Жосан Анна Ивановна
студентка
Научный руководитель
Фомичева Татьяна Леонидовна
канд. экон. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: *в статье рассмотрено место информационной безопасности в системе экономической безопасности предприятия в условиях цифровизации. На основе данных InfoWatch и Positive Technologies проанализированы угрозы для российских организаций, в том числе связанные с человеческим фактором и социальной инженерией. Изучены изменения ответственности за утечки персональных данных с 2025 года и на условном примере рассчитаны возможные потери предприятия. Сделан вывод, что расходы на защиту информации следует рассматривать как инвестиции в устойчивость бизнеса.*

Ключевые слова: *экономическая безопасность, информационная безопасность, цифровизация, утечка персональных данных, социальная инженерия, человеческий фактор, оборотные штрафы.*

Цифровизация перенесла в информационные системы учёт, продажи, документооборот и работу с клиентами, поэтому данные стали одним из главных активов предприятия, а их потеря – прямой угрозой его финансовому положению. По сведениям МВД, которые приводят Е.А. Кравчук и Р.Н. Селезнёв, в 2024 году в России было зарегистрировано 765,4 тыс. киберпреступлений, или 40% от всех

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

выявленных преступлений [3, с. 124]. Цель статьи – показать, как состояние информационной безопасности влияет на экономическую безопасность предприятия, и оценить финансовые последствия инцидентов.

Экономическую безопасность предприятия обычно определяют как состояние, при котором оно сохраняет устойчивость и способно противостоять негативному влиянию внешних и внутренних факторов. В условиях цифровизации её основной составляющей становится информационная безопасность [6, с. 37]. Связь между ними проявляется через последствия угроз: утечка сведений по вине персонала снижает финансовые результаты, утечка клиентских данных ведёт к оттоку клиентов, а недофинансирование защиты в крайнем случае создаёт угрозу банкротства [6, с. 39]. На наш взгляд, потери от инцидентов удобно делить на прямые (штрафы, выкуп, восстановление систем), косвенные (простой, упущенная выгода) и отложенные (утрата доверия клиентов и партнёров).

Угрозы для российских организаций остаются высокими. По данным Positive Technologies, в первом полугодии 2025 года вредоносное ПО применялось в 63% успешных атак, 52% атак завершались утечкой конфиденциальной информации, а в 45% была нарушена основная деятельность организации [1]. За 2023–2025 годы в России скомпрометировано около 4,5 млрд записей персональных данных [2]. В 2025 году InfoWatch зарегистрировал 739 утечек из российских организаций, на 17,8% меньше, чем годом ранее, однако аналитики связывают это снижение в том числе с тем, что компании всё чаще скрывают инциденты [9].

Значительная часть инцидентов связана с человеческим фактором. По оценкам, которые обобщают И.П. Скворцов и А.О. Титарев, с ним, включая социальную инженерию, связано около половины компьютерных инцидентов [7]. Социальная инженерия – это психологическое манипулирование людьми ради доступа к системам и сведениям; к её основным приёмам относятся фишинг, претекстинг (обман по заранее подготовленной легенде) и «приманки» [8]. Так, в 2020 году злоумышленники под видом службы поддержки обзвонили сотрудников Twitter, выманили у них учётные данные через поддельный сайт и за первые часы со-

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

брали около 117 тыс. долл [8]. Не менее опасны и ошибки персонала: доля персональных данных, скомпрометированных в результате случайных инцидентов, выросла с 3% почти до 10%, чаще всего из-за неверной настройки облачных хранилищ [2]. Таким образом, угрозы со стороны персонала мы предлагаем делить на умышленные действия инсайдеров, неосторожные ошибки и действия, спровоцированные извне.

Цена ошибки для бизнеса заметно возросла с конца весны 2025 года, когда начали действовать поправки в КоАП РФ, внесённые законом №420-ФЗ. Компания, допустившая утечку, теперь может заплатить от трёх до двадцати миллионов рублей: сумма растёт вместе с количеством пострадавших людей и чувствительностью сведений. Если инцидент повторится, санкцию рассчитают уже как процент от оборота – от одного до трёх, причём нижняя граница составляет двадцать миллионов, а верхняя пятьсот [5]. Любопытно, что тот же закон вознаграждает добросовестные компании: если организация три года подряд направляла на защиту данных хотя бы десятую долю процента выручки и выполняла установленные требования, повторный штраф назначат в размере одной десятой от минимальной суммы, но в пределах от 15 до 50 млн руб [5]. Посмотрим, что это означает для условной компании с оборотом 5 млрд руб.

Таблица 1

Сравнение затрат условной компании с оборотом 5 млрд руб. при повторной утечке (*расчёт автора по данным* [*5*])

Показатель	Без вложений в защиту	Вложения 0,1% выручки в год
Расходы на защиту за 3 года	-	15 млн руб.
Штраф за повторную утечку	50–150 млн руб.	15 млн руб.
Итого	50–150 млн руб.	30 млн руб.

Даже без учёта того, что защита снижает саму вероятность утечки, второй вариант обходится в 1,7–5 раз дешевле. Отсюда следует практический вывод: защиту стоит выстраивать сразу по четырём направлениям. В организационном плане нужны утверждённые правила работы с информацией, продуманная система прав доступа и заранее расписанный порядок действий при инциденте.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Техническую основу составляют антивирусы, вход с подтверждением вторым фактором, регулярные резервные копии и DLP-системы, которые не дают сотрудникам по ошибке или умышленно вынести конфиденциальные сведения за пределы компании [4, с. 4]. Кадровое направление включает постоянное обучение и пробные фишинговые письма, ведь персонал должен осознавать собственную роль в сохранности данных [7]. Финансовая составляющая – закладывать на защиту не меньше 0,1% выручки.

Таким образом, в условиях цифровизации информационная безопасность стала одной из основных составляющих экономической безопасности предприятия: любой инцидент оборачивается прямыми, косвенными или отложенными потерями. Значительная доля угроз связана с человеческим фактором, поэтому работа с персоналом должна быть равноправной частью системы защиты. С 2025 года законодательство сделало вложения в информационную безопасность экономически выгодными, что позволяет рассматривать их как инвестиции в устойчивость бизнеса.

Список литературы

1. Атаки на разработчиков через GitHub и GitLab достигли рекордного уровня за три года // Хабр : блог компании Positive Technologies. – URL: https://habr.com/ru/companies/pt/news/941620/ (дата обращения: 01.11.2026). – Текст : электронный.

2. За три года в России утекло 4,5 млрд записей персональных данных // InfoWatch: официальный сайт. – URL: https://www.infowatch.ru/company/presscenter/news/za-tri-goda-v-rossii-uteklo-4–5-mlrd-zapisey-personalnykh-dannykh (дата обращения: 01.11.2026). – Текст : электронный.

3. Кравчук, Е. А. Киберугрозы как ключевые угрозы экономической безопасности в условиях современного мира / Е. А. Кравчук, Р. Н. Селезнёв // Вестник юридических исследований. – 2025. – Т. 4, № 3. – С. 123–127. – URL: https://journals.rcsi.science/3034–140X/article/download/378728/351401 (дата обращения: 01.11.2026). – Текст : электронный.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

4. Левинский, А. Т. Система анализа и предупреждения угроз безопасности персональных данных на предприятии / А. Т. Левинский // Политехнический молодежный журнал. – 2019. – № 5. – DOI 10.18698/2541–8009–2019–05–474. – URL: https://ptsj.bmstu.ru/articles/474/474.pdf (дата обращения: 01.11.2026). – Текст : электронный.

5. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : федер. закон : от 30.11.2024 №420-ФЗ. – URL: https://www.klerk.ru/cdoc/view/97be9abc7c135ad43f8c2d8262a4bbd2/ (дата обращения: 01.11.2026). – Текст : электронный.

6. Селезнев, Е. А. Сущность информационной безопасности и ее место в обеспечении экономической безопасности предприятия / Е. А. Селезнев, О. А. Горбунова // Вестник Самарского муниципального института управления. – 2022. – № 1. – С. 36–44. – URL: https://www.imi-samara.ru/wp-content/uploads/2023/03/seleznev-gorbunova-36–44.pdf (дата обращения: 01.11.2026). – Текст : электронный.

7. Скворцов, И. П. О проблеме человеческого фактора в обеспечении информационной безопасности / И. П. Скворцов, А. О. Титарев // Воздушно-космические силы. Теория и практика. – 2022. – № 23. – С. 106–113. – URL: https://cyberleninka.ru/article/n/o-probleme-chelovecheskogo-faktora-v-obespechenii-informatsionnoy-bezopasnosti (дата обращения: 01.11.2026). – Текст : электронный.

8. Социальная инженерия, несовершенный человек / Ж. Нумьер, К. Люмер, А. П. Табурчак, А. Л. Зелезинский // Экономический вектор. – 2022. – № 2 (29). – С. 11–16. – URL: https://cyberleninka.ru/article/n/social-engineering-imperfect-human (дата обращения: 01.11.2026). – Текст : электронный.

9. Утечки данных теряют прозрачность // InfoWatch : официальный сайт. – URL: https://www.infowatch.ru/company/presscenter/news/utechki-dannykh-teryayut-prozrachnost (дата обращения: 01.11.2026). – Текст : электронный.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)