

## **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА В УСЛОВИЯХ НЕОПРЕДЕЛЁННОСТИ: ФОРМИРОВАНИЕ МЕХАНИЗМА ЗАЩИТЫ**

**Лариса Васильевна Кулешова**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Донецкая академия управления и государственной службы», Российская Федерация, Донецкая Народная Республика, 283015, г.о. Донецк, г. Донецк, ул. Челюскинцев, 163-а, ORCID 0009-0004-9389-4548, e-mail: lara-kuleshova@mail.ru

***Аннотация.*** В современных условиях ведения бизнеса, характеризующимися глобальными кризисами, санкциями, технологическими изменениями и усилением киберугроз, информационная безопасность становится ключевым фактором устойчивости бизнеса. Утечка данных, кибератаки и нарушение работы информационных систем могут привести к значительным финансовым и репутационным потерям. В связи с этим возникает необходимость разработки эффективного механизма защиты, способного адаптироваться к быстро меняющимся условиям и обеспечивать безопасность бизнеса на всех уровнях. В связи с этим в статье рассматриваются актуальные вопросы обеспечения информационной безопасности бизнеса в условиях неопределённости, вызванной глобальными экономическими, политическими и технологическими изменениями. Предложен механизм защиты, основанный на интеграции современных технологий, управленческих решений и нормативно-правовых аспектов, способствующих ведению бизнеса в защищённых информационных условиях. Особое внимание уделено элементам адаптации бизнеса к динамичным угрозам и формированию устойчивой системы защиты данных. Результаты исследования могут быть использованы для повышения уровня информационной безопасности в организациях различных отраслей.

***Ключевые слова:*** информация, безопасность, неопределённость, защита, стратегии защиты, информационная безопасность, механизм защиты информационных активов бизнеса.

***Информация о финансировании:*** исследование выполнено в рамках фундаментальной научно-исследовательской работы «Условия и инструментарий развития внешнеэкономической деятельности основных сфер и отраслей народного хозяйства: организационно-институциональный и социально-экономический аспекты» (регистрационный номер НИОКТР 124012500447-8) за счёт субсидии на финансовое обеспечение выполнения государственного задания на оказание государственных услуг (выполнение работ) на 2025 год.

***Для цитирования:*** Кулешова Л.В. Информационная безопасность бизнеса в условиях неопределённости: формирование механизма защиты. Государственное управление и право. 2025. № 3(07). С. 190-202.

## **BUSINESS INFORMATION SECURITY IN CONDITIONS OF UNCERTAINTY: FORMING A PROTECTION MECHANISM**

**Larisa Vasilievna Kuleshova**

Federal state budgetary educational institution of higher education «Donetsk Academy of Management and Public Administration», Russian Federation, Donetsk People's Republic, 283015, Donetsk, 163-a Chelyuskintsev str., ORCID 0009-0004-9389-4548, e-mail: lara-kuleshova@mail.ru

*Annotation.* In today's business environment, marked by global crises, sanctions, technological shifts and growing cyber threats, information security has become a critical factor for business resilience. Data leaks, cyberattacks and disruptions of information systems can lead to significant financial and reputational damage. This creates a need to develop an effective protection mechanism capable of adapting to rapidly changing conditions and ensuring business security at all levels. The article examines current issues of ensuring business information security in conditions of uncertainty caused by global economic, political and technological changes. A protection mechanism is proposed based on integration of modern technologies, management solutions and regulatory aspects that facilitate business operations in secure information environments. Special attention is paid to elements of business adaptation to dynamic threats and building a robust data protection system. The research results can be used to improve information security levels in organizations across various industries.

*Keywords:* information, security, uncertainty, protection, protection strategies, information security, business information assets protection mechanism.

*Financing information:* the study was carried out within the framework of the fundamental research work «Conditions and instruments for the development of foreign economic activity of the main spheres and sectors of the national economy: organizational, institutional and socio-economic aspects» (registration number of R&D 124012500447-8) at the expense of a subsidy for financial support for the implementation of the state assignment for the provision of public services (performance of work) for 2025.

*For citation:* Kuleshova, L.V. (2025). Business information security in conditions of uncertainty: forming a protection mechanism. Public administration and law, 3(07), 190-202.

### **ВВЕДЕНИЕ**

Неопределённость в бизнесе связана с невозможностью точного видения будущих событий или их последствий из-за недостатка информации, изменчивости внешней среды или сложности взаимодействия факторов. Она может быть вызвана как внешними, так и внутренними факторами и классифицируется на следующие виды: экономическая неопределённость, которая связана с изменениями в экономической среде, такими как колебания курсов валют, инфляция, санкции, изменения налоговой политики; политическая неопределённость, возникающая из-за из-

менений в политической ситуации, таких как смена власти, введение санкций, изменения в законодательстве; технологическая неопределённость, характеризующая быстрые изменениями в технологиях, которые могут сделать существующие продукты или процессы устаревшими; социальная неопределённость, которая возникает из-за изменений в поведении потребителей, общественных трендов или культурных норм; экологическая неопределённость, связанная с природными катаклизмами, изменениями климата или экологическими требованиями.

Исследование направлено на

выявление проблем информационной безопасности в условиях неопределённости, которые влияют на результаты ведения бизнеса, выделение объектов и субъектов механизма информационной защиты бизнеса, определение стратегий информационной защиты, позволяющие минимизировать риски бизнес-деятельности в будущем.

В современных экономических исследованиях при определении сущности понятия «неопределённость», в первую очередь, указывается на то, что информация не соответствует её качественным характеристикам, таким как: полнота, понятность, достоверность и адаптивность, которые рассматриваются как атрибуты, способные сделать информацию пригодной для проведения конкретного анализа деятельности, формирования выводов и подведения итогов, принятия решений субъектами бизнеса [1]. Таким образом, неопределённость ограничивает видение результатов и влияет на информационную безопасность ведения бизнеса в настоящем и будущем.

#### *Цель и задачи исследования*

Цель данного исследования заключается в разработке и обосновании механизма обеспечения информационной безопасности бизнеса в условиях неопределённости, направленного на минимизацию рисков, связанных с киберугрозами, экономической, политической и технологической нестабильностью.

Задачи исследования:

- выявить наиболее распространённые угрозы для бизнеса в условиях неопределённости, связанные с информационным обеспечением деятельности;
- рассмотреть ключевые этапы формирования механизма защиты информации;
- дать сущностную характеристику структурных элементов механизма поддержки информацион-

ной безопасности бизнес-структур;

- обосновать необходимость использования механизма защиты информационных активов бизнес-структур в условиях неопределённости.

#### *Методы исследования*

Специально-научные методы исследования:

- метод анализа иерархий. Позволяет провести оценку даже при недостаточном количестве данных, не требуя информации о статистике и вероятностях;

- экспериментальный подход. Позволяет определить эффективность системы защиты путём преодоления защитных элементов системы разработчиками, которые выступают в роли злоумышленников.

Также применялись классические общенаучные методы обобщения, анализа, синтеза и прогнозирования.

#### *Результаты исследования и их обсуждение*

В условиях глобальной неопределённости, вызванной экономическими кризисами, геополитическими конфликтами и пандемиями, информационная безопасность (ИБ) бизнеса сталкивается с новыми вызовами. Рост киберугроз, усложнение методов атак и увеличение числа уязвимостей требуют глубокого теоретического анализа и разработки эффективных механизмов защиты. Основными угрозами информационной безопасности в условиях неопределённости являются: кибератаки, риски удалённой работы, регуляторные требования и человеческий фактор с точки зрения теоретических основ информационной безопасности [2; 3].

Одной из наиболее распространённых угроз в условиях неопределённости являются кибератаки, включая фишинг, ransomware и DDoS-атаки. Рассмотрим их подробнее (таблица 1).

**Таблица 1.** Кибератаки и их угрозы для бизнеса  
**Table 1.** Cyber-attacks and their threats to business

| Тип атаки                 | Описание   | Основные угрозы для бизнеса  | Примеры пострадавших компаний  |
|---------------------------|--|--|--|
| Фишинг                    | Использование поддельных писем, сообщений или сайтов для получения данных              | Утечка конфиденциальной информации (логины, пароли, данные клиентов). Потеря доверия клиентов. Финансовые потери | Google и Facebook (2013-2015): атака через фишинговые письма, приведшая к утечке данных на сумму более \$100 млн                           |
| Ransomware                | Вредоносное ПО, блокирующее доступ к данным или системам до выплаты выкупа             | Потеря доступа к важной информации и данным. Финансовые потери из-за выплаты выкупа. Простой бизнеса             | Colonial Pipeline (2021): атака ransomware привела к остановке работы трубопровода и выплате выкупа в \$4,4 млн                            |
| DDoS-атаки                | Перегрузка серверов или сетей, приводящая к их недоступности                           | Потеря доступа к онлайн-ресурсам. Снижение доходов из-за простоя. Репутационный ущерб                            | GitHub (2018): крупнейшая DDoS-атака с трафиком 1,35 Тбит/с, вызвавшая простой сервиса   |
| Атаки на цепочки поставок | Внедрение вредоносного ПО через уязвимости в программном обеспечении поставщиков       | Утечка данных. Нарушение работы бизнеса. Потеря доверия партнеров и клиентов                                     | SolarWinds (2020): вредоносное ПО Orion использовалось для атак на клиентов, включая правительственные агентства США                       |
| Социальная инженерия      | Манипулирование сотрудниками для получения доступа к данным или системам               | Утечка конфиденциальной информации. Финансовые потери. Репутационный ущерб                                       | Ubiquiti Networks (2015): мошенники получили доступ к финансовым данным через фишинговые письма, потери – \$46,7 млн                       |
| Атаки на IoT-устройства   | Использование уязвимостей в устройствах Интернета вещей для доступа к сети             | Утечка данных. Нарушение работы бизнеса. Риск атак на критическую инфраструктуру                                 | Mirai Botnet (2016): атака на IoT-устройства привела к масштабным DDoS-атакам на Dyn, вызвавшим простой Twitter, Netflix и других сервисов |
| Целевые атаки (APT)       | Долгосрочные и сложные атаки, направленные на конкретную организацию                   | Утечка конфиденциальной информации. Потеря интеллектуальной собственности. Репутационный и финансовый ущерб      | Sony Pictures (2014): атака группы Guardians of Peace привела к утечке фильмов, данных сотрудников и финансовым потерям                    |
| Вредоносное ПО (Malware)  | Программы, предназначенные для повреждения или несанкционированного доступа к системам | Потеря данных. Нарушение работы систем. Финансовые потери из-за восстановления                                   | Maersk (2017): атака вредоносным ПО NotPetya привела к потерям на \$300 млн из-за остановки работы систем                                  |
| Атаки на облачные сервисы | Взлом облачных хранилищ или приложений   | Утечка данных. Нарушение работы бизнеса. Потеря доверия клиентов   | Capital One (2019): утечка данных более 100 млн клиентов через уязвимость в облачной инфраструктуре AWS                                    |
| Атаки на криптовалюты     | Использование вычислительных ресурсов для майнинга криптовалют                         | Снижение производительности систем. Увеличение затрат на электроэнергию. Риск повреждения оборудования           | Tesla (2018): вредоносное ПО для майнинга криптовалют было обнаружено в облачной инфраструктуре компании                                   |

Как видно из таблицы 1, кибератаки представляют серьёзную угрозу для бизнеса, независимо от его масштаба и отрасли. Основные типы атак, такие как фишинг, ransomware, DDoS и атаки на цепочки поставок, приводят к значительным финансовым потерям, утечкам данных, простоям бизнеса и репутационному ущербу.

Среди пострадавших от кибератак есть и крупные компании Российской Федерации, среди которых:

«Евросеть» (2017 г.): тип атаки – Ransomware. Кибератака привела к временной остановке работы систем компании. Злоумышленники заблокировали доступ к данным и потребовали выкуп за их разблокировку. Это привело к простоям бизнеса и репутационному ущербу [4];

«Газпром» и другие нефтегазовые компании (2017 г.): тип атаки – вредоносное ПО (NotPetya). Компания стала одной из жертв глобальной атаки вредоносным ПО NotPetya, которое затронуло её IT-инфраструктуру. Это привело к следующим последствиям: временный сбой в работе систем, финансовые потери [5];

Сбербанк (2020 г.): тип атаки – DDoS-атака. Крупнейший российский банк подвергся масштабной DDoS-атаке, которая привела к временной недоступности онлайн-сервисов. Последствия: снижение доступности сервисов для клиентов, репутационные риски [6];

«Магнит» (2021 г.): тип атаки – утечка данных через смс-рассылки. Злоумышленники получили доступ к данным клиентов сети магазинов через уязвимости в облачной инфраструктуре. Последствия: утечка персональных данных клиентов, репутационный ущерб [7];

«Газпром нефть» (2021 г.): тип атаки: атака на IoT-устройства. Злоумышленники использовали уязвимости в IoT-устройствах для доступа к корпоративной сети. Послед-

ствия: нарушение работы систем, риск утечки данных [8];

«Яндекс» (2022 г.): тип атаки – целевая атака (APT). Хакеры использовали уязвимости в системе для кражи исходного кода поискового алгоритма. Последствия: потеря интеллектуальной собственности, репутационные риски [9].

Также немаловажным в обеспечении информационной безопасности является избежание риска удалённой работы. Технологии, используемые при организации удалённого доступа, рассмотрены Матвеевым Н.В. [10]. Удалённая работа значительно увеличивает риск утечек данных, так как сотрудники часто используют личные устройства и ненадёжные сети для доступа к корпоративным ресурсам. Серьёзными последствиями для бизнеса становятся финансовый ущерб, потеря имиджа, открытие коммерческой тайны. Компьютеры сотрудников бизнес-структур должны быть защищены от кибератак и программного обеспечения, несущего угрозы.

Ещё одной проблемой для бизнеса становится несоблюдение правовых актов международного и федерального уровня, включающих в себя стандарты и правила, направленные на защиту информации и данных. На международном уровне примером такого регулятивного акта является Общий/Генеральный регламент по защите персональных данных (GDPR), а на федеральном – Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). Рассмотрим данные регламенты подробнее.

GDPR (General Data Protection Regulation) – это европейский регламент, который регулирует обработку персональных данных граждан Европейского союза. В нём описаны требования по защите данных и информации, в том числе

указана необходимость получения согласия на обработку, уведомление о утечках данных и назначение ответственного за защиту данных на предприятии или в организации. Несоблюдение данного регламента приводит к штрафам в размере до 4 % от годового оборота компании или 20 миллионов евро (в зависимости от того, какая сумма больше). Для бизнеса это влечёт дополнительные проблемы и риски, в первую очередь для тех компаний, которые осуществляют внешнеэкономическую деятельность или являются субъектами международных рынков [11].

В Российской Федерации действует Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, который направлен на регулирование процесса обработки персональных данных граждан РФ. Современное законодательство в сфере информационной безопасности устанавливает требования к коммерческим организациям по обеспечению сохранности персональных данных. Компании обязаны гарантировать их секретность, неизменность и возможность доступа, а также внедрять защитные технологии и проводить плановые проверки. Несоблюдение этих норм влечёт за собой не только финансовые санкции и приостановку работы, но и подрыв репутации среди клиентов.

Ключевой проблемой в сфере информационной безопасности остаются действия персонала. Несознанные ошибки работников – например, переход по ссылкам в поддельных письмах, установка ненадёжных паролей или неконтролируемая передача данных – способны спровоцировать утечки, финансовые убытки и негативный имидж компании.

Основная причина таких ситуаций – низкая грамотность сотрудников в вопросах защиты инфор-

мации и отсутствие в организации практик, направленных на формирование ответственного отношения к данным. Для снижения рисков эксперты рекомендуют внедрять обучающие программы, организовывать тематические семинары и периодически проверять уровень знаний персонала [13; 14].

Кроме того, теория социальной инженерии показывает, что злоумышленники часто эксплуатируют психологические уязвимости сотрудников, такие как доверчивость или невнимательность. Это делает необходимым не только техническую защиту, но и формирование у сотрудников критического мышления и осознанного отношения к безопасности [15].

Соблюдение регуляторных требований требует комплексного подхода, включающего технические и организационные меры, в то время как минимизация рисков, связанных с ошибками сотрудников, требует постоянного обучения и формирования культуры безопасности. Эти аспекты должны быть интегрированы в общую стратегию информационной безопасности для обеспечения устойчивости бизнеса в условиях современных киберугроз.

Для минимизации указанных угроз информационной безопасности бизнес-структур необходимо использовать определённые методы и механизмы защиты.

Методы, благодаря которым вводятся в действие механизмы защиты информации в информационных системах в полной мере, рассмотрены Треглазовым Г.В., который выделил семь методов защиты информации в информационных системах, которые являются наиболее современными и актуальными в XXI веке [16].

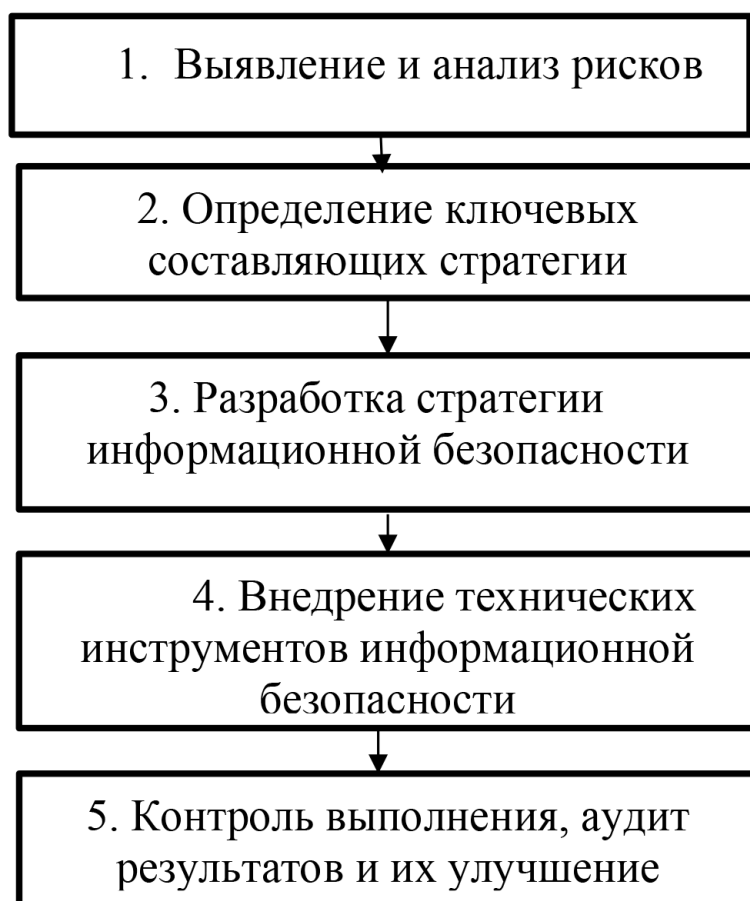
Механизмы безопасности в компьютерных системах рассмотрены Лавреш И.И. В исследовании выделены такие механизмы, как: аутен-

тификация, авторизация, шифрование, контроль доступа, межсетевые экраны и т. п., которые обеспечивают защиту информации и ресурсов от несанкционированного доступа, модификации или уничтожения [17].

Обсуждая тему механизма защиты информации в условиях неопределённости, необходимо дать ему определение. Защитный механизм включает набор действий, призванных предупредить, выявлять и нейтрализовать киберугрозы, а также сокращать ущерб от них. Создание такой системы начинается с аудита текущего состоя-

ния безопасности и последующего внедрения организационных и технических решений разного уровня. Эти меры направлены на повышение уровня защищённости данных компании. Разработанная стратегия основывается на выводах, полученных в ходе аудиторской проверки.

В работе анализируются основные стадии разработки защитной системы, влияние технологических инструментов и методы контроля угроз. Графическое отображение этапов формирования механизма безопасности приведено на рисунке 1.



**Рисунок 1.** Формирование механизма защиты: последовательность этапов  
**Figure 1.** Formation of a protection mechanism: sequence of stages

Как видно на рисунке 1, основных этапов защиты пять. Рассмотрим их подробнее.

Первоначально необходимо выявить возможные информационные риски и угрозы для деятельности. Этот этап позволяет перейти к

следующему, связанному с определением ключевых составляющих стратегии защиты информации, а затем и к её непосредственному формированию. В стратегии обязательно прописываются технологические инструменты защиты ин-

формации, а также ответственные за их разработку и внедрение, что даёт выполнение следующего этапа – контроль полученных результатов по защите информации и определение дальнейших действий компании по недопущению угроз и рисков.

Человеческий фактор нельзя исключать, так как он может привести к потере информации, поэтому обучение сотрудников через тренинги, мастер-классы, направленные на формирование информационной грамотности персонала, являются залогом успешного функционирования бизнеса и важным этапом формирования механизма защиты. Обучение включает в себя:

- проведение тренингов по основам информационной безопасности;

- формирование культуры безопасности в организации;

- тестирование на знание правил обеспечения информационной безопасности ведения бизнеса (например, через фишинговые симуляции).

Регулярный аудит и анализ инцидентов позволяют выявлять слабые места в системе защиты и вносить улучшения. Методы аудита следующие:

- проведение пентестов (тестирование на проникновение);

- анализ инцидентов и разработка мер по их предотвращению;

- обновление политик и процедур информационного обеспечения.

Нельзя не отметить важнейшую роль в поддержании информационной безопасности, которая отводится технологиям защиты. Среди них [19]:

1. Технологии прогнозирования киберугроз. Современные системы безопасности активно внедряют алгоритмы искусственного интеллекта и самообучающиеся модели. Эти инструменты позволяют: спро-

гнозировать потенциальные угрозы на основе поступающих данных; обрабатывать массивы информации в реальном времени для выявления скрытых угроз; автоматизировать процесс реагирования на инциденты.

К примерам реализации относятся ML-платформы, способные: анализировать метаданные сетевых соединений для обнаружения отклонений от нормальных паттернов; идентифицировать подозрительные действия пользователей (несанкционированный доступ, аномальную активность); блокировать кибератаки.

2. Обеспечение безопасности распределённых инфраструктур: распространение облачных сервисов и IoT-экосистем порождает специфические риски: уязвимость в системах хранения облачных данных; целевые атаки на интеллектуальные устройства (сенсоры, промышленные контроллеры, умные гаджеты), функционирующие без постоянного человеческого контроля.

Среди методов противодействия можно выделить: применение многоуровневого шифрования для защиты информации при передаче и хранении; внедрение ролевых моделей доступа с динамической аутентификацией; постоянный аудит активности пользователей в сетях. Для IoT-устройств применяются системы управления и регулярное обновление программного обеспечения.

Для управления рисками в сфере информационной безопасности субъекты бизнеса могут использовать следующие мероприятия:

1. Подготовить планы реагирования на инциденты, которые включают чёткие инструкции для сотрудников в случае кибератаки. Это позволяет минимизировать время реагирования и снизить ущерб.

2. Постоянно использовать программное обеспечение по резервному копированию и восстановлению данных. Это позволяет восстановить данные в случае их потери или повреждения в результате атаки.

Необходимо отметить, что влияние информационных рисков на деятельность бизнес-структур необходимо правильно оценивать. В исследовании Серебряковой Т.А. отмечено, что простейшие методы (анализ чувствительности, анализ сценариев, анализ процесса бизнес-планирования в расплывчатых условиях) являются наименее точными и помогают провести эскизный анализ рискованности проекта, либо используются в качестве расчётов предварительных более

сложным и точным методам (теоретико-вероятностные и выборочные методы). Для оценки устойчивости проекта к изменениям внешней среды и количественного измерения риска, связанного с проектом в целом, автором предложено применение имитационного моделирования по методу Монте-Карло [20].

Особенно уязвимыми в условиях неопределённости становятся компании, которые не уделяют достаточного внимания защите данных, обучению сотрудников и внедрению современных технологий кибербезопасности. Для нивелирования последствий им необходимо внедрять и использовать механизм защиты, характеристика элементов которого представлена в таблице 2.

**Таблица 2.** Сущностная характеристика структурных элементов механизма поддержки информационной безопасности бизнес-структур  
**Table 2.** Essential characteristics of the structural elements of the information security support mechanism for business structures

| Элемент механизма         | Объект защиты                     | Субъект защиты   | Формы защиты   | Методы защиты   |
|---------------------------|-----------------------------------|--|--|---|
| Выявление и анализ рисков | Данные, системы, инфраструктура   | Специалисты по информационной безопасности (ИБ), менеджеры | Идентификация активов. Оценка угроз и уязвимостей                            | Разработка матрицы рисков. Сценарное моделирование                            |
| Разработка стратегии      | Политики и процедуры ИБ           | Руководство компании, отдел информационной безопасности    | Создание политик конфиденциальности. Разработка процедур управления доступом | Внедрение системы управления рисками  |
| Технические решения       | Конечные устройства, сети, данные | Специалисты по ИБ, IT-отдел                                | Внедрение антивирусов. Использование VPN и шифрования                        | Формирование многоуровневой защиты. Автоматизация мониторинга и реагирования  |
| Обучение сотрудников      | Персонал компании                 | Сотрудники компании, отдел ИБ                              | Проведение тренингов. Тестирование на знание ИБ                              | Фишинговые симуляции. Обучение основам ИБ. Формирование культуры безопасности |
| Аудит и улучшение         | Системы ИБ, процессы              | Аудиторы, специалисты по ИБ                                | Проведение пентестов. Анализ инцидентов                                      | Методы анализа причин инцидентов  |

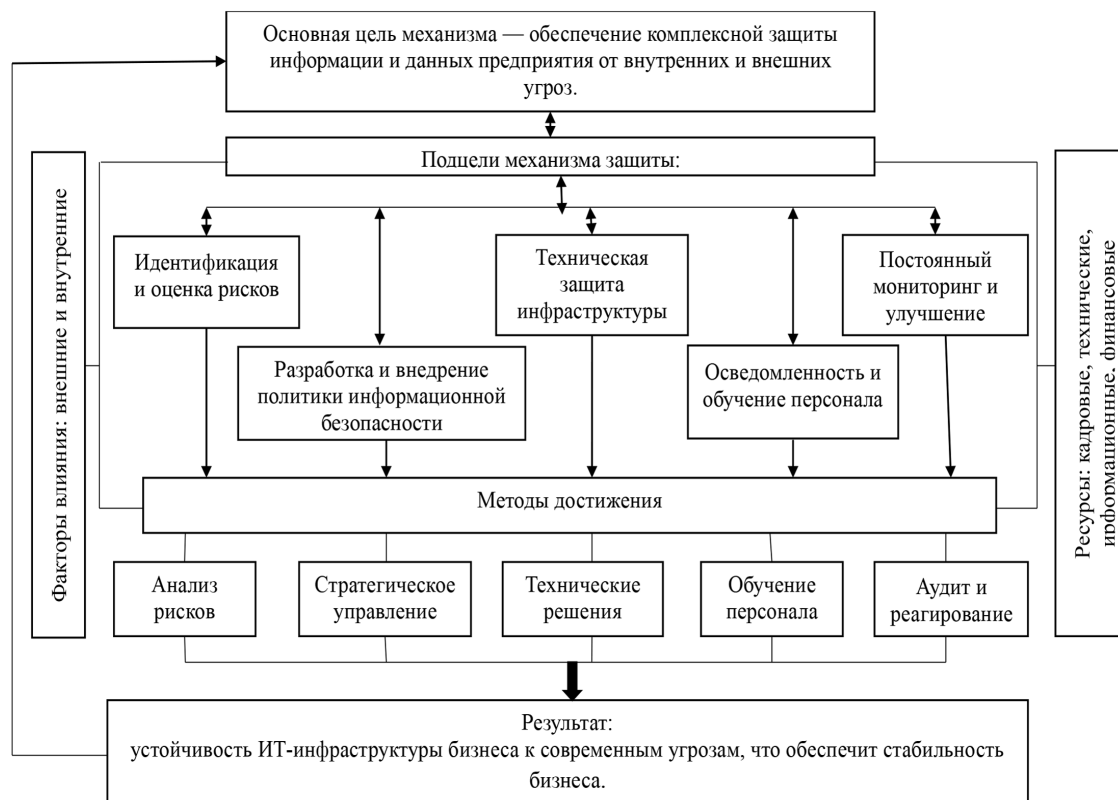
**Продолжение табл. 2**  
**Continuation of table 2**

| Элемент механизма  | Объект защиты                    | Субъект защиты                  | Формы защиты   | Методы защиты                                 |
|--------------------|----------------------------------|---------------------------------|--|---|
| Технологии         | Данные, сети, устройства         | Специалисты по ИБ, разработчики | Использование программ для прогнозирования угроз. Защита облачных сред и IoT | Внедрение систем на основе машинного обучения |
| Управление рисками | Данные, системы, бизнес-процессы | Руководство компании, отдел ИБ  | Разработка планов реагирования на инциденты. Резервное копирование данных    | Внедрение систем специального ПО              |

Как представлено в таблице 1, механизм защиты информационной безопасности включает комплексный подход, охватывающий объекты, субъекты, формы и методы защиты. Объектами защиты являются данные, системы, устройства и бизнес-процессы, а субъектами – специалисты по ИБ, IT-отдел, руководство и сотрудники компании. Формы защиты включают анализ рисков, разра-

ботку стратегий, внедрение технических решений, обучение персонала и регулярный аудит, а методы защиты основаны на международных стандартах, современных технологиях и управлении рисками.

Учитывая рассмотренные структурные элементы механизма защиты, сам механизм можно представить следующим образом (рисунок 2).



**Рисунок 2.** Структурные элементы механизма защиты информации  
**Figure 2.** Structural elements of the information security mechanism

Для эффективного функционирования представленного механизма необходимо интегрировать все элементы: от выявления проблем и угроз, и их идентификации до разработки и использования программного обеспечения, направленного на нивелирование данных угроз, что позволит бизнесу свести к минимуму возможные информационные и экономические риски, и будет способствовать его развитию в дальнейшей перспективе.

### **Выводы**

Функционирование бизнеса в условиях современных вызовов обязывает компании, которые ориентированы на долгосрочную перспективу эффективной деятельности, использовать для своей информационной безопасности различные цифровые технологии, способные защитить бизнес-структуры от различных киберугроз. Они становятся составной частью системы информационной безопасности, формируя эффективный ме-

ханизм защиты.

Для российского бизнеса надёжная защита информации превратилась из обычной практики в стратегический ресурс развития. Она даёт компаниям конкурентные преимущества как на внутреннем, так и на международном рынках, повышая устойчивость бизнеса в условиях неопределённости.

Разработанный комплексный подход к информационной безопасности включает несколько ключевых элементов: тщательную оценку потенциальных угроз; разработку адаптивной стратегии защиты; внедрение современных технических решений; регулярное обучение персонала; постоянный аудит системы безопасности.

Механизм защиты становится важным инструментом для поддержания стабильности бизнеса, укрепления его конкурентоспособности и обеспечения долгосрочного успеха в условиях современных вызовов.

## **СПИСОК ИСТОЧНИКОВ**

1. Романюк А.В. Неопределённость в предпринимательской деятельности. URL: <https://cyberleninka.ru/article/n/neopredelyonnost-v-predprinimatelskoy-deyatelnosti>.
2. Николаева М.О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации // Мониторинг. Образование. Безопасность. 2023. № 1. С. 51-57. EDN РТСЕНС.
3. Наскидашвили К.А. Информационная безопасность. Виды угроз информационной безопасности // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». 2020. № 1(12). С. 187-189. EDN AGGRLS.
4. «Евросеть» избавилась от антивирусного зоопарка. URL: <https://www.itweek.ru/security/article/detail.php?ID=107472&ysclid=ma0w7oo8r7233872722>.
5. Petya/GoldenEye Вирус-вымогатель. URL: [https://www.tadviser.ru/index.php/Статья:Petya/ExPetr/GoldenEye\\_\(вирус-вымогатель\)?ysclid=ma0whhi4yz249385341](https://www.tadviser.ru/index.php/Статья:Petya/ExPetr/GoldenEye_(вирус-вымогатель)?ysclid=ma0whhi4yz249385341).
6. Сбербанк в январе подвергся мощнейшей в своей истории DDOS-атаке, которую отразил – банк. URL: <https://mfd.ru/news/view/?id=2335903>.
7. Мошенники начали выманивать данные россиян с помощью смс от «Магнита». URL: <https://kazanfirst.ru/news/544824>.
8. Цель кибератаки – российская нефтяная компания «Газпром нефть». URL: <https://ru.famagusta.news/news/kosmos/stochos-kyvernoepithesis-i-rosiki-petrelaiki-gazprom-neft?ysclid=ma0x9kexaj422896419>.
9. Группировка APT31 атакует российский топливно-энергетический комплекс и СМИ. URL: <https://www.securitylab.ru/news/533116.php>.

10. Матвеев Н.В. Исследование механизмов защиты информации в системах удалённого доступа // Научный аспект. 2023. Т. 6, № 2. С. 704-713. EDN OGKHRN.
11. Луцкая Е.Е. Американский доллар как главная мировая валюта: перспективы изменения его статуса // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 2: Экономика. Реферативный журнал. 2020. № 2. С. 95-99. EDN LLDNQI.
12. GDPR /General Data Protection Regulation (Общий/Генеральный регламент по защите персональных данных). URL: <https://ogdpr.eu/ru>.
13. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (последняя редакция) // СПС КонсультантПлюс. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/).
14. Крупко О.О., Шабурова А.В. Аудит информационной безопасности и его методы в управлении информационной безопасностью организации // Интерэкспо Гео-Сибирь. 2024. Т. 6. С. 115-120. DOI 10.33764/2618-981X-2024-6-115-120. EDN AQMJJZ.
15. Левина В.И. Информационная безопасность и угрозы информационной безопасности в коммерческих организациях // Вопросы образования и науки: сборник научных трудов по материалам международной научно-практической конференции, Тамбов, 30 ноября 2017 года. Том Часть 2. Тамбов: ООО «Консалтинговая компания Юком», 2017. С. 53-54. EDN YOXCXR.
16. Бондарев В.В. Психологические аспекты информационной безопасности // Безопасные информационные технологии: сборник трудов Девятой всероссийской научно-технической конференции, Москва, 04-05 декабря 2018 года. Москва: Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет), 2018. С. 28-32. EDN SOJXMB.
17. Треглазов Г.В. Реализация перспективных механизмов технической защиты информации в обществе XXI века // Евразийское Научное Объединение. 2021. № 7-1(77). С. 42-44. EDN AOKHLW.
18. Лавреш И.И., Пунегов А.И. Разработка механизмов защиты информации // Февральские чтения: Тридцать первая годовичная сессия учёного совета Сыктывкарского Государственного университета имени Питирима Сорокина, Сыктывкар, 01-29 февраля 2024 года. Сыктывкар: Сыктывкарский государственный университет им. Питирима Сорокина, 2024. С. 408-413. EDN FIUAUD.
19. Константинов М.А. Война за информацию: стратегии защиты от промышленного шпионажа // Журнал монетарной экономики и менеджмента. 2024. № 11. С. 288-292. DOI 10.26118/2782-4586.2024.78.85.154. EDN HDEWVM.
20. Овчинникова Е.А., Герасимов В.А., Воропаев А.Д. Основы управления рисками информационной безопасности. Планирование управления рисками: учебное пособие. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2024. 81 с. EDN WLGXPE.
21. Серебрякова Т.А. Инструмент для оценки рисков, связанных с внедрением информационного обеспечения в практику управления предприятием // Учёные заметки ТОГУ. 2014. Т. 5, № 4. С. 1016-1019. EDN TCFABH.

### *Информация об авторе*

Кулешова Лариса Васильевна – кандидат экономических наук, доцент, доцент кафедры менеджмента внешнеэкономической деятельности

## **REFERENCES**

1. Romaniuk, A.V. Uncertainty in entrepreneurial activity. Retrieved from <https://cyberleninka.ru/article/n/neopredelyonnost-v-predprinimatelskoy-deyatelnosti>. (In Russ.)
2. Nikolaeva, M.O. (2023). Information security: Modern picture of the problem of information security and information protection. Monitoring. Education. Security, 1, 51-57. (In Russ.)
3. Naskidashvili, K.A. (2020). Information security. Types of information security threats. Bulletin of Student Scientific Society of Donetsk National University, 1(12), 187-189. (In Russ.)

4. Euroset got rid of antivirus zoo. Retrieved from <https://www.itweek.ru/security/article/detail.php?ID=107472>. (In Russ.)
5. Petya/GoldenEye ransomware. Retrieved from <https://www.tadviser.ru/index.php/>. (In Russ.)
6. Sberbank faced the most powerful DDoS attack in its history in January, which it repelled – bank. Retrieved from <https://mfd.ru/news/view/?id=2335903>. (In Russ.)
7. Fraudsters began to extract Russians' data using SMS from "Magnit". Retrieved from <https://kazanfirst.ru/news/544824>. (In Russ.)
8. The target of the cyber-attack is Russian oil company Gazprom Neft. Retrieved from <https://ru.famagusta.news/news/kosmos/stochos-kyvernoepithesis-i-rosiki-petrelaiki-gazprom-neft>. (In Russ.)
9. APT31 group attacks Russian fuel and energy complex and media. Retrieved from <https://www.securitylab.ru/news/533116.php>. (In Russ.)
10. Matveev, N.V. (2023). Research of information protection mechanisms in remote access systems. *Scientific Aspect*, 6(2), 704-713. (In Russ.)
11. Lutskaya, E.E. (2020). US dollar as the main world currency: Prospects for changing its status. *Social and Humanitarian Sciences. Domestic and Foreign Literature. Series 2: Economics. Abstract Journal*, 2, 95-99. (In Russ.)
12. GDPR/General Data Protection Regulation. Retrieved from <https://ogdpr.eu/ru>. (In Russ.)
13. Federal Law of the Russian Federation of July 27, 2006 No. 152-FZ "On Personal Data" (latest edition). Retrieved from [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/). (In Russ.)
14. Krupko, O.O., & Shaburova, A.V. (2024). Information security audit and its methods in managing the organization's information security. *Interexpo Geo-Siberia*, 6, 115-120. (In Russ.)
15. Levina, V.I. (2017). Information security and information security threats in commercial organizations. *Questions of Education and Science: Collection of Scientific Papers of the International Scientific-Practical Conference, Tambov, November 30, 2017. Part 2*, 53-54. (In Russ.)
16. Bondarev, V.V. (2018). Psychological aspects of information security. *Safe Information Technologies: Proceedings of the Ninth All-Russian Scientific and Technical Conference, Moscow, December 4-5, 2018*, 28-32. (In Russ.)
17. Treglazov, G.V. (2021). Implementation of advanced technical information protection mechanisms in the society of the XXI century. *Eurasian Scientific Association*, 7-1(77), 42-44. (In Russ.)
18. Lavresh, I.I., & Punegov, A.I. (2024). Development of information protection mechanisms. *February Readings: The Thirty-First Annual Session of the Academic Council of Pitirim Sorokin Syktyvkar State University, Syktyvkar, February 1-29, 2024*, 408-413. (In Russ.)
19. Konstantinov, M.A. (2024). Information war: Strategies for protection against industrial espionage. *Journal of Monetary Economics and Management*, 11, 288-292. (In Russ.)
20. Ovchinnikova, E.A., Gerasimov, V.A., & Voropaev, A.D. (2024). Fundamentals of information security risk management. *Risk management planning: Textbook. Siberian State University of Telecommunications and Informatics*. (In Russ.)
21. Serebryakova, T.A. (2014). A tool for assessing risks associated with the implementation of information support in enterprise management practice. *Scientific Notes of PNU*, 5(4), 1016-1019. (In Russ.)

#### *Information about the author*

Larisa V. Kuleshova – Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Foreign Economic Activity Management

*Автор заявляет об отсутствии конфликта интересов.*

*The author declares no conflicts of interests.*

Поступила в редакцию (Reserved) 19.03.2025

Поступила после рецензирования 17.09.2025

Принята к публикации (Accepted) 25.09.2025