

МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

С. С. Солдатова

Пензенский государственный университет, Пенза, Россия
sssoldatova@mail.ru

Аннотация. *Актуальность и цели.* Нарастание внешнеполитической напряженности в мире и, как следствие, рост финансово-экономических угроз и санкций для российских товаропроизводителей диктуют повышенные требования к уровню обеспечения их экономической безопасности. Цифровизация экономического пространства привела к повышению востребованности на рынке информации как специфического товара. В данных условиях актуальность совершенствования методов и механизмов защиты конфиденциальной информации совершенно очевидна. Цель и задачи данного процесса сводятся к повышению уровня защищенности информационных ресурсов объекта от несанкционированного доступа и воздействия. *Материалы и методы.* В ходе выполненного научного исследования применялись общенаучные и экономико-статистические методы сбора и анализа информации по проблематике исследования, что позволило решить поставленные задачи. *Результаты.* Исследованы виды и типы конфиденциальной информации, которые наиболее часто подвержены хищению. Выявлены основные причины нарушений в сфере информационной безопасности, что позволило выработать рекомендации по совершенствованию работы службы экономической безопасности субъекта в сфере защиты конфиденциальной информации. Определены основные направления защиты информационных ресурсов хозяйствующего субъекта в целях повышения его экономической безопасности. *Выводы.* Предложены рекомендации по совершенствованию методов и механизмов защиты информационных ресурсов российских компаний от несанкционированного доступа и хищений на основе внедрения комплексного подхода к защите конфиденциальной информации от всех видов угроз.

Ключевые слова: конфиденциальная информация, информационные ресурсы, угрозы, информационная безопасность, экономическая безопасность

Для цитирования: Солдатова С. С. Методы защиты конфиденциальной информации в целях обеспечения экономической безопасности хозяйствующего субъекта // Модели, системы, сети в экономике, технике, природе и обществе. 2025. № 2. С. 36–46. doi: 10.21685/2227-8486-2025-2-3

METHODS OF PROTECTING CONFIDENTIAL INFORMATION IN ORDER TO ENSURE THE ECONOMIC SECURITY OF AN ECONOMIC ENTITY

S.S. Soldatova

Penza State University, Penza, Russia
sssoldatova@mail.ru

Abstract. *Background.* The increase in foreign policy tensions in the world and, as a result, the growth of financial and economic threats and sanctions for Russian producers dictate increased requirements for the level of ensuring their economic security. The digitalization of the economic space has led to an increase in demand for information as a specific product on the market. In these circumstances, the relevance of improving methods and mechanisms for protecting confidential information is quite obvious. The purpose and objectives of this process are to increase the level of protection of the object's information resources from unauthorized access and exposure. *Materials and methods.* In the course of the performed scientific research, general scientific and economic-statistical methods of collecting and analyzing information on the problems of research were used, which made it possible to solve the tasks set. *Results.* The types and types of confidential information that are most often susceptible to theft are investigated. The main causes of violations in the field of information security have been identified, which made it possible to develop recommendations for improving the work of the economic security service of the subject in the field of confidential information protection. The main directions of protection of information resources of an economic entity in order to increase its economic security are determined. *Conclusions.* Recommendations are proposed to improve methods and mechanisms for protecting information resources of Russian companies from unauthorized access and theft, based on the introduction of an integrated approach to protecting confidential information from all types of threats.

Keywords: confidential information, information resources, threats, information security, economic security efficiency

For citation: Soldatova S.S. Methods of protecting confidential information in order to ensure the economic security of an economic entity. *Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve* = *Models, systems, networks in economics, technology, nature and society*. 2025;(2):36–46. (In Russ.). doi: 10.21685/2227-8486-2025-2-3

Введение

Для каждого хозяйствующего субъекта вопрос обеспечения собственной экономической безопасности в современных условиях, характеризующихся высокой степенью неопределенности внешней среды, нарастанием экономических угроз вследствие ужесточения экономических санкций и ограничений со стороны коллективного Запада относительно России, является жизненно важным. Ускорение темпов развития информационных технологий и цифровизация экономического пространства вывели на первый план именно информационную составляющую экономической безопасности хозяйствующего субъекта. Актуальность защиты безопасности информационных ресурсов на сегодняшний день является неоспоримой управленческой задачей, так как от

степени защищенности конфиденциальной бизнес-информации от несанкционированного доступа и утечки во многом зависят финансово-экономические результаты работы компании.

Информационная безопасность является одним из ключевых элементов системы обеспечения экономической безопасности объекта. К числу информационных ресурсов хозяйствующего субъекта принято относить: непосредственно информационные данные; аппаратные средства накопления и хранения информации; программное обеспечение, в том числе прикладные компьютерные программы; документы в бумажном виде [1].

Всем субъектам, осуществляющим производственно-коммерческую деятельность на территории Российской Федерации, согласно требованиям Федерального закона № 149-ФЗ «Об информации, информационных технологиях и защите информации» [2], необходимо реализовать комплекс управленческих мер по трем основным направлениям:

- 1) защита информационных ресурсов от несанкционированного доступа, копирования, распространения, уничтожения информации и иных неправомерных действий с ней;

- 2) своевременное выявление и пресечение правонарушений в сфере информационной безопасности объекта;

- 3) мониторинг и контроль функционирования системы информационной безопасности объекта [3].

Понятие конфиденциальной информации используется не только в бизнес-сообществе, но и на государственном уровне. В условиях нарастания напряженности в геополитической и макроэкономической сферах защита подобного рода информации практически для любого субъекта экономической деятельности является первостепенной задачей.

Конфиденциальная информация – это информационные ресурсы и сведения, имеющие особую ценность для их владельца (личности, организации, органов власти, государства). От эффективности процесса защиты и сохранения целостности данной информации напрямую зависят экономический результат, конкурентоспособность и экономическая безопасность объекта (собственника информации) [4].

По своей сути конфиденциальная информация – это персональные сведения о сотрудниках компании, ее клиентах, партнерах, поставщиках и прочих контрагентах. К данному виду информации относятся технологии, сведения о финансовом, материально-техническом состоянии, бизнес-план и стратегия развития, в том числе стратегия создания и развития конкурентных преимуществ.

Материалы и методы

В процессе исследования теоретической базы, а также изучения практического опыта ряда промышленных предприятий Пензенской области были выявлены, систематизированы данные, характеризующие основные проблемы в сфере информационной безопасности.

В течение ряда последних лет количество противоправных действий, нацеленных на несанкционированный доступ к конфиденциальной информации, имеет устойчивую динамику к росту. По официальным данным, ежегодно объем утечки конфиденциальной информации увеличивается приблизительно на 30 % [5]. При этом если до 2022 г. хакеров в основном интересовал малый и средний бизнес, то в настоящее время объектом внимания злоумышленников

является крупный российский бизнес, в особенности компании и организации, функционирующие в сфере военно-промышленного комплекса (ВПК). Конечно, в современных условиях данный факт никого не удивляет. На долю предприятий ВПК приходится 20 % от всех преступлений в сфере информационной безопасности [6].

На рис. 1 представлен результат анализа официальных данных о несанкционированном доступе и утечке конфиденциальной информации промышленных российских предприятий, которые были выявлены в течение прошедшего года.

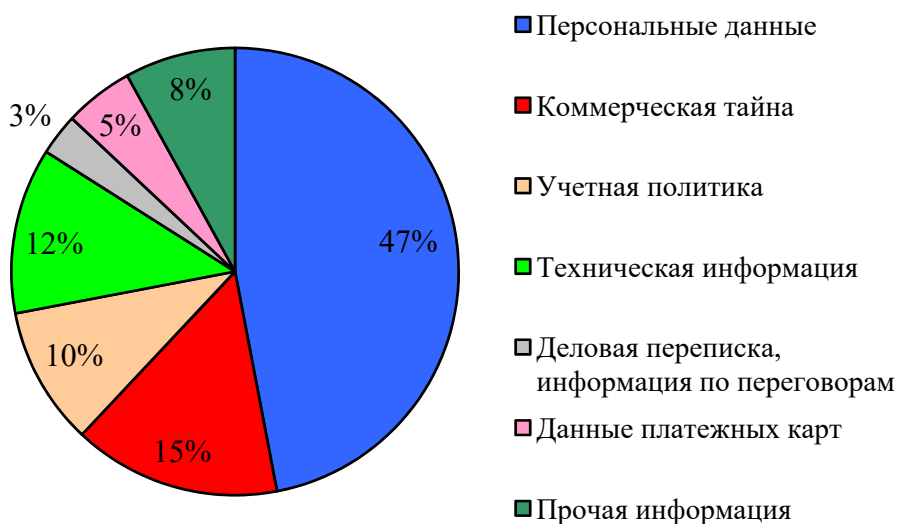


Рис. 1. Основные виды украденной конфиденциальной информации у промышленных предприятий [6]

В качестве основной причины нарушений в сфере информационной безопасности, повлекшей утечку конфиденциальной информации, выделяется человеческий фактор.

Ошибки, нарушения, недостаточный уровень профессиональной компетенции и должностная халатность – это первая группа причин, вследствие которых нарушается экономическая и информационная безопасность хозяйствующего субъекта. Экономические потери и ущерб, как результат некомпетентности сотрудников, причем прежде всего на руководящих должностях, может быть весьма ощутимым и привести к катастрофическим последствиям для компании.

Однако вероятность утечки конфиденциальной информации, составляющей коммерческую тайну бизнеса, вследствие противоправных действий сотрудников (или бывших сотрудников) компании значительно выше. Так, на долю нарушений информационной безопасности в результате преступной деятельности сотрудников компании, связанной с коррупцией, нарушением или превышением должностных обязанностей, приходится порядка 43 % от общего числа утечек информации. Для сравнения: утечки конфиденциальной информации вследствие несанкционированного проникновения в компьютерную систему занимают 18 %, а кража документов – 10 % от общего числа [7].

Таким образом, уровень защищенности конфиденциальной информации и обеспеченности информационной безопасности хозяйствующего субъекта в целом напрямую зависит от эффективности процесса разработки и реализации кадровой стратегии на предприятии.

В контексте сегодняшнего дня, когда на российский бизнес оказывается колоссальное давление извне, роль информационной составляющей процесса обеспечения экономической безопасности субъекта и национальной безопасности государства является решающей. Развитие информационных технологий, к сожалению, привело также и к развитию мошенничества в IT-сфере. Таким образом, при разработке и совершенствовании методов и средств обеспечения информационной безопасности организация сталкивается с массой проблем. Часть трудностей и проблем связаны с противостоянием внешнему воздействию на систему безопасности объекта, а большая часть – с преодолением внутренних разногласий и конфликтов, которые ведут к ухудшению рабочей обстановки и внутрикорпоративной культуры, ускорению текучести кадров.

Совершенствование процесса обеспечения информационной безопасности хозяйствующего субъекта и защиты конфиденциальной информации от несанкционированного доступа должно опираться на улучшение функционирования службы (подразделения) экономической безопасности предприятия (рис. 2), а также с учетом наиболее приоритетных направлений защиты информационных ресурсов (рис. 3).

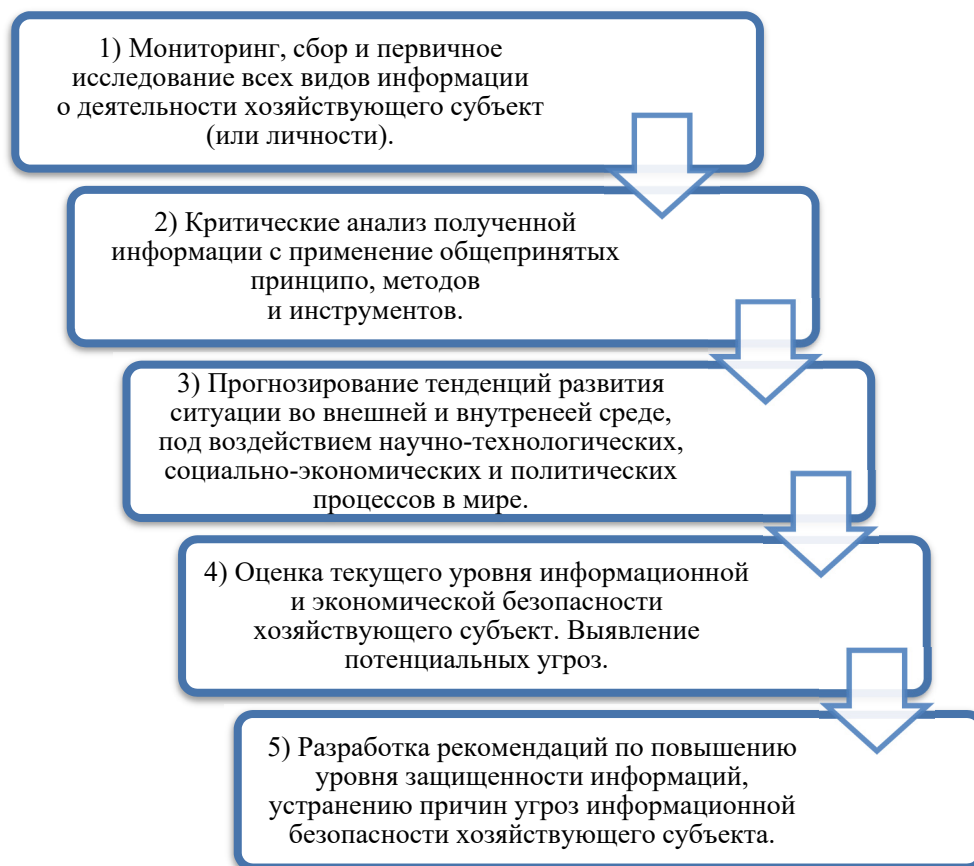


Рис. 2. Основные функции отдела экономической безопасности предприятия в сфере защиты информационных ресурсов

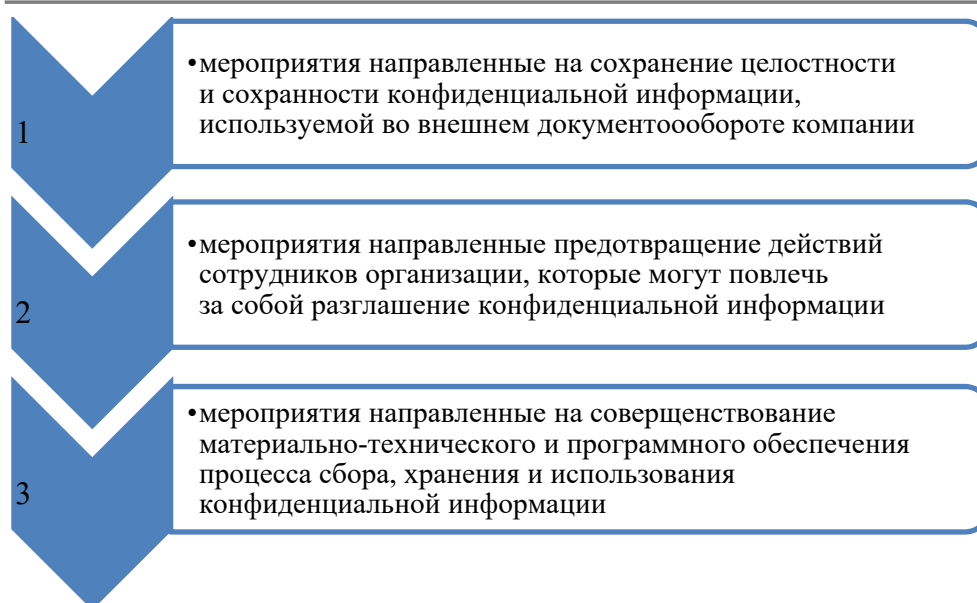


Рис. 3. Основные направления защиты информационных ресурсов хозяйствующего субъекта

Вопросы и проблемы, связанные с обеспечением информационной и экономической безопасности хозяйствующего субъекта, стоят на приоритетном месте среди управленческих задач. Динамика роста угроз безопасности отечественных производственных компаний за последние три года имеет негативный характер. Количество нарушений и преступлений в сфере информационной безопасности каждый год увеличивается. Так, за 2023 г. рост оценивается в 12 % относительно 2022 г., а за 2024 г. +24 % относительно прошлого периода [6].

Основным методом несанкционированного доступа к информационным ресурсам объекта на сегодняшний день является использование специальных вредоносных программ, на их долю приходится до 80 % от общего числа [8].

В качестве наиболее часто используемых источников хакерских атак выделяются интернет и методы удаленного подключения, что обусловлено не совсем рациональным и корректным расположением модемов сотовой связи [9]. На рис. 4 представлено распределение хакерских атак на информационные ресурсы организаций по механизмам их реализации.

Одним из наиболее часто используемых методов получения несанкционированного доступа к конфиденциальной информации является фишинговая атака, в результате которой сотрудник компании получает письмо, содержащее вредоносную программу. Результатом подобной атаки является установка на компьютер жертвы вредоносной (шпионской) программы, позволяющей манипулировать информацией. Чтобы максимально заинтересовать человека в данном письме, злоумышленники используют фишинговые сообщения следующих видов: сообщение от контрагентов (27 % от общего числа); от техподдержки (15 %); от государственных или контролирующих органов (13 %); актуальные новости и сообщения (10 %); сообщения от работодателя (9,5 %); сообщения на тему трудоустройства (7 %); развлекательный контент (3 %) [6].

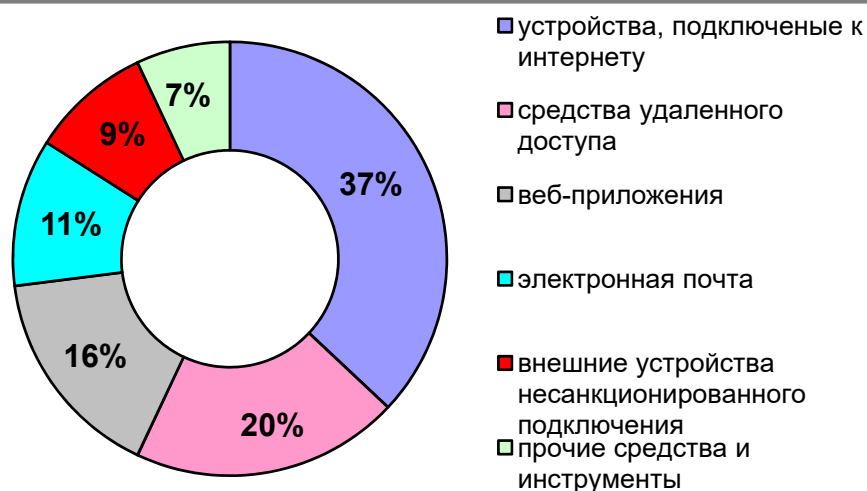


Рис. 4. Механизмы, используемые для реализации хакерских атак на информационные ресурсы организаций [9]

Обобщая вышеприведенные данные, можно сделать вывод, что в современных условиях хозяйствующему субъекту необходимо уделять пристальное внимание вопросам обеспечения защиты и безопасности собственной конфиденциальной информации. Данный процесс должен осуществляться на постоянной, непрерывной основе.

Результаты и обсуждение

Обеспечение информационной и экономической безопасности в целом требует от компании не только внимания, но и финансовых ресурсов. Приоритетность финансирования данной сферы деятельности должна определяться в зависимости:

- от текущей ситуации в бизнес-среде и наличия потенциальных угроз для хозяйствующего субъекта;
- от финансовых возможностей самой организации, уровня ее финансовой устойчивости и стратегии распределения затрат.

Разработку и применение методов и средств защиты конфиденциальной информации рекомендуется осуществлять на основе результатов подробного анализа динамики изменения показателей, характеризующих информационную безопасность объекта:

- коэффициент защищенности конфиденциальной информации;
- коэффициент информационной вооруженности;
- производительность информации [9].

При этом необходимо учитывать, что информационная и экономическая безопасности хозяйствующего субъекта представляют собой целый комплекс организационно-технических, финансово-экономических и управленческих показателей и критериев. В связи с этим совершенствование методов, механизмов и инструментов защиты информационных ресурсов в целях повышения уровня безопасности объекта – это задача многогранная, требующая комплексного подхода, ориентированного на непрерывное, планомерное развитие всей материально-технической базы предприятия (рис. 5).

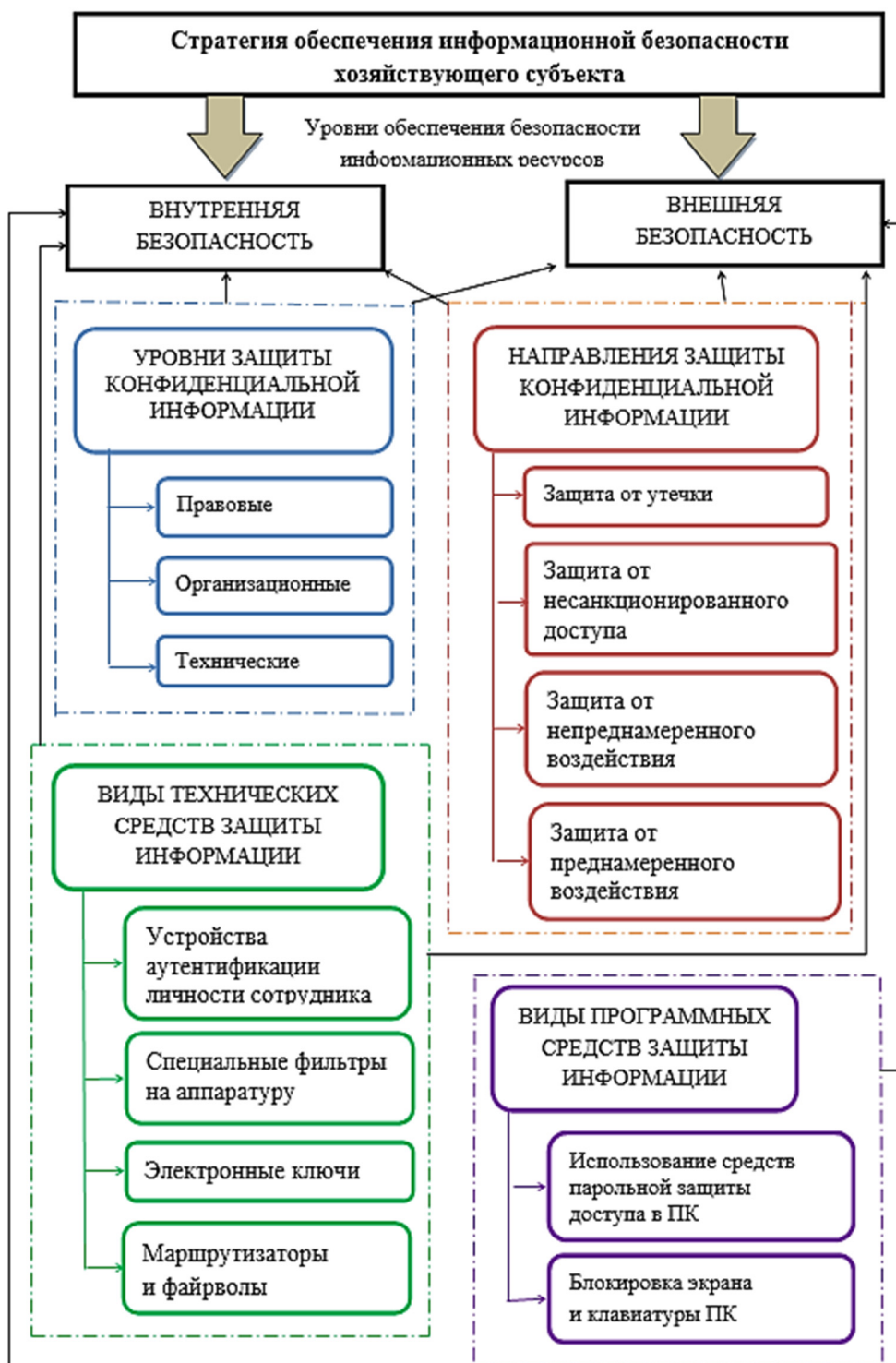


Рис. 5. Комплексный подход к совершенствованию методов и механизмов защиты информационных ресурсов организаций

Согласно официальным данным, главной причиной утечки конфиденциальной информации (до 80 % от общего числа) и других нарушений в сфере защиты информационных ресурсов хозяйствующего субъекта, является человеческий фактор, тогда организации необходимо усилить контроль за действиями своих сотрудников [8].

Основные направления совершенствования кадровой политики в сфере управления информационной безопасностью и, в частности, обеспечения защиты конфиденциальной информации:

- 1) повышение уровня информационной грамотности, теоретических и практических знаний в области защиты конфиденциальной информации;
- 2) повышение персональной ответственности сотрудников компании за сохранность сведений конфиденциального характера, усиление трудовой дисциплины и ужесточение мер (способов) дисциплинарного взыскания за нарушения;
- 3) организация и проведение профилактической работы с трудовым коллективом по предупреждению нарушений (должностных преступлений) в сфере информационной безопасности;
- 4) совершенствование методов и способов стимулирования сотрудников, имеющих доступ к конфиденциальной информации и средствам защиты информационных ресурсов объекта.

Таким образом, одними из первостепенных задач руководителей хозяйствующего субъекта являются разработка и внедрение эффективных мер, направленных на снижение текучести кадров в организации, стабилизацию кадровой политики, мотивацию персонала на обеспечение сохранности конфиденциальной информации и повышение уровня информационной безопасности объекта в целом [10]. Уровень качества материально-технического и программного обеспечения процесса «сбор – хранение – использование конфиденциальной информации» также во многом зависит от обеспеченности компании кадровыми и финансовыми ресурсами [11, 12].

Заключение

Обобщая все вышесказанное, можно сделать следующий вывод: на современном этапе развития экономического пространства, бизнес-процессов и общества информация является своеобразным товаром, обладающим особой ценностью и значимостью. В связи с этим проблема защиты конфиденциальной бизнес-информации от утечки и разглашения – это ключевая задача хозяйствующего субъекта в сфере реализации собственной стратегии обеспечения финансово-экономической стабильности и экономической безопасности.

Тесная взаимосвязь уровня экономической безопасности хозяйствующего субъекта, его финансовой устойчивости, стратегии обеспечения конкурентоспособности на долгосрочную перспективу и возможности по предотвращению утечки конфиденциальной информации, доказывают необходимость реализации комплексного подхода к обеспечению информационной безопасности объекта. Основу данной комплексной системы должны составлять административно-управленческие, организационно-технические и программно-аппаратные методы защиты информационных ресурсов от несанкционированного доступа и использования. Уровень эффективности функционирования данной системы напрямую зависит от уровня профессиональной компетентности сотрудников предприятия, а также их порядочности и морально-этических принципов.

Таким образом, несмотря на рост уровня информатизации и компьютеризации всех бизнес-процессов, самым приоритетным направлением в сфере обеспечения экономической безопасности хозяйствующего субъекта по-прежнему остается совершенствование кадровой политики компании, в том числе по вопросу защиты конфиденциальности информационных ресурсов бизнеса.

Список литературы

1. Кондрашова Н. Г. Защита информации как важная составляющая экономической безопасности // *Modern Economy Success*. 2022. № 6. С. 149–153.
2. Об информации, информационных технологиях и о защите информации : федер. закон № 149-ФЗ от 27.07.2006 (ред. от 09.11.2024) // КонсультантПлюс. URL: www.consultant.ru (дата обращения: 26.11.2024).
3. Ткачева М. В., Береснев Н. Р. Средства и методы защиты информации в рамках обеспечения экономической безопасности организации: основная характеристика // *Современная экономика: проблемы и решения*. 2024. № 5 (173). С. 165–177.
4. Фомичева И. В., Юдина О. В., Поляков Д. В. Разработка мер защиты конфиденциальной управленческой информации в организации // *Научные исследования и разработки. Экономика*. 2024. Т. 12, № 2. С. 56–60.
5. Евсултанова М. М., Селиванова С. Е., Мощенко О. В. Информационная безопасность как составляющая экономической безопасности организации // *Экономические науки*. 2023. № 229. С. 124–127.
6. Positive technologies. URL: <https://www.ptsecurity.com/ru-ru/> (дата обращения: 27.11.2024).
7. Сорокин П. А. Разработка мер по совершенствованию системы защиты коммерческой тайны в целях повышения уровня экономической безопасности коммерческих организациях // *Вестник евразийской науки*. 2023. Т. 15, № S6.
8. Кибербезопасность 2023 в цифрах, прогноз на 2024. URL: <https://wtcmoscow.ru/company/news/5334/?ysclid=lun0s> (дата обращения: 27.11.2024).
9. Лунова С. К., Комиссарова М. А., Семенова В. Н. Актуальные вопросы обеспечения информационной безопасности объектов экономики // *Технико-технологические проблемы сервиса*. 2024. № 2 (68). С. 107–114.
10. Гамидуллаева Л. А. Управление и прогнозирование инновационного развития социально-экономических систем: теория, методология и практика. Пенза : Изд-во ПГУ, 2019. 430 с. EDN: ACCSCO
11. Vasin S. M., Gamidullaeva L. A., Finogeev A. G. [et al.]. The use of benchmarking tool to improve efficiency of company's innovation activities in the conditions of digital economy // *International Journal of Process Management and Benchmarking*. 2021. Vol. 11, № 2. P. 151–177. doi: 10.1504/IJPMB.2021.113736 EDN: GFZIU Y
12. Васин С. М., Финогеев А. Г., Гамидуллаева Л. А. [и др.]. Разработка методики моделирования и прогнозирования конкурентоспособности научно-технических предприятий с использованием технологии бенчмаркинга // *РИСК: Ресурсы, Информация, Снабжение, Конкуренция*. 2019. № 4. С. 190–196. EDN: QWSZLR

References

1. Kondrashova N.G. Information protection as an important component of economic security. *Modern Economy Success*. 2022;(6):149–153. (In Russ.)
2. About information, information technologies and information protection : feder. Law № 149-FZ of 27.07.2006 (as amended on 09.11.2024). *ConsultantPlus*. (In Russ.). Available at: www.consultant.ru (accessed 26.11.2024).
3. Tkacheva M.V., Beresnev N.R. Means and methods of information protection in the framework of ensuring the economic security of the organization: the main characteristics. *Sovremennaya ekonomika: problemy i resheniya = Modern economics: problems and solutions*. 2024;(5):165–177. (In Russ.)

4. Fomicheva I.V., Yudina O.V., Polyakov D.V. Development of measures to protect confidential management information in an organization. *Nauchnye issledovaniya i razrabotki. Ekonomika = Scientific research and development. Economy*. 2024;12(2): 56–60. (In Russ.)
5. Evsultanova M.M., Selivanova S.E., Moshchenko O.V. Information security as a component of an organization's economic security. *Ekonomicheskie nauki = Economic sciences*. 2023;(229):124–127. (In Russ.)
6. *Positive technologies*. Available at: <https://www.ptsecurity.com/ru-ru/> (accessed 27.11.2024).
7. Sorokin P.A. Development of measures to improve the system of trade secret protection in order to increase the level of economic security of commercial organizations. *Vestnik evraziyskoy nauki = Bulletin of Eurasian Science*. 2023;15(S6). (In Russ.)
8. *Kiberbezopasnost' 2023 v tsifrah, prognoz na 2024 = Cybersecurity 2023 in numbers, forecast for 2024*. (In Russ.). Available at: <https://wtcmoscow.ru/company/news/5334/?ysclid=lun0s> (accessed 27.11.2024).
9. Luneva S.K., Komissarova M.A., Semenova V.N. Current issues of ensuring information security of economic facilities. *Tekhniko-tehnologicheskie problemy servisa = Technical and technological problems of the service*. 2024;(2):107–114. (In Russ.)
10. Gamidullaeva L.A. *Upravlenie i prognozirovaniye innovatsionnogo razvitiya sotsial'no-ekonomicheskikh sistem: teoriya, metodologiya i praktika = Management and forecasting of innovative development of socio-economic systems: theory, methodology and practice*. Penza: Izd-vo PGU, 2019:430. (In Russ.).
11. Vasin S.M., Gamidullaeva L.A., Finogeev A.G. [et al.]. The use of benchmarking tool to improve efficiency of company's innovation activities in the conditions of digital economy. *International Journal of Process Management and Benchmarking*. 2021; 11(2):151–177. doi: 10.1504/IJPMB.2021.113736
12. Vasin S.M., Finogeev A.G., Gamidullaeva L.A. [et al.]. Development of a methodology for modeling and forecasting the competitiveness of scientific and technical enterprises using benchmarking technology. *RISK: Resursy, Informatsiya, Snabzhenie, Konkurentsiya = RISK: Resources, Information, Supply, Competition*. 2019;(4):190–196. (In Russ.).

Информация об авторах / Information about the authors

Светлана Сергеевна Солдатова

кандидат экономических наук, доцент
кафедры менеджмента
и государственного управления,
Пензенский государственный университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: sssoldatova@mail.ru

Svetlana S. Soldatova

Candidate of economical sciences,
associate professor of the sub-department
of management and public administration,
Penza State University
(40 Krasnaya street, Penza, Russia)

**Автор заявляет об отсутствии конфликта интересов /
The author declares no conflicts of interests.**

Поступила в редакцию/Received 02.12.2024

Поступила после рецензирования/Revised 23.01.2025

Принята к публикации/Accepted 29.01.2025