ЭКОНОМИЧЕСКИЙ РОСТ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ / ECONOMIC GROWTH: PROBLEMS AND PROSPECTS

DOI 10.24182/2073-6258-2025-24-2-9-14

Обзорная статья / Review article
УДК 004.056.5

Проблемы информационной безопасности хозяйствующих субъектов

О. Б. Репкина

доктор экономических наук, профессор
РТУ МИРЭА,
Москва, Россия
olrepk@mail.ru

Аннотация: *В статье рассмотрены проблемы обеспечения безопасности в процессе обработки, хранения и передачи информации в современных условиях хозяйствования. При рассмотрении всеобъемлющего характера, важности и необходимости информационного обеспечения любого процесса выделены основные проблемы его защиты. Здесь отдельно рассматривается информационная безопасность на различных уровнях использования и различными субъектами; анализируется актуальная нормативно-правовая база. Информация определяется как элемент конкурентного преимущества и конкурентоспособности, что определяется потенциальной способностью роста на основе получаемой, особенно принципиально новой базы данных, и как элемент защиты уже имеющихся преимуществ, заключаемых в определенном содержании информации. В результате делаются выводы об актуальных опасностях защиты информации для хозяйствующих субъектов и выдвигаются направления возможного решения выявленных проблем и трудностей.*

Ключевые слова: *информация, информационная безопасность, хозяйствующий субъект, защита информации.*

Для цитирования: *Репкина О.Б. Проблемы информационной безопасности хозяйствующих субъектов. Ученые записки Российской академии предпринимательства. 2025. Т. 24. № 2. С. 9—14. https://doi.org/10.24182/2073-6258-2025-24-2-9-14.*

Problems of information security of economic entities

O. B. Repkina

Dr. Sci. (Econ.), Prof.
RTU MIREA,
Moscow, Russia
olrepk@mail.ru

Abstract: *The article examines the problems of ensuring security in the process of processing, storing and transmitting information in modern economic conditions. Having considered the comprehensive nature, importance and necessity of information support for any process, the main problems of its protection are highlighted. Here, information security is considered separately at various levels of use and by various entities; the current regulatory framework is analyzed. Information is defined as an element of competitive advantage and competitiveness, which is determined by the potential ability to grow on the basis of the received, especially fundamentally new database, as well as the protection of existing advantages contained in a certain content of information. As a result, conclusions are drawn about the current dangers of information protection for economic entities and directions for possible solutions to the identified problems and difficulties are put forward.*

Keywords: *information, information security, economic entity, information protection.*

For citation: *Repkina O.B. Problems of information security of economic entities. Scientific notes of the Russian academy of entrepreneurship. 2025. T. 24. № 2. P. 9—14. https://doi.org/10.24182/2073-6258-2025-24-2-9-14.*

Информация является неотъемлемым источником любой деятельности. Именно в результате сбора, обработки и анализа информации решаются практически все возникающие проблемы во все сферах жизнедеятельности. То есть информация лежит в основе всего и является результатом всего, а, следовательно, развивается параллельно не только со всеми технологическими и техническими новшествами, но и со всеми идеями и мыслями. Граница оценки угроз безопасности информации — совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации (безопасность) в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации (обеспечения безопасности).[1]

Рассмотрим, какие области работы с данными являются уязвимыми в современных условиях хозяйствования.

Несмотря на практически постоянный набор мероприятий и последовательность работы с данными, научно-технический прогресс существенно меняет инструменты работы с ними. В современный век цифровизации появляются все большие возможности сбора, обработки и хранения информации. Бумажные носители все больше дублируются цифровыми аналогами, и основная предпосылка такого активного перехода определялась, в первую очередь, скоростью обработки и передачи практически неограниченного объема данных между практически не ограниченным количеством участников, при необходимости.

Однако появившиеся возможности работы с данными в условиях цифровой трансформации также приводят к большому количеству потенциальных и реальных проблем.

Во-первых, и, наверное, наиболее главное, — это проблема защиты информации на всех этапах работы с ней. Традиционно методы защиты информации рассматривают с точки зрения состояния среды ее обработки, хранения и передачи, которые регламентированы нормативно-правовой базой. «В правовом аспекте информационная безопасность может быть нарушена при умышленном или случайном нарушении свойств информационной среды. Менеджмент хозяйствующего субъекта столкнется тогда с уничтожением или модификацией информации».[2] И, конечно, так называемые «инженерно-технические методы защиты информации».[3] Если при использовании физических носителей основной вопрос был в ограничении физического доступа к носителю информации, то с появлением цифровых аналогов появились угрозы несанкционированного доступа, характерные для нового формата хранения. Сейчас мы рассматриваем информацию, которая не относится к какому-либо уровню секретности, но является не менее важной в жизни и деятельности любого хозяйствующего субъекта. В условиях рыночного ведения хозяйства практически любая информация, будь то базы данных покупателей или поставщиков, контакты клиентов, бизнес-планы или система мотивации, может стать серьезной угрозой конкурентного преимущества.

Во-вторых, нормативно-правовое регулирование работы с информацией.

Основными нормативно-правовыми актами на сегодняшний день являются: ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (рассматривается в основном область государственных информационных систем), ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи», ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне», ФЗ от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» (принципиально затрагивается автоматизированная система управления технологическим процессом).

[1] «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) https://www.consultant.ru/document/cons_doc_LAW_378330/8539d19b30e5fe187e659af4e0aa91a8415db318/

[2] Богданова А. М., Путилов А. О. Защита конфиденциальных данных, как способ поддержания информационной безопасности. Скиф. 2020. № 5-1 (45). – URL: https://cyberleninka.ru/article/n/zaschita-konfidentsialnyh-dannyh-kak-sposob-podderzhaniya-informatsionnoy-bezopasnosti (дата обращения: 23.03.2025).

[3] Аль-аммори А., Дяченко П. В., Клочан А. Е., Бакун Е. В., Козелецкая И. К. Методы и средства защиты информации. The Scientific Heritage. 2020. № 51-1. – URL: https://cyberleninka.ru/article/n/metody-i-sredstva-zaschity-informatsii (дата обращения: 23.03.2025).

Ряд Указов Президента РФ: от 06.03.1997 № 188-ФЗ «Об утверждении перечня сведений конфиденциального характера»; от 05.12.2016 № 646-ФЗ «Об утверждении Доктрины информационной безопасности РФ»; от 22.05.2015 № 260-ФЗ «О некоторых вопросах информационной безопасности РФ». Также ряд Постановлений Правительства РФ, Приказы ФАПСИ РФ; ФСТЭК РФ; ФСБ РФ. Основные из них, как мы видим, принимались преимущественно до 2017 года. Это объясняется появившимися объективными требованиями хозяйствования в новых условиях. Однако данная сфера развивается слишком динамично и здесь необходима постоянная адаптация нормативно-правовых актов под новые условия.

Здесь наблюдается некоторое противоречие. Объективно практически все понимают, насколько важна информационная безопасность для всех участников хозяйственной деятельности и для жизни каждого гражданина. Формально решение потенциальных или возникающих проблем осуществляют в формате имеющегося нормативно-правового регулирования. В частности, работа с информацией защищена разрешительным форматом. Однако это не уменьшает опасность потери или утечки информации, а, скорее, наоборот. Повсеместное распространение информации, защищенное лишь формально, не уменьшает ее распространение. А увеличивает ее количество в большем количестве использования и, соответственно, повышает вероятность потери и утечки.

К основным каналам утечки информации, кроме бумажных носителей, файловых хранилищ, баз данных и флэш-накопителей, съемных носителей, с использованием сети Интернет можно отнести:

- электронную почту,
- мессенджеры,
- социальные сети,
- облачные сервисы и др.

Ну и, конечно, человек рассматривается как центр рисков информационной безопасности, как следствие:

- халатности,
- переманивания,
- хищения,
- утечки.

Также недостаточно хорошо работает система отзыва неактуальной для текущего момента информации. В результате большое количество информации, которая «уже была отработана», становится потенциально опасным для повторного несанкционированного использования.

Так, например, в современных условиях санкций произошло существенное изменение на рынке программных продуктов для бизнеса. С одной стороны, это приводит к замещению отечественными аналогами, но они присутствуют не во всех областях. В результате бизнес использует программное обеспечение без обновлений, что ограничивает функциональность и снижает степень защищенности процесса эксплуатации.

Еще одна перманентная проблема заключается в самом подходе к защищенности информации, а, вернее, в его отсутствии. При решении каких-либо вопросов, как и при проведении аналитических действий, ценность информации определяется ее полезностью для обработки, и вопросы безопасности не берутся во внимание. Защищают информацию в основном с помощью соблюдения формальных требований по согласию на ее обработку. При этом запрашивающая сторона выполняет свою часть, определенную законодательно, а сторона, дающая такое согласие, объективно не имеет выбора.

Бесспорность необходимости защиты информации очевидна, но здесь можно также отметить некоторые трудности.

Во-первых, это очень широкий круг возможных угроз. Кроме традиционного деления на внешние и внутренние источники выделяют также уязвимость информации на электронных носителях, например. Цифровой формат отличается тем, что большой объем данных можно копировать и перемещать практически мгновенно без нарушения содержания, объема и оформления. Новые методы атак появляются постоянно, а система защиты играет роль догоняющего, то есть потенциальные угрозы и фактические атаки опережают обновление защитных систем.

Во-вторых, отсутствие возможности не столько поиска, сколько доказательства виновников утечки данных. Это происходит по причине того, что далеко не вся информация, которая может быть потенциально интересна злоумышленникам, имеет конфиденциальный характер, а значит, используется и доступна большому количеству пользователей.

В настоящее время существуют законодательные меры регламентации работы с информацией. Сюда можно отнести классификацию, согласно законодательству (государственная, служебная и профессиональная тайна; персональные данные и т.д.); требования государственных органов (например, Роскомнадзора) и отраслевые стандарты (например, положения ЦБ РФ); договорное (юридическое) закрепление ответственности и санкции за ее разглашение; технические мероприятия по защите (например, аутентификация) и др.

Тем не менее на уровне отдельного хозяйствующего субъекта можно рассмотреть организационные мероприятия по защите информации:

- четкая регламентация доступа, что в некоторых случаях может стать очень хлопотным мероприятиям, как по процедуре, так и по обеспечению ресурсами, но с позиции сокращения угроз — может быть оправдана;
- распределение персональной ответственности, в частности, во всех должностных инструкциях и регламентах работ, где необходимо в обязательном порядке ввести персональную ответственность за соблюдение информационной безопасности;
- создание системы разделения обязанностей по защите информации;
- стандартизация работы с документами через классификацию данных (например, по уровню конфиденциальности).

Таким образом, необходимо обеспечить баланс между защитой и удобством. Это означает, что меры безопасности должны быть такими, чтобы, с одной стороны, не ограничивать информацию для использования, а, с другой стороны, чтобы чрезмерно не блокировать пользователей информации, то есть баланс между свободой информации и необходимостью ее ограничения. Одновременно наблюдается ограниченная осведомленность пользователей о рисках, связанных с работой с информацией. Это представление формируется преимущественно интуитивно.

Перечень угроз безопасности информации содержится, в частности, в «Методическом документе. “Методика оценки угроз безопасности информации” (утв. ФСТЭК России 05.02.2021)». Также в нашей стране существует проработанная система уведомления об утечке (в частности, персональных данных) Роскомнадзора и ФСБ.

Обозначим основные опасности и угрозы информационной безопасности:

- утечка информации через спланированные кибератаки, вирусы, фишинг и др.;
- утечка по вине физической потери из-за человеческого фактора или несовершенства системы защиты;
- мошенничество через дезинформацию и манипуляцию, несанкционированный доступ к базам данных;
- повреждение целостности информации из-за использования санкционного программного обеспечения;
- техногенные нарушения из-за быстро устаревающих технических средств;
- утечка данных, как следствие работы недобросовестных конкурентов, в том числе, внедрение в компанию для сбора информации;
- отсутствие должного контроля за действиями сотрудников.

В результате на уровне хозяйствующего субъекта возникают юридические риски, риски репутации, потери клиентов и конкурентоспособности.

Специфической областью, требующей защиты информации хозяйствующих субъектов, является промышленный шпионаж или конкурентная разведка (первый можно считать незаконным аналогом второго). Если конкурентная разведка используется для изучения обстановки и бизнес-процессов, оценки и прогнозирования действия конкурентов, то промышленный шпионаж связан с нарушением законодательства при проведении конкурентной разведки.

К основным направлениям защиты информации можно отнести:
- нормативно-правовую защищенность;
- техническую защищенность;
- административную защищенность, выраженную правилами и обязательствами по обеспечению информационной безопасности;
- работу с человеческим фактором;
- прогнозирование угроз в результате анализа угроз и потоков данных;
- ретроспективный анализ.

Список литературы

1. Авакьян С.А. Задачи конституционного права в аспекте защиты (от) информации. Конституционное и муниципальное право. 2022. № 8.
2. Аль-аммори А., Дяченко П.В., Клочан А.Е., Бакун Е.В., Козелецкая И. К. Методы и средства защиты информации. The Scientific Heritage. 2020. № 51–1. – URL: https://cyberleninka.ru/article/n/metody-i-sredstva-zaschity-informatsii (дата обращения: 23.03.2025).
3. Богомолова Людмила Валерьевна Информационная безопасность: что это такое в современных реалиях. Вестник науки и образования. 2023. № 1 (132)-1. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-chto-eto-takoe-v-sovremennyh-realiyah (дата обращения: 23.03.2025).
4. Курбанов Т.К., Карачаев А.Р., Пашаева Ф.Р., Гитинов Х.Х. Анализ методов защиты от несанкционированного доступа к личной информации. Образование и право. 2022. № 5. – URL: https://cyberleninka.ru/article/n/analiz-metodov-zaschity-ot-nesanktsionirovannogo-dostupa-k-lichnoy-informatsii (дата обращения: 23.03.2025).
5. Богданова А.М., Путилов А.О. Защита конфиденциальных данных, как способ поддержания информационной безопасности. Скиф. 2020. № 5-1 (45). – URL: https://cyberleninka.ru/article/n/zaschita-konfidentsialnyh-dannyh-kak-sposob-podderzhaniya-informatsionnoy-bezopasnosti (дата обращения: 23.03.2025).
6. Громов Павел. Что такое информационная безопасность и с какими угрозами она борется. Подробнее на РБК: https://trends.rbc.ru/trends/industry/674c87529a79474ade9314d3?from=copy.
7. Чапис М.А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере. Наукосфера. 2024. № 6-1. С. 551–557.
8. Bissaliyev M.S., Shakirov K.N. ENSURING SAFETY AND PROTECTION OF PERSONAL DATA ON THE INTERNET: ISSUES OF SELECTION OF OPTIMAL RESEARCH METHODOLOGY. Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan. 2024. № 3 (78). С. 42–54.
9. Нурмаммедова О., Гылыджов О., Акыев С., Арсланова Г. Охрана личных данных, информационная защита в современном обществе. Символ науки: международный научный журнал. 2024. Т. 1. № 10-1. С. 66–68.

Reference

1. Avakyan S.A. Tasks of constitutional law in the aspect of protection (from) information. Constitutional and municipal law. 2022. № 8.
2. Al-Ammori A, Dyachenko PV, Klochan AE, Bakun EV, Kozeletskaya IK. Methods and means of information protection. The Scientific Heritage. 2020. № 51-1. – URL: https://cyberleninka.ru/article/n/metody-i-sredstva-zaschity-informatsii (access date: 23.03.2025).
3. Bogomolova Lyudmila Valerievna Information security: what is it in modern realities. Herald of Science and Education. 2023. № 1 (132)-1. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-chto-eto-takoe-v-sovremennyh-realiyah (дата обращения: 23.03.2025).
4. Kurbanov TK, Karachaev A.R., Pashayeva F.R., Gitinov H.Kh. Analysis of methods of protection against unauthorized access to personal information. Education and law. 2022. № 5. – URL: https://cyberleninka.ru/article/n/analiz-metodov-zaschity-ot-nesanktsionirovannogo-dostupa-k-lichnoy-informatsii (дата обращения: 23.03.2025).
5. Bogdanova A.M., Putilov A.O. Protection of confidential data as a way to maintain information security. Scythian. 2020. № 5-1 (45). – URL: https://cyberleninka.ru/article/n/zaschita-konfidentsialnyh-dannyh-kak-sposob-podderzhaniya-informatsionnoy-bezopasnosti (дата обращения: 23.03.2025).
6. Gromov Pavel. What is information security and what threats it fights. Read more on RBC: https://trends.rbc.ru/trends/industry/674c87529a79474ade9314d3?from=copy.

7. Chapis M.A. Information security of the state as a legal procedure for ensuring national security in the information sphere. Scientosphere. 2024. № 6-1. S. 551–557.
8. Bissaliyev M.S., Shakirov K.N. ENSURING SAFETY AND PROTECTION OF PERSONAL DATA ON THE INTERNET: ISSUES OF SELECTION OF OPTIMAL RESEARCH METHODOLOGY. Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan. 2024. № 3 (78). S. 42–54.
9. Nurmammedova O, Gylydzhov O, Akyev S, Arslanova G. Personal data protection, information protection in modern society. Symbol of science: international scientific journal. 2024. VOL. 1. № 10-1. S. 66–68.

Статья поступила в редакцию 13.04.2025; одобрена после рецензирования 05.05.2025; принята к публикации 15.05.2025.

The article was submitted 13.04.2025; approved after reviewing 05.05.2025; accepted for publication 15.05.2025.