瑙尔，俄罗斯）

摘要

经济主体信息及其保障该信息运行的基础设施的安全性，仍然是当前经济关系发展阶段面临的挑战之一。对信息的未授权访问、对信息的偶然或恶意影响，以及第三方侵入相关支撑基础设施的运行，都会导致经济利益受损，并对经济主体—无论是法人还是自然人—造成损害。在这种背景下，组织经济安全部门的任务之一，就是防范威胁并控制企业敏感信息、财务信息以及员工个人数据遭受未授权访问的风险。本文旨在提出关于企业信息安全风险管理流程组织的方法建议。研究过程中，作者取得了以下成果：从比较视角考察了信息安全各项要素—包括信息保护、信息访问限制、加密、安全系统、双因素认证、信息传输、文件伪造、信息来源脆弱性检验以及信息真实性—的现状及其历史演变；系统梳理了信息窃取及未授权访问信息的方式；分析了制约个人数据保护原则落实的因素，并在"对象—脆弱性—威胁"框架下系统归纳了信息安全风险。研究结果的实践意义在于，可将其整合到组织管理体系和内部控制体系建设中，以最大限度减少针对敏感信息、财务信息和员工个人数据的未授权访问威胁，并控制相关风险。

关键词： 个人数据，敏感信息与财务信息，未授权访问风险

引用格式：

Rudakova T.A., Rudakova O.Yu. (2026)。企业信息安全保障战略：监测与管理。战略决策与风险管理, 17(1): 73–83. DOI: 10.17747/2618-947X-2026-1-73-83. （俄文）

Введение

Глобализация процесса цифровой трансформации мировой экономики сопровождается развитием информационных технологий и появлением инновационных технических решений, интегрируемых во все сферы экономики и государственного управления. Активным участникам процесса это дает ряд преимуществ в конкурентной среде, способствует снижению издержек, повышению качества предоставляемых услуг, росту эффективности производственных процессов, увеличению экономических выгод в текущих условиях с прогнозом аналогичных преимуществ в будущем. Положительные моменты происходящих изменений не исключают существование негативных сторон этого процесса, к которым следует отнести потенциальную информационную уязвимость экономических субъектов.

Информация как продукт обмена в экономическом пространстве выполняет роль источника данных об интересующем субъекте хозяйствования. Задачей лица, ее формирующего, в современных условиях является не только достоверное содержание передаваемых сообщений, но и ограждение от несанкционированных фактов воздействия. В круг задач по сохранению данных от несанкционированного доступа и вмешательства в содержание информации входит и защита поддерживающей ее инфраструктуры, или информационная безопасность, как принято ее сегодня характеризовать. Большинство авторов научных работ и практиков, занимающихся вопросами оценки защищенности данных информационных источников и инфраструктуры, считают, что вероятность несанкционированного доступа к данным хозяйствующих субъектов потенциально возможна. Прогнозирование и предотвращение таких воздействий зависит от ряда факторов, а эффективность управления такими событиями способствует минимизации ущерба в результате их возникновения. В августе 2025 года российский аналитический портал и интернет-издание TAdviser, специализирующееся на теме корпоративной информатизации, провели опрос, участниками которого выступали как эксперты, так и представители бизнес-структур; по данным этого опроса, «две из трех российских компаний (67%) можно взломать менее чем за сутки и более чем в 60% случаев реализовать событие, которое могло бы остановить работу бизнеса»[1]. Из этого следует, что декларируемый уровень киберзащиты информации бизнес-структур намного ниже фактического, а риски и потенциальные угрозы остаются недооцененными, при этом время, необходимое для подключения к интересующей системе данных, неуклонно сокращается. Разработчики инновационных решений в области информационной безопасности обозначили причины происходящего.

В первую очередь это решение менеджментом организации приоритетных для себя задач, таких как своевременное предоставление отчетов инвесторам и государственным институтам, организация проверочных мероприятий и получение положительного аудиторского заключения о достоверности отчетной информации, эффективности системы управления и соблюдении принципа непрерывности деятельности.

На второй план уходит защита информации и доступ к ней недобросовестных пользователей. Недооценивание темпов развития современных технологий и инновационных ИТ-решений и опережающие темпы их использования в противоправных действиях делает уязвимой информационную систему экономического субъекта, а удобство применяемых технологий зачастую снижает ее стойкость. В результате у руководства складывается впечатление о наличии управляемого риска. Однако специалисты обращают внимание на присутствующие слабые стороны в части информационной безопасности, к которым относят идентификацию, аутентификацию, вопросы предоставляемых привилегий а именно «разросшиеся права в Active Directory, сервисные учетные записи без MFA, устаревшие и повторно используемые пароли, «вечно живые» VPN-доступы подрядчиков», а также «..наследованные Windows-среды, неуправляемые

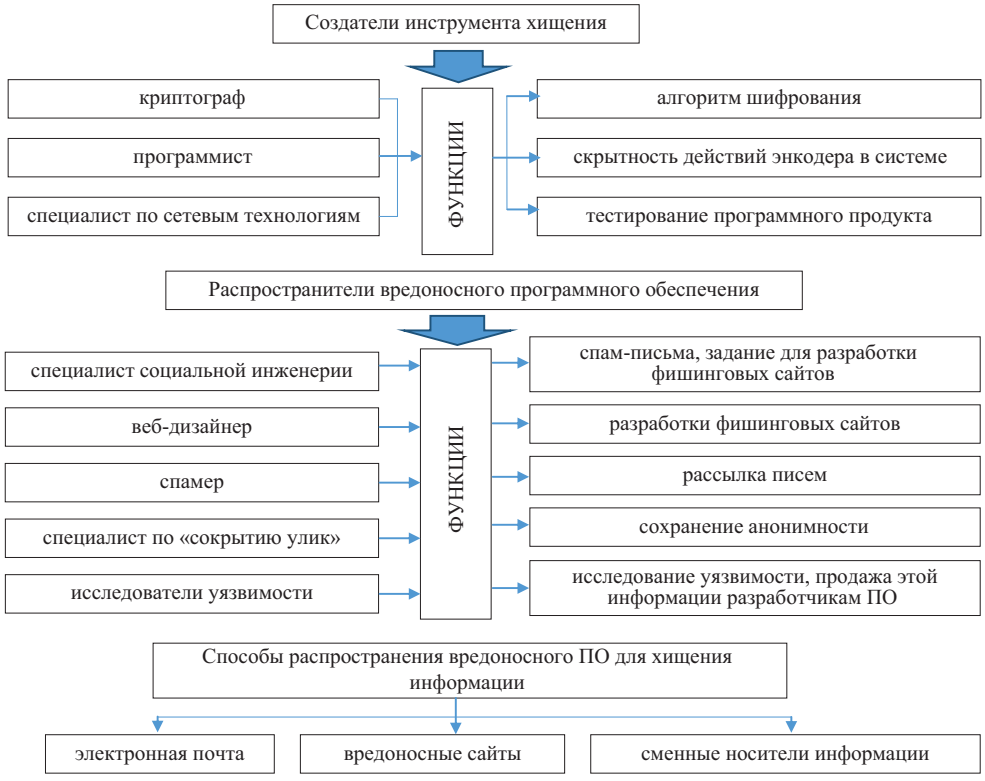
[1] Информационная безопасность в компании. https://clck.ru/3Pt26q/.

обновления, слабая сегментация, из-за чего компрометация пользовательского узла превращается в отказ ключевых систем»[2].

Информационная безопасность организации, проблемы и факторы, ограничивающие правовую защиту данных, в том числе персонального характера, стали предметом исследования большого объема научных публикаций отечественных и зарубежных авторов. Так, влияние технологии больших данных и инструментов, разработанных не ее основе для защиты персональных данных, оценена в [Савельев, 2015]. Информационная безопасность и стандарты индустрии безопасности платежных карт сопоставлены в [Борхаленко, 2015]. Результаты библиометрического анализа атак фишинга и WhatsApp[3] с использованием Vosviewer представлены в [Sujiwana et al., 2024]. Международная правовая регламентация цифрового пространства освещена в [Ястребова, 2025]. Киберпреступность в современном мире и организация борьбы в отдельных странах Глобального Юга стали предметом научных размышлений в [Цыплакова, 2025]. Авторы работы [Селиванова, Конопий, 2025] оценили участие интеллектуальных систем в процессе принятия решений в периметре правового поля с позиции юридического статуса искусственного интеллекта. Обнаружение атак на корпоративные сети с использованием системы объяснимого искусственного интеллекта определены как цель в работе [Yaz, Süzen, 2023]. По мнению авторов статьи [Van Deursen et al., 2013], необходимо в процессе мониторинга рисков информационной безопасности учитывать влияние человеческих и социальных факторов. Для определения и оценки угроз информационной безопасности в [Jouini, 2015] предложена количественная модель риска. Роли финансовой и нефинансовой информации в концепции кибербезопасности посвящено исследование [Cristea, 2020]. В [Lee, 2011] представлена модель оптимизации прибыли от инвестиций в информацию о безопасности клиентов.

1. Несанкционированный доступ к информации

Словари русского языка дают определение: «санкционировать – дать разрешение». Отсюда следует, что информация, полученная без разрешения ее создателя, может рассматриваться как кража. Несанкционированный доступ к информации в современных условиях цифровой трансформации социально-экономических процессов – это угроза и серьезная проблема, затрагивающая интересы как частных лиц, так и организаций независимо от размера, форм собственности, отраслевой принадлежности. Несанкционированный доступ к информации как явление обращает на себя внимание исследователей с начала компьютерной эры. Участники хищения информации и способы получения представлены на рис. 1.



Источник: составлено авторами.

Рис. 1. Участники хищения информации и способы несанкционированного доступа
Fig. 1. Actors Involved in Information Theft and Methods of Unauthorized Access

[2] Информационная безопасность в компании. https://clck.ru/3Pt26q/.
[3] Принадлежит компании Meta, деятельность которой признана экстремистской, запрещена на территории РФ.

Процесс хищения информации предполагает участие создателей инструментов хищения, распространителей вредоносного программного обеспечения, наличие интересующих объектов, каналы подключения к местам хранения информации. Создателями инструментов хищения информации могут выступать как несколько, так и один специалист при наличии у него необходимых компетенций в области создания алгоритма шифрования, обеспечении скрытности действий энкодера в системе и способности тестирования программного продукта. Распространение вредоносного ПО обеспечивают специалисты социальной инженерии, веб-дизайнеры, спамеры, специалисты, в функции которых входят сохранение анонимности и исследования уязвимости программного обеспечения.

2. Технологические инновации и риски утечки информации

Основные пути доступа к информации – это электронная почта при отсутствии спам-фильтра и антивирусной программы, вредоносные сайты, которые посещает пользователь, или приложения, которые он скачивает на устройство, и сменные носители информации, которые могут быть заражены вредоносными программами. В любом из этих случаев основным виновником доступа к информации является пользователь устройства – персонального компьютера, планшета, телефона.

В 2025 году появился вирус-вымогатель, способный внедряться в микрокод процессоров. Об этом на одной из конференций сообщил старший директор по аналитике угроз компании *Rapid7* К. Бейк, который и является создателем демонстрационного вредоноса, наделенного способностями внедряться в микрокод процессора AMD Zen (устанавливаются в широкий спектр устройств, включая настольные компьютеры, ноутбуки, серверы и встраиваемые системы) и изменять его поведение. Он скрыт от традиционных систем защиты, что делает угрозу особенно серьезной. По мнению Бейка, специалисты в области кибербезопасности более увлечены продвинутыми технологиями, в число которых входит искусственный интеллект, оставляя без должного внимания проблемы кибербезопасности[4].

Список технологических инноваций в области получения, хранения и передачи информации пополнился инструментами на базе генеративного искусственного интеллекта, которых сегодня насчитывается более двух тысяч; применяются они в самых разных областях. Внедрение инструментов происходит с большой скоростью и набирает популярность, стремительно развиваются различные платформы, а это – свидетельство широкого применения и демонстрация потенциала трансформации социально-экономических процессов.

По данным Ассоциации больших данных в сотрудничестве с консалтинговой компанией «Б1» и TAdviser, рынок больших данных демонстрирует серьезные темпы роста в 2024 году по сравнению с 2023-м. Практически все сегменты: услуги, прикладное программное обеспечение и инфраструктура – имеют темпы роста в диапазоне от 26 до 33% (табл. 1).

В структуре сегмента «Услуги» наибольший темп роста демонстрирует аналитика и DaaS (данные как услуга) (табл. 2). Наибольший темп роста в сегменте «Программное обеспечение» – 139,9%, или 13 млрд руб., – наблюдается в составе аналитического ПО (ИИ-платформы) (табл. 3).

Таблица 1
Рынок больших данных и искусственного интеллекта в России
Table 1
Big Data and Artificial Intelligence Market in Russia

Показатель	Объем рынка (млрд руб.)		Темпы роста	
	2023	2024	в стоимостном выражении (млрд руб.)	в относительном выражении (%)
Услуги	179	239	60	133,51
Прикладное программное обеспечение	95	127	32	133,68
Инфраструктура	53	67	14	126,41
Итого	327	433	106	132,41

Источник: составлено авторами по данным TAdviser: https://www.tadviser.ru/a/910779.

Таблица 2
Услуги рынка больших данных и искусственного интеллекта в России
Table 2
Services Segments of the Big Data and Artificial Intelligence Market in Russia

Показатель	Объем рынка (млрд руб.)		Темпы роста	
	2023	2024	в стоимостном выражении (млрд руб.)	в относительном выражении (%)
ИТ-консалтинг, бизнес-консалтинг, разметка данных и поддержка обучения моделей	85	105	20	123,5
Аналитика и DaaS				
Рекламные дата-продукты	44	67	23	152,2
Нерекламные дата-продукты	50	67	17	134

Источник: составлено авторами по данным TAdviser: https://www.tadviser.ru/a/910779.

Таблица 3
Программное обеспечение на рынке больших данных и искусственного интеллекта в России
Table 3
Software in the Big Data and Artificial Intelligence Market in Russia

Показатель	Объем рынка (млрд руб.)		Темп роста	
	2023	2024	в стоимостном выражении (млрд руб.)	в относительном выражении (%)
Прикладное программное обеспечение	29	39	10	134,48
Цифровая инфраструктура	22	29	7	131,81
Аналитическое ПО ИИ-платформы	33	46	13	139,39
BI, EPM, IBP аналитика, геоинформационные системы, поисковое ПО и ПО для интеллектуальной работы с контентом	11	13	2	118,18

Источник: составлено авторами по данным TAdviser: https://www.tadviser.ru/a/910779.

[4] Георгиев Р. (2025). Создан шифровальщик, внедряемый прямо в микрокод процессоров. https://cnews.ru/link/a640902.

Использование возможностей инструментов на базе генеративного искусственного интеллекта в решении профессиональных задач сотрудниками организаций несет в себе риски передачи в загружаемых файлах и в содержании промптов персональной, платежной и чувствительной информации. Это нельзя рассматривать как несанкционированный доступ к персональным данным и корпоративной информации – скорее, как отсутствие корпоративной культуры и непрофессиональное поведение сотрудников по причине неэффективного функционирования системы внутреннего контроля и системы управления рисками.

У менеджмента бизнес-структур возникает потребность в разработке регламента работы с инструментами генеративного искусственного интеллекта, в противном случае риски утечки персональных данных способны привести к финансовым потерям в виде штрафа в размере 15 млн руб. за первую утечку и 3% оборота компании – при повторении инцидента и отсутствии возможности найти виновника[5].

Возможности современных инновационных технических решений во многом определяются массивом информационных данных, которыми загружены все возможные технические устройства по причине перевода социально-экономических процессов в виртуальное пространство посредством сети Интернет. Объем данных увеличивается в геометрической прогрессии, и справиться с ними традиционными средствами уже не представляется возможным. В этом случае на помощь приходит генеративный искусственный интеллект или инструменты, разработанные на его базе, позволяющие генерировать любую информацию, попавшую в базу данных, и здесь следует заметить – не всегда с согласия индивидов (в части персональных данных) и юридического лица (в части финансовой и чувствительной информации для юридического лица). Такова природа технологий анализа больших данных как совокупности инструментов и методов, предназначенных для обработки и структурирования постоянно меняющегося большого потока данных, определяющих возможность применения инструментов генеративного искусственного интеллекта, являющихся его основой – базисом для функционирования [Савельев, 2015].

Сегодня информация играет главную роль в различных сферах как предпринимательской деятельности, так и в сфере государственного управления, ее не без основания наделили качеством товара – «новой нефтью» [Arthur, 2013] – и включили в перечень факторов производства. Качество актива и его объем позволяют обладателям информации при наличии необходимых технических возможностей занимать одно из приоритетных звеньев в цепочке создания добавленной стоимости, повышать производительность, сокращать издержки и, как следствие, способствовать росту темпов развития индустрии – технологий и сервиса, поддерживающих анализ данных.

3. Информационная безопасность: ретроспективный аспект

Передача и хранение информации от нежелательного вмешательства в ее содержимое и использование данных в корыстных целях ставили перед создателями информации задачи не только по обеспечению ее подлинности, но и по ограничению несанкционированного доступа к документу. Об этом свидетельствуют результаты исследований периода зарождения криптографии как явления, которые подтверждают озабоченность вопросами информационной безопасности (табл. 4).

Система, контролирующая и фильтрующая сетевой трафик в современном мире и способствующая предотвращению несанкционированного доступа к устройству или компьютерной сети, – фаерволы – заменила использу-

Таблица 4
Элементы информационной безопасности
Table 4
Information Security Elements: Modern Practices and Historical Analogues

Термины	Современность	Аналог в истории
Защита информации	Антивирусы	Двойные конверты – с незначимой и значимой информацией, дублирование писем, тайные метки и стеганография на пергаменте
Ограничение доступа к информации	Разделение прав доступа посредством индивидуального пароля	Разделение ключей зашифрованной информации между гонцами
Шифрование	Кодирование информации с целью предотвращения несанкционированного доступа	Гомофоническое шифрование для информационный энтропии (мера неопределенности)
Система безопасности	Фаерволы – система, которая контролирует и фильтрует сетевой трафик, чтобы предотвратить несанкционированный доступ к компьютерной сети или устройству	Воск, пергамент и головы гонцов
Двухфакторная аутентификация	Два разных фактора для подтверждения личности при входе в аккаунт или систему, биометрия	Восковая печать для скрепления письма, почерк
Передача информации	Почта, электронная почта	Гонцы
Подделка документов	Атака на цепочку поставок (Supply Chain Attack) – кибератака, при которой злоумышленники используют уязвимости в цепочке поставок ПО или оборудования для получения доступа к системам целевой организации	Подделка информации посредством изменения текста письма на пергаменте: текст либо изменяется, либо вписывается позже после подписи пергамента
Проверка уязвимости источника информации	Баг-баунти (bug bounty) – открытый конкурс по поиску уязвимостей в программном продукте	Сообщения о подделках гербов и печатей
Подлинность информации	Электронная подпись	Сургучная, восковая печать

Источник: составлено авторами.

[5] Ст. 13.11 Кодекса РФ об административных правонарушениях от 30.12.2001 # 195-ФЗ (ред. от 04.11.2025). https://www.consultant.ru/document/cons_doc_LAW_34661/.

емые в XIV веке воск, пергамент и головы гонцов, отвечающих за сохранность и доставку информации от создателя до получателя. В настоящее время одним из основных способов передачи и обмена большим количеством данных остается электронная почта (исторически эту функцию выполняли гонцы). Ограничением для несанкционированного доступа к информации являлось гомофоническое шифрование содержимого информации, размещенной на пергаменте, что обеспечивало ее неопределенность (энтропию). Шифрование или кодирование как инструмент защиты информации используется и в настоящее время. Исторически разработка шифра лежала на его создателе; в дипломатической переписке часто использовался гомофонический шифр информации, когда буквы заменялись символами, причем для обозначения одной и той же буквы использовались разные символы; уровень грамотности самого шифровальщика не позволял понять содержание такого письма. Кроме того, информацию защищали от утраты и перехвата посредством дублирования гонцов, разделяя ключи защищенной информации между ними [Ларин, 2010].

В настоящее время ограничение доступа к информации определяется разделением прав доступа посредством индивидуального пароля, использованием двух разных факторов для подтверждения личности при входе в аккаунт или системой биометрии; раньше эти функции выполняли восковая печать и почерк автора письма. В современных условиях защиту информации, передаваемой по телекоммуникационным каналам связи, защищают с помощью программных продуктов – антивирусов; в древности использовались способы двойных конвертов, когда в одном из них содержалась незначимая информация, а во втором – подлежащая передаче получателю. Нередко письма дублировались для большей вероятности «добраться» по назначению, использовались тайные метки для усложнения возможности воспользоваться содержимым при перехвате письма. Подлинность информации подтверждалась скреплением письма восковой печатью, которую имел каждый важный человек – епископ, герцог, король. Современным аналогом такого инструмента является электронная подпись, которая имеет разные способы защиты в зависимости от владельца и значимости документа, который удостоверяется.

Тем не менее, несмотря на наличие различных инструментов, соответствующих времени развития социальных и экономических отношений, всегда существовала подделка информации посредством изменения текста письма на пергаменте и бумаге, когда он либо изменялся, либо вписывался позднее, после подписи.

Современное общество сталкивается с атаками на цепочку поставок (Supply Chain Attack) – кибератаками, когда злоумышленники используют уязвимости в цепочке поставок программного обеспечения или оборудования для получения доступа к системам целевой организации. В таком случае информация становится доступной и может быть использована преступниками для вымогательства и шантажа. В настоящее время одним из способов борьбы с киберпреступниками является проверка уязвимости источника информации – баг-баунти (bug bounty) – открытый конкурс по поиску уязвимостей в программном продукте. Это можно сравнить с сообщениями людей о подделках гербов и печатей в древности: если сообщения не подтверждались, то источник мог быть жестоко наказан за недостоверность информации в доносе.

4. Стандартизация процесса информационной безопасности и защита персональных данных

Построение системы информационной безопасности организации является одной из приоритетных задач менеджмента. Регулирование данного процесса опирается на действующие стандарты национального либо международного характера. Федеральный закон «О техническом регулировании»[6] и государственный стандарт ГОСТ Р 1.0–2004 «Стандартизация в РФ. Основные положения»[7] определили правила стандартизации и применения национальных стандартов. Национальные стандарты информационной безопасности разрабатывались на базе международного опыта и стандартизации. В тексте действующего в настоящее время стандарта ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»[8] делаются ссылки на международные стандарты, однако только в том случае, если отсутствует аналог национального документа. Поскольку стандарты национального характера постоянно претерпевают изменения, то рекомендуется с целью корректного использования стандарта ГОСТ Р ИСО/МЭК 27005–2010 следить за изменениями в содержании национальных документов[9, 10, 11, 12].

Нормы защиты персональных данных закреплены как международным правом, так и нормативными документами национального характера. Следует отметить, что международная практика была озабочена проблемой несанкционированного доступа к персональным данным намного раньше отечественной. Конвенция о защите физических лиц в процессе сбора персональных данных принята Советом

[6] Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ. https://www.consultant.ru/document/cons_doc_LAW_40241/.
[7] ГОСТ Р 1.0-2004. Национальный стандарт РФ. «Стандартизация в Российской Федерации. Основные положения» (утв. Приказом Ростехрегулирования от 30.12.2004 № 152-ст).
[8] ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт РФ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (от 01.12.2011).
[9] ГОСТ Р ИСО/МЭК 27001-2021. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
[10] ГОСТ Р ИСО/МЭК 27002-2021. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности» от 30.11.2021.
[11] ГОСТ Р ИСО/МЭК 16085-2007. «Менеджмент риска. Применения в процессах жизненного цикла систем и программного обеспечения» от 01.09.2008.
[12] ГОСТ ISO/IEC 29100-2021. Межгосударственный стандарт «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных» от 30.11.2021.

Европы еще в 1981 году в Страсбурге, что стало отправной точкой в принятии странами Европы национальных законов и рядов директив ЕС[13, 14, 15, 16, 17].

Национальная правовая система пополнилась Федеральным законом 2006 года №152-ФЗ «О персональных данных»[18], вступившем в силу в 2007 году после ратификации в 2005 году Конвенции Совета Европы.

Это позволяет утверждать, что правое поле содержит достаточное количество норм в части защиты персональных данных, но возникают сомнения по соблюдению указанных норм всеми участниками информационного обмена – как на этапе сбора и обработки информации, так и на этапе передачи и генерации новых данных. Физические лица на добровольной основе оставляют персональные данные не только работодателям и государственным институтам, которые берут на себя обязательства по их сохранности, но и в мессенджерах, на электронных площадках, интернет-ресурсах. В результате персональные данные пополняют базу больших данных и дают возможность генерации на их основе новой информации за счет объединения с другими данными, не сочетающимися ни с целями размещения, ни с целями обработки персональных данных (табл. 5).

Несоблюдению принципа соответствия целям сбора оператором персональных данных способствует ряд обстоятельств, таких как техническая возможность работодателя в части работы с персональными данными сотрудников и наличие мощностей, обеспечивающих хранение копий документов кадрового отдела, квалификация персонала, имеющего доступ к персональным данным сотрудников, цифровая грамотность и работа с персональными данными в процессе использования инструментов генеративного искусственного интеллекта для решения профессиональных задач, несоблюдение цифровой гигиены сотрудниками и др., а также отсутствие гарантии того, что экономический субъект, предоставляющий возможность хранения персональных данных арендатору на своем ресурсе, не прекратит свою деятельность до окончания срока договора как добровольно, так и принудительно с привлечением института банкротства.

Все больше организаций решают задачи управления кадровым потенциалом, используя возможности облачных технологий. Безопасность кадровых документов после заключения договора с организацией становится обязанностью поставщика облачных решений, что для заказчика услуги сопряжено с определенными рисками в области информационной безопасности. Объясняется это тем, что облачный провайдер является собственником такой инфраструктуры[19]. Преимущества, которые получает организация от хранения данных в публичном облаке, не снимают с нее обязанность по соблюдению мер информационной безопасности и защиты персональных данных и требуют соблюдения организационных и технических мер, позволяющих сохранять документы продолжительное время и делать их доступными. Юридическую значимость документов (электронную подпись) способны поддерживать не все облачные решения кадрового документооборота, также не все могут обеспечивать их долговременное хранение. Следовательно, организация-заказчик должна иметь возможность после выгрузки документов разместить их на собственном сервере.

Анализ нормативных документов и источников научного характера позволяет сделать неутешительный вывод

Таблица 5
Принципы защиты персональных данных, имеющие ограничения в части их соблюдения
Table 5
Personal Data Protection Principles with Barriers to Their Compliance

Принципы	Ограничения соблюдения принципов защиты персональных данных
Добровольное согласие физического лица при условии информирования о цели оператора	Большой объем информации оператора о целях обработки, с которым сложно ознакомиться в момент доступа на ресурс Сложность изложения информации оператором персональных данных, требующего от физического лица наличия компетенций юридического характера
Невозможность объединения персональных данных с другими источниками и генерации новой информации	Философия технологии анализа больших данных – повторное использование данных Накопление персональной информации, добровольно оставленной на различных электронных площадках, сайтах, в мессенджерах и других источниках
Соответствие целям сбора персональных данных оператором	Технические ограничения Квалификация персонала Цифровая грамотность персонала Несоблюдение цифровой гигиены сотрудниками оператора персональных данных Соблюдение принципа непрерывности деятельности экономического субъекта, арендодателя облачных пространств Фишинг

Источник: составлено авторами.

[13] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28.01.1981) вместе с поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми комитетом министров в Страсбурге 15.06.1999.

[14] Регламент (ЕС) 2016/679 Европейского парламента и Совета ЕС «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС (Общие правила защиты данных)».

[15] Директива Европейского парламента и Совета Европейского союза 2002/58/ЕС от 12.07.2002 в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи).

[16] Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (резолюция 79/243 Генеральной Ассамблеи ООН от 24.12.2024).

[17] Фадеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». https://www.consultant.ru/document/cons_doc_LAW_57153/.

[18] Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных». https://www.consultant.ru/document/cons_doc_LAW_61801/.

[19] Кадровые архивы в облаке: безопасно ли хранить персональные данные вне компании? https://www.tadviser.ru/a/871609.

о том, что несанкционированный доступ к персональной и чувствительной информации, интересующий всех участников социально-экономических отношений и рыночного пространства, остается актуальным в современных условиях и не потеряет своей значимости в ближайшем будущем. Это объясняется трансформационными процессами, происходящими как в экономике, так и в обществе под влиянием цифровизации, перевода информации в облачные пространства, освоения новых видов технологических достижений в эпоху больших данных, создания и развития инструментов генеративного искусственного интеллекта. Процесс цифровизации может занимать продолжительный период, и каждый новый этап развития технологий будет сопровождаться вызовами для его участников, порождать новые проблемы и ставить новые задачи.

На современном этапе социально-экономического развития в состав базовых вызовов следует включить несанкционированный доступ к информации, его причины и способы предотвращения. Участники социально-экономических отношений должны быть готовы их принимать. В первую очередь речь идет о компетенциях, которыми должен обладать каждый участник информационного обмена. Руководители организаций и государственных институтов должны обладать компетенциями не только управления, но и построения системы информационной безопасности как корпоративного, так и персонального характера, а для этого необходим мониторинг развития и совершенствования новейших технологий в области информационной безопасности и ограничений несанкционированного доступа к персональным данным сотрудников. Физическим лицам в зависимости от возрастных особенностей и ограничений необходимо прививать правила цифровой гигиены. Учитывая, что информация сегодня – это товар, имеющий коммерческую ценность, менеджмент организации должен позаботиться о сохранении ее стоимости в прямом и переносном смыслах, выделяя для этого приоритетные направления и задачи.

5. Мониторинг и управление рисками информационной безопасности на предприятии

В контексте информационной безопасности для организации работы по купированию потенциальных угроз и минимизации рисков целесообразно на первом этапе выделить объект, который может быть подвержен угрозе, определить характеристики инструмента или актива, который может быть использован для реализации угрозы и способствовать возникновению риска, и определить перечень потенциальных негативных событий в результате уязвимости объекта (рис. 2).

Второй этап организации процесса управления должен быть посвящен детализации информации об объектах, характеристике их уязвимости, конкретизации потенциальных угроз и последствий их реализации для организации (табл. 6).

Распределение функциональных обязанностей по мониторингу и контролю за объектами системы информационной безопасности между подразделениями (центрами ответственности) системы управления в организации и конкретными сотрудниками системы менеджмента может зависеть от ряда факторов, связанных с размером бизнеса, финансовыми возможностями, особенностями организационной структуры предприятия, кадрового обеспечения и т. д.

Как показывают исторические данные и настоящие потребности бизнеса, информационная безопасность как элемент экономической безопасности субъекта хозяйствования будет занимать одно из первых мест в перечне задач, требующих решения в краткосрочной перспективе. Способствует этому стремительный рост объемов информации, перевод ключевых процессов жизнедеятельности в интернет, возрастание роли информации как продукта в предпринимательской деятельности и системе государственного управления. Информационные технологии способствовали тому, что многие процессы и общественные отношения с переводом в онлайн-среду сделали возможным

Источник: составлено авторами по данным [Лапина и др., 2024].

Рис. 2. Элементы риска информационной безопасности
Fig. 2. Components of Information Security Risk

Таблица 6
Аппарат управления информационными рисками
Table 6
Information Risk Management Framework

Объект	Уязвимость	Угроза	Риски
Управление кадрами			
Персонал с соответствующими компетенциями	Недостаточный уровень квалификации в области информационных технологий	Несоблюдение цифровой гигиены Передача информации случайно или осознанно третьим лицам	Репутационные Финансовые
Управление рисками информационного характера			
Программное обеспечение	Принадлежность (зарубежные, национальные)	Отсутствие лицензии на использование ПО, либо дополнительные сложности в ее продлении или получении	Потеря информации Затраты на восстановление данных Финансовые потери по причине приостановления деятельности при переводе данных на другое ПО (выручка, прибыль, штрафы неустойки)
Мощность технических средств	Недостаточная мощность технических средств для хранения большого объема информации	Ограниченные сроком договора возможности обязательного долгосрочного хранения большого объема информации в облачных хранилищах	Утрата возможного доступа к информации длительного срока хранения (кадровая и др.)
Электронный документ	Несанкционированный доступ Ограниченные сроки хранения информации	Потеря юридической формы (цифровой электронной подписи при хранении кадровых и других документов в облаке на арендованном сервисе)	Утрата возможного доступа к информации длительного срока хранения
Персональная, чувствительная и финансовая информация	Низкий уровень защищенности информации от несанкционированного доступа	Кража, фальсификация, шантаж	Репутационные Финансовые

Источник: составлено авторами.

вторжение в частную жизнь индивида, изменили границы личного пространства. Разработан ряд нормативных актов, регламентирующих работу с информацией корпоративного и персонального характера, для предотвращения от несанкционированного доступа к ней, искажения и использования в мошеннических действиях. Однако этого недостаточно в силу стремительного развития информационных технологий, появления инновационных технических решений, позволяющих пользоваться информацией интернет-пространства, имеющей цифровой след. Для организации работы по минимизации угроз и купированию потенциальных информационных рисков экономического субъекта недостаточно обладать знаниями в области юриспруденции.

В системе менеджмента необходимо обратить внимание на решение следующих вопросов:

1. В системе управления рисками организации выделить объекты, на которые должно быть направлено пристальное внимание, определить их уязвимость, потенциальные угрозы и вероятности их последствий.

2. Для мониторинга и анализа происходящих событий с информацией организации и персональными данными сотрудников необходимо распределение полномочий и обязанностей между подразделениями и персоналом с целью недопущения несанкционированного доступа к чувствительной, финансовой информации и персональных данных.

3. Сотрудники организации должны на постоянной основе получать информацию о современных способах несанкционированного доступа к информации частного и корпоративного характера, совершенствовать компетенции по противодействию такому доступу. Несоблюдение правил цифровой гигиены сотрудниками повышает вероятность финансовых рисков не только для компании, но и для отдельной личности ст. 13.11 КоАП.

Организация процесса формирования и совершенствования компетенций сотрудников по работе с чувствительной информацией и персональными данными должна стать элементом системы управления персоналом организации. Это обеспечит нахождение экономического субъекта в правовом поле в части защиты персональных данных, минимизирует нарушение личных границ сотрудников и риски различного характера, включая финансовые.

Литература

Борхаленко В.А. (2015). Верификация требований стандарта pci DSS 3.1 на соответствие требованиям законодательства РФ. *Вопросы кибербезопасности*, 5(13): 11–15.

Лапина М.А., Медведева А.С., Лапин В.Г., Бойков Н.С., Ледян Д.И. (2024). Анализ рисков информационной безопасности экономических информационных систем. *Auditorium*, 2(42). https://cyberleninka.ru/article/n/analiz-riskov-informatsionnoy-bezopasnosti-ekonomicheskih-informatsionnyh-sistem.

Ларин Д.А. (2010). Защита информации в древней Руси. *История и архивы*, 12(55): 13–35.

Савельев А.И. (2015). Проблемы применения законодательства о персональных данных в эпоху больших данных (Big Data). *Право. Журнал ВШЭ*, 1: 43–66.

Селиванова Е.С., Конопий А.С. (2025). Юридически значимые признаки искусственного интеллекта и их влияние на правовой статус решений, принимаемых интеллектуальными системами. *Право и управление. XXI век*, 21(3): 49–61.

Цыплакова А.Д. (2025). Противодействие киберпреступлениям в отдельных странах Глобального Юга: современное состояние, проблемы и перспективы. *Право и управление. XXI век*, 21(3): 62–75.

Ястребова А.Ю. (2025). Понятие и защита персональных данных в контексте международно-правовой регламентации цифрового пространства. *Право и управление. XXI век*, 21(2): 15–25.

Arthur C. (2013). Tech Giants May Be Huge, but Nothing Matches Big Data. *Guardian*, August 23. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data/

Cristea L.M. (2020). Current Security Threats in the National and International Context. *Journal of Accounting and Management Information Systems*, 19(2): 351–378.

Jouini M.A. (2015). Multidimensional Approach towards a Quantitative Assessment of Security Threats. *Procedia Computer Science*, 52: 507–514.

Lee Y.J. (2011). Profit-Maximizing Firm Investments in Customer Information Security. *Decision Support Systems*, 51(4): 904–920.

Sujiwana R.K., Ridho A.F.A., Aryanti D.C., Rakhmawati N.A. (2024). Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer. *Jurnal Esensi Sistem Informasi dan Sistem Komputer*, 8(1): 101–105.

Van Deursen N., Buchanan W.J., Duff A. (2013). Monitoring Information Security Risks within Health Care. *Computers & Security*, 37: 31–45.

Yaz Ö., Süzen A.A. (2023). Kurumsal Ağlara Yapılan Saldırılarda Açıklanabilir Yapay Zekânın Yeri. *International Conference on Applied Engineering and Natural Sciences*, 1(1): 528–534.

References

Borhalenko V.A. (2015). Verification of the pci DSS 3.1 Standard for Compliance with the Requirements of the Legislation of the Russian Federation. *Cyberspace Issues*, 5(13): 11-15. (In Russ.)

Lapina M.A., Medvedeva A.S., Lapin V.G., Boikov N.S., Ledyan D.I. (2024). Information Security Risk Analysis of Economic Information Systems. *Audience*, 2(42). https://.cyberleninka.ru/article/n/analiz-riskov-informatsionnoy-bezopasnosti-ekonomicheskih-informatsionnyh-sistem. (In Russ.)

Larin D.A. (2010). Information Protection in Ancient Russia. *History and Archives*, 12(55): 13-35. (In Russ.)

Savelyev A.I. (2015). Problems of the Application of Legislation on Personal Data in the Era of Big Data. Law. *HSE Journal*, 1: 43-66. (In Russ.)

Selivanova E.S., Konopiy A.S. (2025). Legally Significant Features of Artificial Intelligence and Their Impact on the Legal Status of Decisions Made by Intelligent Systems. *Law and Management. XXI Century*, 21(3): 49-61 (In Russ.)

Tsyplakova A.D. (2025). Countering Cybercrime in Selected Countries of the Global South: Current State, Problems and Prospects. *Law and Management. XXI Century*, 21(3): 62-75. (In Russ.)

Yastrebova A.Yu. (2025). The Concept and Protection of Personal Data in the Context of the International Legal Regulation of the Digital Space. *Law and Management. XXI Century*, 21(2): 15-25. (In Russ.)

Arthur C. (2013). Tech Giants May Be Huge, but Nothing Matches Big Data. *Guardian*, August 23. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data/

Cristea L.M. (2020). Current Security Threats in the National and International Context. *Journal of Accounting and Management Information Systems*, 19(2): 351-378.

Jouini M.A. (2015). Multidimensional Approach towards a Quantitative Assessment of Security Threats. *Procedia Computer Science*, 52: 507-514.

Lee Y.J. (2011). Profit-Maximizing Firm Investments in Customer Information Security. *Decision Support Systems*, 51(4): 904-920.

Sujiwana R.K., Ridho A.F.A., Aryanti D.C., Rakhmawati N.A. (2024). Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer. *Jurnal Esensi Sistem Informasi dan Sistem Komputer*, 8(1): 101-105.

Van Deursen N., Buchanan W.J., Duff A. (2013). Monitoring Information Security Risks within Health Care. *Computers & Security*, 37: 31-45.

Yaz Ö., Süzen A.A. (2023). Kurumsal Ağlara Yapılan Saldırılarda Açıklanabilir Yapay Zekânın Yeri. *International Conference on Applied Engineering and Natural Sciences*, 1(1): 528-534.

Об авторах

Татьяна Алексеевна Рудакова
Кандидат экономических наук, доцент кафедры экономики, Алтайский государственный технический университет им. И.И. Ползунова (Барнаул, Россия); доцент кафедры экономической безопасности, учета, анализа и аудита, Алтайский государственный университет (Барнаул, Россия). ORCID: 0000-0002-8735-7058.
Область научных интересов: цифровые финансы, экономическая безопасность, управление рисками, учетно-аналитические аспекты банкротства, достоверность учетно-отчетной информации, риски реального сектора экономики.
aleks_rudakova@mail.ru

Оксана Юрьевна Рудакова
Кандидат экономических наук, доцент, заведующий кафедрой менеджмента, организации бизнеса и инноваций, Алтайский государственный университет (Барнаул, Россия). ORCID: 0000-0001-9714-2483.
Область научных интересов: антикризисное управление, управление изменениями и развитием, экономическая безопасность, управленческий консалтинг, инновации.
rud-oksana@yandex.ru

About the Authors

Tatyana A. Rudakova
Cand. Sci. (Econ.), Associate Professor, Department of Economics, Altai State Technical University named after I.I. Polzunov (Barnaul, Russia); Associate Professor, Department of Economic Security, Accounting, Analysis and Audit, Altai State University (Barnaul, Russia). ORCID: 0000-0002-8735-7058.
Research interests: digital finance, economic security, risk management, accounting and analytical aspects of bankruptcy, reliability of accounting and reporting information, risks of the real sector of the economy.
aleks_rudakova@mail.ru

Oksana Yu. Rudakova
Cand. Sci. (Econ.), Associate Professor, Head of the Department of Management, Business Organization and Innovation, Altai State University (Barnaul, Russia). ORCID: 0000-0001-9714-2483.
Research interests: anti-crisis management, change and development management, economic security, management consulting, innovation.
rud-oksana@yandex.ru

作者简介

Tatyana A. Rudakova
经济学博士，副教授，伊·伊·波尔祖诺夫阿尔泰国立技术大学经济学系（巴尔瑙尔，俄罗斯）；副教授，阿尔泰国立大学经济安全、会计、分析与审计系（巴尔瑙尔，俄罗斯）。ORCID: 0000-0002-8735-7058。
研究方向：数字金融、经济安全、风险管理、破产的会计与分析问题、会计报告信息的真实性、实体经济部门风险。
aleks_rudakova@mail.ru

Oksana Yu. Rudakova
经济学博士，副教授，阿尔泰国立大学管理、商业组织与创新系主任（巴尔瑙尔，俄罗斯）。ORCID: 0000-0001-9714-2483。
研究方向：危机管理、变革与发展管理、经济安全、管理咨询、创新。
rud-oksana@yandex.ru

Статья поступила в редакцию 10.02.2026; после рецензирования 26.02.2026 принята к публикации 28.02.2026. Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 10.02.2026; revised on 26.02.2026 and accepted for publication on 28.02.2026. The authors read and approved the final version of the manuscript.
文章于 10.02.2026 提交给编辑。文章于 26.02.2026 已审稿。之后于 28.02.2026 接受发表。作者已经阅读并批准了手稿的最终版本。