

СОХРАННОСТЬ КОММЕРЧЕСКОЙ ТАЙНЫ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

*А.Ш. ХУАЖЕВА, доктор экономических наук, профессор, профессор кафедры экономики и финансов, Адыгейский государственный университет
e-mail: a.khuazheva@mail.ru*

Аннотация

В статье показана роль коммерческой тайны как объекта обеспечения информационной и экономической безопасности. Утечка конфиденциальной информации может привести к финансовым потерям, потере репутации организации и снижению стабильности функционирования. Авторами отмечается, что это особенно актуально не только для предприятий и организаций, но и для органов местного самоуправления, которые управляют финансовыми и информационными потоками на местах, обеспечивая стабильность социально-экономического развития территорий.

Ключевые слова: экономическая безопасность предприятия, коммерческая тайна, конфиденциальность, система защиты, утечка информации, синтетические показатели, бюджет, экономическая безопасность региона, безопасность страны.

DOI: 10.31429/2224042X_2025_77_55

В соответствии с федеральным законодательством коммерческая тайна — это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, избегать неоправданных расходов, сохранять положение на рынке товаров, работ, услуг или получать иную коммерческую выгоду. Такая информация является объектом принятых мер по ее защите и не является общедоступной.

Конфиденциальность информации является более широким понятием, так как, помимо коммерческих сведений, она включает в себя персональные данные, информацию об организации, штате сотрудников, сведения о служебной тайне и др.

Основные критерии, характеризующие отличие коммерческой тайны от других видов

конфиденциальной информации, приведены в таблице.

Эффективная защита коммерческой тайны невозможна без глубокого анализа факторов, угрожающих ее сохранности. Угрозы можно разделить на внутренние и внешние, а также учитывать такие явления, как промышленный шпионаж и корпоративное мошенничество.

К внутренним угрозам относятся действия и бездействия, исходящие от сотрудников компании или других лиц, имеющих доступ к конфиденциальной информации. Основные причины внутренних угроз включают:

1. Недобросовестность сотрудников: умышленное разглашение информации с целью получения личной выгоды (продажа данных конкурентам или использование в собственных интересах); переманивание сотрудниками клиентов и партнеров после увольнения.

2. Небрежность и ошибки персонала: использование слабых паролей или их передача посторонним лицам; неправильное хранение документов (оставленные на столе бумаги, доступ к общим сетевым папкам); случайное распространение информации через электронную почту или мессенджеры.

3. Отсутствие внутренней культуры информационной безопасности: недостаток обучения сотрудников правилам защиты конфиденциальности; отсутствие регламентов и политик по обращению с коммерческой тайной.

4. Злоупотребление доступом: чрезмерный доступ сотрудников к конфиденциальной информации без необходимости; использование личных устройств для хранения и передачи корпоративных данных.

Отличия коммерческой тайны от других видов конфиденциальной информации

Критерий	Коммерческая тайна	Служебная тайна	Персональные данные	Государственная тайна	Банковская тайна
Цель защиты	Экономическая выгода	Обеспечение работы органов	Защита личной жизни	Государственная безопасность	Защита финансовых данных
Регулирующий закон	ФЗ № 98-ФЗ	Ведомственные акты	ФЗ № 152-ФЗ	ФЗ № 5485-1	ФЗ № 395-1
Характер информации	Коммерческая и стратегическая	Должностная информация	Личная информация	Секретная государственная	Финансовая информация
Примеры информации	Клиентская база, ноу-хау	Проекты решений, переписка	Паспортные данные, адрес	Разведывательные данные	Состояние счетов и операций
Меры защиты	Режим защиты, NDA	Режим ограниченного доступа	Шифрование, согласие субъекта	Секретность, допуск	Банковские регламенты

5. Незащищенность внутренних систем — слабая IT-инфраструктура, отсутствие шифрования и контроля доступа к информации.

К внешним угрозам относятся действия третьих лиц, направленные на незаконное получение или распространение коммерчески ценной информации.

К их числу следует отнести в первую очередь:

1. Промышленный шпионаж и недобросовестная конкуренция: целенаправленные действия конкурирующих организаций для получения данных о стратегических планах, технологиях, клиентах и партнерах компании; использование инсайдеров, подкупа сотрудников и внедрения агентов.

2. Хакерские атаки и киберугрозы: кража информации через фишинговые письма, вирусы и трояны; взлом корпоративных серверов и баз данных для извлечения ценной информации.

3. Корпоративное мошенничество третьих лиц: незаконное использование доверительных отношений (например, поставщики или подрядчики могут получить доступ к документам компании и использовать их в своих интересах); имитация деловых переговоров для получения конфиденциальных сведений.

4. Социальная инженерия: манипулирование сотрудниками компании для получения

доступа к информации (например, выдача себя за IT-специалиста или контрагента); использование поддельных запросов на предоставление данных.

5. Утечка через партнеров и подрядчиков: недостаточно защищенные системы контрагентов могут стать причиной распространения информации; несоблюдение договорных обязательств о конфиденциальности.

Как известно, информация является особым экономическим ресурсом, а создание информации — долговременным и затратным процессом, результат которого к тому же обладает признаками неопределенности. Это связано прежде всего с несовершенством практики правоприменения созданной коммерчески ценной информации, отсутствием эффективно функционирующего организационно-экономического механизма и инструментария защиты коммерческой тайны на предприятии.

Создание системы систем сохранности коммерческой тайны и эффективности мер обеспечения экономической безопасности предприятий и организаций может строиться только на комплексном подходе к решению данной задачи.

Оценка экономической эффективности мер по защите коммерческой тайны должна начинаться с проверки организационно-распорядительной документации предприятия,

анализа применяемых технологий обеспечения защиты информации, приравненной к коммерческой тайне и других мероприятий. По полученным результатам данной оценки разрабатываются рекомендации по совершенствованию организационных и технических мер защиты коммерческой тайны с целью повышения эффективности систем защиты и соответствия их правовому полю.

В наиболее оптимальном и универсальном виде, комплекс предлагаемых мер включает в себя такие аспекты, как организационные, технические и правовые меры, а также позволяет оценить их экономическую эффективность.

К числу организационных мер относятся:

1. Разработка и утверждение внутреннего регламента защиты коммерческой тайны. Регламент должен включать перечень конфиденциальных сведений, порядок их обработки и хранения, а также описание ответственности сотрудников за соблюдение конфиденциальности.

2. Назначение ответственного лица за защиту информации, обладающего полномочиями по контролю за выполнением регламента.

3. Проведение регулярных инструктажей для сотрудников, включая обучение методам распознавания угроз и правилам работы с конфиденциальной информацией. Дополнительно, внедрить практические тренинги по использованию систем защиты информации, включая использование DLP и многофакторной аутентификации.

4. Создание специализированной экспертной комиссии, которая займется разработкой перечня сведений, составляющих коммерческую тайну, и проведением аналитической работы по предотвращению утечки и утраты конфиденциальной информации.

5. Введение обязательного подписания соглашений о неразглашении (NDA) с сотрудниками и контрагентами.

В качестве технических мер предлагается:

1. Внедрение системы предотвращения утечек данных (DLP), которая отслеживает и предотвращает несанкционированный доступ и передачу конфиденциальной информации.

2. Организация резервного копирования данных с использованием защищенных серверов.

3. Установка современного антивирусного программного обеспечения и файрволов для защиты от внешних киберугроз.

4. Внедрение многофакторной аутентификации для доступа к системам, содержащим конфиденциальные данные.

5. Регулярное обновление IT-инфраструктуры, включая внедрение сертифицированных решений для мониторинга активности пользователей и анализа инцидентов безопасности.

6. Использование защищенных систем электронного документооборота с возможностью отслеживания доступа и действий пользователей в реальном времени.

Наиболее значимыми правовыми мерами являются:

1. Подготовка юридически обоснованных локальных нормативных актов, регулирующих порядок работы с конфиденциальной информацией в соответствии с требованиями федерального законодательства.

2. Проведение регулярных аудитов соблюдения правовых норм, связанных с защитой данных.

3. Организация мониторинга правоприменения заключённых NDA и проведение внутренних расследований при подозрениях на нарушение их условий.

4. Разработка положений по использованию электронной цифровой подписи (ЭЦП) для подписания финансовых и административных документов, с акцентом на защиту ключей ЭЦП от утраты и несанкционированного использования.

Одним из ключевых шагов обеспечения эффективности системного подхода к защите информации должно стать внедрение политики конфиденциальности предприятия. Для этого необходимо разработать и утвердить локальные нормативные акты, регулирующие правила обращения с конфиденциальной информацией, ее хранения и использования.

Безусловно, следует иметь в виду, что технические меры играют не менее важную роль в защите коммерческой тайны.

В первую очередь предлагается внедрить актуальное программное обеспечение для защиты данных. К примеру, это могут быть системы предотвращения утечек данных (DLP), которые способны контролировать передачу информации, блокировать несанкционированное копирование или отправку файлов за пределы внутренней сети.

Хотя внедрение DLP-систем, резервного копирования и других технических решений требует значительных финансовых вложений, затраты на эти меры значительно ниже возможных потерь от утечки данных.

Особое внимание следует уделить оценке экономической эффективности предложенных мер, которая должна всегда основываться на принципе разумной достаточности финансовых затрат на защиту, когда затраты на нее перекрывают уровень потенциальной ценности защищаемой информации, т.е. затраты на защиту коммерчески ценной информации не должны превышать возможный ущерб от ее разглашения. Кроме того, при реализации данного комплексного подхода необходимо учитывать, что темп уменьшения потерь вследствие нарушения коммерческой тайны должен превышать темп увеличения степени защиты информации, а темп роста степени защищенности коммерческой тайны должен расти быстрее, чем затраты на нее.

Реализация предложенного комплекса мер позволит существенно укрепить защиту конфиденциальности информации, минимизировать риски утечек данных и обеспечить устойчивую и эффективную работу всех структур предприятия и повысить его экономическую безопасность.

Для оценки эффективности предлагаемых мер нами смоделированы три сценария: пессимистичный, реалистичный и оптимистичный.

Пессимистичный сценарий. При отсутствии финансирования на внедрение DLP-систем и обновление IT-инфраструктуры администрация остается уязвимой для внешних и внутренних угроз. Последствия могут включать: увеличение числа утечек данных; увеличение финансовых потерь ежегодно из-за затрат на устранение последствий

утечек; снижение доверия потребителей и партнеров; высокая нагрузка на сотрудников из-за частых инцидентов и необходимости их устранения.

Реалистичный сценарий. При частичной реализации предложенных мер (например, установка антивирусного ПО и организация резервного копирования) можно ожидать: снижение количества инцидентов; уменьшение финансовых потерь; поддержание стабильного уровня доверия со стороны потребителей и контрагентов; сокращение времени на обработку инцидентов за счёт внедрения базовых автоматизированных систем мониторинга; повышение эффективности внутреннего документооборота за счёт внедрения защищенных систем управления.

Оптимистичный сценарий. Полная реализация всех предложенных мер, включая внедрение DLP-систем, обучение сотрудников и модернизацию IT-инфраструктуры, приведет к практически полному устранению утечек данных; снижению финансовых потерь до минимальных значений; увеличению доверия потребителей и партнеров, что улучшит репутацию предприятия и повысит эффективность его работы; повышению мотивации сотрудников за счёт улучшенной организации работы и минимизации угроз; возможности перенаправления сэкономленных ресурсов на развитие социально-экономических проектов.

Выбор сценария зависит от доступных ресурсов, однако даже частичная реализация рекомендаций способна привести к значительным улучшениям в защите конфиденциальной информации и минимизации рисков утечек.

Внедрение предложенных организационных, технических и правовых мер по защите конфиденциальной информации позволит добиться значительных положительных результатов в различных аспектах деятельности предприятия.

1. Укрепление информационной безопасности. Организация контроля доступа к конфиденциальным данным, внедрение DLP-систем и резервного копирования приведут к снижению вероятности утечек данных. За

счет разграничения прав доступа и мониторинга действий сотрудников будет минимизирован риск несанкционированного использования информации.

2. Повышение юридической защищенности. Заключение соглашений о неразглашении (NDA) с сотрудниками и контрагентами, а также разработка локальных актов о защите информации создадут дополнительные правовые барьеры для утечек данных. Это позволит снизить вероятность судебных исков со стороны граждан и партнеров, а также исключить штрафные санкции за нарушение законодательства, например, Федерального закона № 152-ФЗ «О персональных данных». С учетом текущих рисков такие меры могут уменьшить вероятность юридических проблем на 50–60%.

3. Финансовая экономия и предотвращение потерь. Инвестиции в защиту информации позволят избежать значительных финансовых потерь от утечек данных. Прямые экономические выгоды включают предотвращение затрат на ликвидацию последствий утечек и штрафов за нарушение законодательства.

4. Повышение эффективности работы сотрудников. Четко организованный документооборот и разграничение доступа к информации сократят количество ошибок и упростят внутренние процессы, высвобождая ресурсы для выполнения других задач.

5. Снижение рисков кибератак. Обновление IT-инфраструктуры, внедрение многофакторной аутентификации и использование сертифицированного программного обеспечения

значительно снизят вероятность успешных атак хакеров.

6. Укрепление управляемости предприятия. Благодаря системному подходу к защите информации, руководству предприятий станет проще контролировать доступ к данным, отслеживать их использование и принимать обоснованные решения.

Реализация предложенных мер не только снизит риски утечек информации и киберугроз, но и позволит предприятиям и организациям работать более эффективно, в условиях высокого уровня экономической безопасности.

Библиографический список

1. Белова О. Л. Конфиденциальная информация и управление ею в условиях цифровизации. СПб., 2023.
2. Рекомендации по созданию системы защиты коммерческой тайны на предприятиях. М., 2023.
3. Федеральный закон № 98-ФЗ «О коммерческой тайне» от 29 июля 2004 года (с изменениями на 8 августа 2024 года) // Официальный портал «Кодекс». URL: <https://docs.cntd.ru/document/901904607?marker=64U0IK>
4. Хуажева А.Ш., Чиназирова С.К., Водождова З.А. Оценка влияния элементов теневой экономики на экономическую безопасность страны // Вестник Адыгейского государственного университета. Серия 5: Экономика. 2023. № 1 (315). С. 35–42.
5. Хуажева А.Ш., Чиназирова С.К., Харсеева А.В., Ильина Т.В., Веселова Н.Ю., Ищенко О.В., Бондарь О.О. Экономическая безопасность: учебник. М., 2024.