6 [2026]
ISBN 978-5-901722-96-1
ТРАНСПОРТ. ГОРИЗОНТЫ РАЗВИТИЯ

УДК 338.24

АНАЛИЗ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МЕТОДЫ ПРОТИВОДЕЙСТВИЯ И ИХ ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ

Парамонов Руслан Камильевич[1], студент
e-mail: rus.paramonov.06@mail.ru
Лыкова Елизавета Аексеевна[2], магистрант
e-mail: lisalikova@bk.ru
Лыкова Елена Сергеевна[1], к.э.н., доцент кафедры экономики и менеджмента
e-mail: likova_elena@bk.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия
[2] Московский энергетический институт, Москва, Россия

Аннотация. Актуальность противодействия внутренним угрозам и инсайдерским утечкам баз данных обусловлена их значительным влиянием на устойчивость бизнеса и национальную безопасность. Существует ряд факторов, которые делают внедрение современных методов защиты востребованными и необходимыми, такие как: рост тяжести последствий от скомпрометированных записей, необходимость соблюдения законодательства о коммерческой тайне и реализация целей цифровой экономики. Использование таких инструментов, как DLP-системы и регламентация бизнес-процессов, приводит к значительным экономическим эффектам за счет снижения финансовых потерь и сохранения корпоративных активов.

Ключевые слова: внутренние угрозы, инсайдерские утечки, информационная безопасность, коммерческая тайна, DLP-системы, кадровый аудит.

ANALYSIS OF INTERNAL INFORMATION SECURITY THREATS: METHODS OF COUNTERACTION AND THEIR ECONOMIC EFFICIENCY

Ruslan K. Paramonov[1], Student
e-mail: rus.paramonov.06@mail.ru
Elizaveta A. Lykova[2], Master's degree Student
e-mail: lisalikova@bk.ru
Elena S. Lykova[1], Candidate of Economic Sciences, Associate Professor at the Department of Economics and Management
e-mail: likova_elena@bk.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia
[2] Moscow Power Engineering Institute, Moscow, Russia

Abstract. The relevance of countering internal threats and insider data breaches is driven by their significant impact on business resilience and national security. Several factors make the implementation of modern protection methods both in-demand and necessary, such as: the growing

severity of consequences stemming from compromised records, the need to comply with legislation on trade secrets, and the pursuit of digital economy goals. The use of tools such as DLP systems and the regulation of business processes leads to considerable economic benefits by reducing financial losses and preserving corporate assets.

Keywords: internal threats, insider data breaches, information security, trade secrets, DLP systems, personnel audit.

1. Введение и проблематика

На сегодняшний день внутренние угрозы, реализуемые через инсайдерские сливы баз данных и преднамеренный корпоративный саботаж, формируют основной профиль риска для устойчивости бизнеса. Статистика 2024 года демонстрирует качественную трансформацию инцидентов: при снижении общего числа утечек в мире на 25,2%, тяжесть их последствий возросла. Доля крупных утечек (от 1 млн записей) составила лишь 8,2% от общего количества инцидентов, однако именно на них пришлось 98,6% всех скомпрометированных записей персональных данных в мире. При этом до 70% внутренних сливов информации инициируется сотрудниками в период подготовки к увольнению.

Указанная проблематика выходит за рамки частных корпоративных рисков и классифицируется как системный вызов национальной безопасности Российской Федерации. В соответствии с Указом Президента РФ № 400 «О Стратегии национальной безопасности Российской Федерации», внутренний саботаж и хищение интеллектуальной собственности рассматриваются как критические факторы, препятствующие экономическому росту страны. Стратегия напрямую ставит императивную задачу: снижение количества утечек информации ограниченного доступа до минимально возможного уровня (пункт 57.6). Одновременно внутренние угрозы выступают прямым фактором торможения национальной программы «Цифровая экономика Российской Федерации». Ключевой целевой показатель федерального проекта «Информационная безопасность» — сокращение среднего времени простоя государственных и корпоративных информационных систем в результате атак до 1 часа к 2024 году — абсолютно недостижим без нейтрализации инсайдерского фактора. Государство инвестировало в данный проект более 30,2 млрд рублей, однако эффективность этих макроэкономических вложений напрямую зависит от защищенности локальных периметров предприятий.

2. Нормативно-правовая база

Отечественная нормативно-правовая база предоставляет бизнесу легальный и жесткий инструментарий для противодействия внутренним угрозам, опирающийся на Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и профильные стандарты информационной безопасности. Данный закон задает правила преобразования корпоративных данных в защищаемый актив, позволяющий компании увеличивать доходы и сохранять позиции на рынке.

Механизмы, которые закон дает бизнесу, строго алгоритмизированы. Для легитимизации режима коммерческой тайны статья 10 ФЗ-98 требует от предприятия выполнения исчерпывающего комплекса мер:

1. Утверждение точного перечня защищаемой информации, за исключением сведений, не подлежащих засекречиванию по статье 5 (например, система оплаты труда, задолженности перед персоналом, нарушения законодательства).
2. Ограничение доступа к документам и установление постоянного контроля за обращением с данными.

3. Ведение электронных журналов и реестров учета лиц, получивших доступ к информации.

4. Регулирование отношений через трудовые договоры с персоналом и соглашения о неразглашении (NDA) с контрагентами.

5. Обязательное физическое и цифровое нанесение грифа «Коммерческая тайна» на документы с указанием полных реквизитов обладателя.

Безукоризненное выполнение данных требований легитимизирует применение технических систем контроля (таких как DLP). В рамках трудовых отношений статья 11 ФЗ-98 закрепляет обязанность работника соблюдать режим и возвращать все носители (включая электронные токены) при расторжении договора. За нарушение режима закон предусматривает жесткие санкции: дисциплинарную, материальную, гражданско-правовую, административную (штрафы до 200 000 рублей для юридических лиц по ст. 13.14 КоАП РФ) и уголовную ответственность. Реформа 2025 года (ФЗ № 175-ФЗ) радикально ужесточила статью 183 УК РФ: за незаконное получение и разглашение коммерческой тайны, повлекшее тяжкие последствия (саботаж, срыв госконтрактов, крупный ущерб), предусмотрено лишение свободы на срок от 3 до 7 лет со штрафом до 5 млн рублей.

3. Современные методы защиты

Анализ технологических, правовых и кадровых инструментов за 2022–2024 годы позволяет выделить три наиболее эффективных метода минимизации внутренних угроз предприятия.

Внедрение DLP-систем (Data Loss Prevention) контроля утечек

Техническая и организационная механика: DLP-системы обеспечивают непрерывный анализ информационных потоков, пересекающих периметр защищаемой инфраструктуры. Архитектура развертывания охватывает три уровня: Endpoint (конечные рабочие станции, контроль USB-портов и печати), Network (сетевые и почтовые шлюзы) и Discovery (сканирование корпоративных баз данных). Системы контролируют информацию в использовании (Data-in-use), в покое (Data-at-rest) и в движении (Data-in-motion). Механизмы анализа включают оптическое распознавание символов (OCR), технологию цифровых отпечатков документов (Digital Fingerprinting) и лингвистический анализ [1]. Современным трендом является использование поведенческой аналитики (UEBA) для выявления аномалий в рутинных действиях пользователей. Активные системы в режиме реального времени автоматически блокируют передачу защищаемых файлов [2].

Прямой экономический эффект: Внедрение DLP-системы снижает прямые финансовые потери бизнеса от внутреннего мошенничества на 60%. Дополнительный функционал контроля продуктивности дает рост эффективности работы персонала на 23%. Общая совокупная стоимость владения (TCO) компенсируется в течение 12–18 месяцев за счет предотвращения хищений и недопущения оборотных штрафов [3]. На макроэкономическом уровне внедрение подобных систем позволило предотвратить прямой ущерб для российских организаций в 2024 году на сумму от 0,4 до 1,1 трлн рублей.

Аудит прав доступа и управление кадровой безопасностью

Техническая и организационная механика: Метод базируется на интеграции программных инструментов управления привилегированным доступом (PAM) с постоянным кадровым аудитом. Информация классифицируется по уровням ценности, и доступ предоставляется исключительно по принципу служебной необходимости. Служба безопасности выстраивает профили риска сотрудников, осуществляя мониторинг профессионального выгорания, наличия неисполненных долговых обязательств или аффилированности с конкурентами. Выявленные профили риска синхронизируются с DLP-системами для автоматического перевода неблагонадежных лиц в режим усиленного

контроля. Внедряется строгий протокол отзыва цифровых сертификатов и блокировки учетных записей в момент инициации процедуры увольнения сотрудника.

Прямой экономический эффект: Технология пресекает до 70% утечек данных, генерируемых увольняющимся персоналом. Оптимизируются затраты на устранение последствий саботажа и постоянный подбор новых кадров из-за текучести "рисковых" специалистов. Блокировка несанкционированного доступа прямо предотвращает безвозвратную утрату критических производственных технологий (ноу-хау) и баз клиентов, обеспечивая сохранение конкурентных позиций компании на рынке.

Жесткая регламентация бизнес-процессов в рамках режима коммерческой тайны

Техническая и организационная механика: Метод реализуется через управление жизненным циклом информации: от создания документа до его помещения в архив или физического уничтожения. На предприятии вводится алгоритм обязательного подписания соглашений о конфиденциальности (NDA) с сотрудниками и внешними контрагентами, в которых закрепляются сроки охраны данных (минимум 2 года после завершения сотрудничества). Производится сплошная физическая и электронная маркировка носителей визуальным грифом «Коммерческая тайна». Внутренними приказами запрещается использование личных устройств для работы с корпоративными файлами и вынос носителей за пределы офиса.

Прямой экономический эффект: Соблюдение бюрократической и формальной регламентации является единственным легальным основанием для успешного судебного взыскания прямого ущерба и упущенной выгоды с виновного инсайдера в полном объеме. Строго документированные бизнес-процессы делают невозможным оправдание нарушителя «незнанием» статуса информации. Прозрачность операционной деятельности

защищает капитализацию компании от резких падений из-за репутационных потерь и

штрафов за утечку персональных данных, повышая инвестиционную привлекательность

актива [4].

4. Резолюция

Резюмируя вышеизложенное, необходимо сделать жесткий вывод: локальная информационная и экономическая безопасность отдельного предприятия — это базовый фундамент для реализации любых государственных экономических программ. Цели национального проекта «Цифровая экономика Российской Федерации» и Стратегии национальной безопасности физически недостижимы без логической изоляции корпоративных контуров от внутренних деструктивных воздействий. Технологический и экономический суверенитет государства складывается из надежности каждого хозяйствующего субъекта. Внедрение DLP-систем, строгая юридическая легализация режима коммерческой тайны и непрерывный кадровый аудит более не являются факультативной статьей расходов [4]. Сегодня это критические, обязательные инструменты сохранения активов и выживания бизнеса, обеспечивающие экономический суверенитет всей страны в условиях беспрецедентных глобальных и внутренних вызовов.

Список литературы:

1. Буйневич, М.В. Методы выявления инсайдеров в информационных системах: монография / М.В. Буйневич, К.Е. Израилов. — СПб.: Политехника, 2020. — 187 с.

2. Кабанов, А.С. Противодействие инсайдерским угрозам: теория и практика / А.С. Кабанов, А.Б. Лось. — М.: Инфра-М, 2019. — 168 с.

3. Отчёт «Инсайдерские угрозы в российских компаниях: статистика и тренды» / InfoWatch. — 2025. — URL: https://www.infowatch.ru/analytics (дата обращения: 12.05.2026).

4. Лыкова, Е. С. Поиск оптимального уровня конкретизации запроса для максимизации точности релеватности ответов генеративных языковых моделей / Е. С. Лыкова, Е. А. Лыкова // Экономика и предпринимательство. – 2026. – № 2(187). – С. 1089-1094.