Гребнев Михаил Александрович

магистрант

Научный руководитель

Гребнева Оксана Александровна

канд. техн. наук, доцент

ФГБОУ ВО «Иркутский национальный исследовательский технический университет»

г. Иркутск, Иркутская область

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ ИНТЕРНЕТ-ТЕХНОЛОГИЙ В БИЗНЕСЕ

Аннотация: *авторы статьи отмечают, что в современном мире в связи с повсеместным внедрением цифровых технологий информационные системы играют ключевую роль в развитии экономики. При этом возникают большие риски нарушения информационной безопасности компаний. Поэтому главными задачами в настоящее время становятся задачи разработки мер по защите данных, безопасности их обработки и передачи, что и является целью статьи. Для создания таких мер авторами предлагается использовать системный подход, который позволит не только своевременно реагировать на угрозы, но и предупреждать их негативное воздействие. В статье на примере предприятия по разработке программного обеспечения сформированы меры по обеспечению защиты данных, внедрение которых показало значительное снижение риска нарушения информационной безопасности.*

Ключевые слова: *информационная безопасность, интернет-технологии, угрозы безопасности, бизнес, экономика.*

В современных условиях цифровизация всех отраслей, в том числе и экономики [1], требует более серьезного развития инструментов обработки, хранения и защиты информации. При этом происходит совершенствование программного

обеспечения и технических средств несанкционированного доступа и использования информации.

Смысл термина «информационная безопасность» зависит от конкретного контекста. В Доктрине по информационной безопасности Российской Федерации [2] термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. В Законе РФ «Об информации, информационных технологиях и о защите информации» [3] информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Таким образом, информационная безопасность является важнейшей составляющей для обеспечения национальной и международной безопасности. Для предприятий, работающих с большими объемами данных, обработка которых связана с использованием информационных технологий, осуществление мер по информационной безопасности деятельности предприятия становится особенно важной.

Угрозы безопасности данных. Интернет-технологии предоставляют широкие возможности для ведения бизнеса, но также создают уязвимости для кибератак [4–6]. Под угрозой информационной безопасности понимается потенциально возможные действия или же процессы, которые способны оказать нежелательные воздействия на саму систему или информацию, находящуюся в ней.

Среди основных угроз безопасности данных можно выделить следующие, представленные на рисунке 1 угрозы [7; 8]: 1) незащищенные базы данных, слабые пароли и недостаточная защита сетевых ресурсов могут привести к утечке конфиденциальной информации компании; 2) фишинговые атаки, когда злоумышленник пытается обманом заставить раскрыть личные данные, такие как логины, пароли или финансовую информацию предприятия через фальшивые электронные письма или сайты; 3) вирусы, вредоносное ПО, которые распространяются сами по себе и могут нанести вред локально компьютеру или в целом

сети (могут копировать себя, уничтожать данные, использовать ресурсы компьютера без ведома владельца или выполнять другие вредоносные функции); 4) несанкционированный доступ к системам и данным, когда используются уязвимости в системах безопасности или попросту пытаются подобрать пароли; 5) атаки социальной инженерии направлены на получение доступа к информационным системам компании путем манипуляции и обмана сотрудников; 6) потеря или повреждение данных из-за аппаратных сбоев, природных катастроф, человеческих ошибок или злонамеренных действий, что может иметь серьезные последствия для бизнеса.

Рис. 1. Классификация угроз безопасности
(ПО – программное обеспечение) (составлено авторами)

Эти угрозы требуют тщательной проработки стратегий защиты информации, чтобы минимизировать риски и обеспечить безопасную работу компаний в интернете.

Существующие в настоящее время публикации говорят о том [9–11], что техника защиты информации отстает в своем развитии от технологий, которыми пользуются взломщики для того, чтобы завладеть чужой тайной. Только комплексное использование технических средств, организационных мер и обучения сотрудников может обеспечить достаточный уровень безопасности.

Методы и средства защиты информации на предприятии. Для защиты информации от вышеперечисленных угроз применяются различные современные методы и технологии, к которым относятся: 1) использование шифрования данных, которое является одним из наиболее важных методов защиты данных, в результате действия которого данные переводятся в неразборчивый формат, что делает их недоступными для злоумышленников в случае утечки; 2) применение многофакторной аутентификации, которая вместо использования одного метода аутентификации (пароля) требует двух или более факторов для подтверждения личности сотрудника; 3) внедрение систем обнаружения вторжений, которые способны предупреждать администраторов информационных систем о попытках несанкционированного доступа, вирусных атаках и других подозрительных действиях; 4) установка антивирусного программного обеспечения и фаерволлов, которые обеспечивают защиту от вредоносного ПО; 5) регулярное проведение образовательных треннингов сотрудников по правилам кибербезопасности, которые позволят персоналу соблюдать политику безопасности компании.

Разработка мероприятий по обеспечению информационной безопасности предприятия ООО «Х». В качестве примера выбрано предприятие ООО «Х», которое занимается разработкой и продажей ПО. Деятельность предприятия связана с работой в сети Интернет, включая взаимодействие с клиентами, хранение и обработку данных и др. С целью обеспечения информационной безопасности на предприятии ООО «Х» был проведен аудит текущего состояния системы защиты данных. В ходе аудита выявлены следующие основные угрозы, представленные в таблице 1.

Таблица 1

Анализ текущих рисков ООО «Х» (составлено авторами)

№ пп	Риск	Описание
1	Утечка данных	Слабые пароли, незащищенные базы данных и отсутствие многофакторной аутентификации приводят к высокому риску утечки конфиденциальной информации
2	Фишинговые атаки	Сотрудники часто открывают подозрительные ссылки и вложения в электронных письмах, что увеличивает вероятность фишинговых атак

3	Вирусы и вредоносное ПО	Недостаточная защита рабочих станций и серверов приводит к высоким рискам внедрения вредоносного ПО

Представленные в таблице 1 угрозы указывают на необходимость разработки дополнительных мер по защите данных и повышения уровня осведомленности сотрудников о возможных киберугрозах.

Для защиты данных от внешних и внутренних угроз ООО «Х» принято решение о внедрении современных технических средств, а именно:

1) шифрования данных: вся конфиденциальная информация, включая персональные данные клиентов и внутреннюю документацию, будет зашифрована с использованием современных алгоритмов;

2) многофакторной аутентификации: вводится обязательная многофакторная аутентификация для доступа к корпоративной сети и критическим системам;

3) системы обнаружения вторжений (IDS): интегрируется система, которая будет отслеживать подозрительную активность в сети и уведомлять администраторов о потенциальных атаках;

4) антивирусного программного обеспечения и фаерволлов: обновляются и усиливаются меры защиты рабочих станций и серверов, включая установку современных антивирусных программ и настройку фаерволлов.

Чтобы сотрудники могли эффективно работать в условиях повышенной информационной безопасности, было принято решение о проведении регулярного обучения и повышение квалификации.

После внедрения предложенного комплекса мер по защите данных ООО «Х» и обучению сотрудников произошло значительное снижение факторов нарушения информационной безопасностью, что помогло предотвратить большинство кибератак и утечек данных.

Список литературы

1. Распоряжение Правительства РФ «О цифровой экономике Российской Федерации» от 28.07.2017 №1632-р [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 25.03.2025).

2. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента Российской Федерации от 5 декабря 2016 г. №646 [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 25.03.2025).

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ (ред. от 31 июля 2023 г.) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/12148555/ (дата обращения: 25.03.2025).

4. Актуальные киберугрозы: итоги года (2018–2022 гг.): аналитический ежегодный отчет агентства информационной безопасности Positive Research [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape2021/ (дата обращения: 25.03.2025).

5. Основные типы компьютерных атак в кредитно-финансовой сфере: отчет ФинЦЕРТа Банка России [Электронный ресурс]. – Режим доступа: https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 25.03.2025).

6. Балаклеец Н.А. Пространственный аспект современных войн: от традиционной войны к кибервойне / Н.А. Балаклеец // Социодинамика. – 2021. – №4. – С. 136–148 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/prostranstvennyy-aspekt-sovremennyh-voyn-ot-traditsionnoy-voyny-k-kibervoyne (дата обращения: 25.03.2025). DOI 10.25136/2409-7144.2021.4.32652. EDN TZZKLG

7. Утарбеков Ш.Г. Основные угрозы информационной безопасности / Ш.Г. Утарбеков // Вестник Челябинского государственного университета. Серия: Право. – 2021. – Т. 6. Вып. 4. – С. 49–51 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/osnovnye-ugrozy-informatsionnoy-bezopasnosti (дата обращения: 25.03.2025). DOI 10.47475/2618-8236-2021-16409. EDN ERLSXR

8. Шкодинский С.В. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике / С.В. Шкодинский, М.Н. Дудин, Д.И. Усманов // Финансовый журнал. – 2021. – Т. 13. №3. – С. 38–53 [Электронный ресурс]. – Режим доступа: https://doi.org/10.31107/2075-1990-2021-3-38-53 (дата обращения: 25.03.2025). EDN MHVBTK

9. Александров В.В. Подход к разработке системы выявления инцидентов информационной безопасности информационных ресурсов банковских систем при реализации этапов противодействия противоправным действиям / В.В. Александров, Ю.В. Малий, Ю.В. Александрова // Экономика. Информатика. – 2021. – Т. 48. №1. – С. 116–122 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/podhod-k-razrabotke-sistemy-vyyavleniya-intsidentov-informatsionnoy-bezopasnosti-informatsionnyh-resursov-bankovskih-sistem-pri (дата обращения: 25.03.2025). DOI 10.52575/2687-0932-2021-48-1-116-122. EDN PWSSMJ

10. Барков А.В. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур / А.В. Барков, А.С. Киселев // Банковское право. – 2022. – №4. – С. 20–27 [Электронный ресурс]. – Режим доступа: http://elib.fa.ru/art2022/bv1270.pdf (дата обращения: 25.03.2025). DOI 10.18572/1812-3945-2022-4-20-27. EDN YQADIO

11. Levinson P. Micro-cyberwar vs. macro-cyberwar: towards the beginning of a taxonomy / P. Levinson // Digital War. – 2020. – Vol. 1. No. 1-3. – P. 171–172. DOI 10.1057/s42984-020-00020-z. EDN SMEUKI