МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ им. А. И. ГЕРЦЕНА»

**ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И
ТЕХНОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ**
Кафедра информационных технологий и электронного обучения

Основная профессиональная образовательная программа
Направление подготовки 09.03.01 Информатика и вычислительная техника
Направленность (профиль) «Технологии разработки программного обеспечения»
форма обучения – очная

Аналитический отчёт

«Анализ проблематики безопасности ИТ (System security and privacy)»

Обучающегося 4 курса
Пальчука Германа Андреевича

Научный руководитель:
кандидат физико-математических наук,
доцент кафедры ИТиЭО
Власов Дмитрий Викторович

Санкт-Петербург
2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современных условиях объёмы цифровой информации растут экспоненциально, и в основном это – личные данные пользователей [1]. Цифровизация повышает эффективность бизнеса, но одновременно резко расширяет поверхность кибератак [2]. Информационная безопасность (ИБ) базируется на трёх основных принципах – конфиденциальности, целостности и доступности информации [3]. Сегодня ИБ уже не сводится к защите периметра: как отмечают эксперты, «информационная безопасность – это не просто защита данных и периметра, а комплексное направление, требующее интеграции с бизнес-процессами» и активного участия в стратегии компании [4]. При этом понятия «конфиденциальность» (запрет на разглашение информации) и «приватность» (право неприкосновенности личной жизни и контроля над персональными данными) дополняют друг друга, причём, по замечанию Лаборатории Касперского, в Интернете «приватность и безопасность всегда идут бок о бок» [1].

СОВРЕМЕННЫЕ УГРОЗЫ И ВЫЗОВЫ ИТ-БЕЗОПАСНОСТИ

Анализ литературы показывает, что угрозы исходят не только извне, но и изнутри организации [5]. По данным практиков, до 60 % инцидентов ИБ связаны с внутренними факторами – ошибками или действиями сотрудников [5], тогда как целевые внешние атак отличаются особой сложностью и ущербом. Эксперты отмечают, что свыше 70 % критических атак в 2025 году были направлены на физическое уничтожение инфраструктуры компаний [6]. Преступники всё чаще применяют новые техники и сотрудничают между собой [6]. По статистике операторов, более 50 % кибератак приводят к утечке конфиденциальной информации, а около 40 % – к нарушению работы предприятий и простою [7]. Основными причинами взломов остаются фишинг, уязвимости в веб-приложениях и отсутствие многофакторной аутентификации [6]. Анализ показывает, что 83 % компаний имеют открытые административные интерфейсы, а 19 % используют пароль по умолчанию [6], что делает их уязвимыми к банальным атакам. При этом человеческий фактор остаётся наиболее распространённым источником инцидентов – до 90 % случаев связаны с действиями персонала [6][5].

Основные типы современных угроз можно свести к следующим категориям:

1) **Вредоносное ПО (malware):** программы-вымогатели, троянские вирусы, криптоджекинг (онлайн-угроза, которая прячется на компьютере или мобильном устройстве и использует ресурсы машины для «майнинга» различных видов онлайн-валют, известных как криптовалюты) и др. По оценкам, это самая частая угроза с высоким потенциалом ущерба [5]. Шифровальщики составляют до четверти новых образцов вредоносного ПО, а требования выкупа достигают сотен тысяч долларов [5].
2) **Социальная инженерия:** фишинг, BEC-атаки, поддельные сайты и приложения. Эти приёмы имеют среднюю частоту, но также наносят серьёзный ущерб – злоумышленник выманивает от сотрудника пароли и данные через психологические приёмы [5][6].
3) **Утечки данных и инсайдерские угрозы:** включают несанкционированное копирование, передачу или раскрытие конфиденциальной информации. Инциденты с утечками наносят компании долгосрочные убытки и ущерб репутации [7][5]. Ошибки в настройках облачных сервисов являются частой причиной утечек [5].
4) **DDoS-атаки:** направлены на блокировку доступности сервисов (низкая частота, средний ущерб) [5]. Несмотря на относительную редкость, они выводят из строя сайт или инфраструктуру, вызывая простои.
5) **APT-атаки:** целевые многоэтапные кампании с использованием сложных методов. Это редкая, но «очень высокая» угроза [5]. Примерами служат атаки на критическую инфраструктуру, промышленность и госучреждения с целью саботажа или промышленного шпионажа.

Таким образом, современные киберугрозы эволюционируют в сторону более избирательных, «нацеленных» атак, часто с ростом использования ИИ [2][6]. Крупные инциденты показывают стратегический уровень риска: например, атаки на компании Marks & Spencer и Asahi в 2025 году привели к потерям, сравнимым с ощутимой долей годового оборота [8]. Это доказывает, что кибер-риски уже напрямую угрожают бизнес-целостности и требуют интегрированной защиты.

КОНФИДЕЦИАЛЬНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Важной составляющей ИБ является защита конфиденциальности и личных данных. Конфиденциальность информации определяется как принцип и практика защиты данных от

несанкционированного доступа и разглашения [3]. В ряде стран кибербезопасность и приватность трактуются по-разному: конфиденциальность фокусируется на запрете передачи данных третьим лицам, тогда как приватность – на правах субъекта контролировать доступ к своим личным сведениям. Законодательство обязывает организации технически и организационно защищать персональные данные: так, согласно Федеральному закону № 152-ФЗ «О персональных данных», оператор обязан принимать необходимые правовые, организационные и технические меры для защиты данных от неправомерного доступа, уничтожения, изменения и других угроз [9]. Ключевые шаги включают определение потенциальных угроз, применение средств криптографической защиты и шифрования, регулярный аудит и мониторинг информационных систем. Нарушение этих норм грозит штрафами и судебными исками: например, утечка персональных данных влечёт за собой реакции регуляторов и возмещение ущерба.

Сегодня защита персональных данных неизбежно пересекается с технологическими вызовами: распространение облачных сервисов, Big Data, мобильных устройств и интернета вещей создаёт новые «поверхности» для сбора и утечек данных. Поэтому внедряются стандарты Privacy by Design – принципа, при котором конфиденциальность учитывается на всех этапах разработки систем. Многие организации стремятся к соответствию международным стандартам (например, ISO 27001 с расширением ISO 27701 по приватности) и отраслевым требованиям ФСТЭК, ФСБ, регуляторов и саморегулируемых ассоциаций. Как подчёркивают эксперты, соблюдение нормативных требований (ФЗ-152, закон о КИИ, правила работы с биометрией, цифровым рублём, приказ ФСТЭК № 117 и др.) становится основой эффективной системы защиты [2][9]. При этом регулирующие органы отмечают, что эти требования представляют собой «необходимый минимум», который необходимо дополнить реальными мерами защиты на предприятии [2].

ТЕХНОЛОГИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ

Для противодействия указанным угрозам применяются многоуровневые меры защиты. Анализ показывает, что эффективная система включает технические решения в сочетании с политиками и обучением персонала.

Основные направления защиты можно обобщить так:

1) **Оценка рисков и архитектура защиты.** Защита должна начинаться с анализа рисков и построения системы безопасности, адаптированной под бизнес-процессы организации [5]. Это включает категоризацию информации, ограничение прав доступа и настройку безопасности с учётом реальных угроз.

2) **Обучение сотрудников и повышение осведомлённости.** Регулярные тренинги и моделирование атак снижают роль человеческого фактора. Исследования показывают, что компании, регулярно обучающие персонал ИБ, в шесть раз реже становятся жертвами фишинга [2]. Формирование «киберкультуры» и практические занятия (а не одноразовые курсы) повышают эффективность защиты на уровне каждого сотрудника [2][6].

3) **Технические средства защиты.** Внедряются антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), DLP-системы и SIEM-платформы для мониторинга событий безопасности. Важны регулярное обновление ПО и патч-менеджмент. Для борьбы с вредоносными программами комбинируют сигнатурный анализ и поведенческий анализ, что помогает выявлять и новые угрозы [5].

4) **Двухфакторная аутентификация (2FA).** Использование MFA сильно повышает безопасность учётных записей. Даже если злоумышленник получает пароль, второй фактор (SMS-код, токен, биометрия) не позволит войти в систему [5][6].

5) **Шифрование и резервное копирование.** Конфиденциальная информация и резервные копии должны храниться в зашифрованном виде, что защищает их при утечках или физической краже устройств. При атаках шифровальщиков (ransomware) наличие копий данных позволяет быстро восстановить работу с минимальными убытками.

6) **Соответствие нормативам и реагирование.** Установление внутриорганизационных политик ИБ, регламентация инцидентов и плана реагирования на них (Incident Response). Строгое исполнение требований закона (например, ФЗ-152 обрабатывающих персональные данные систем) и отраслевых стандартов обеспечивает «правовую гигиену» в области безопасности [9].

7) **Финансовая ответственность поставщиков ИБ.** Новым трендом становится предоставление гарантий и страховых полисов от вендоров. Крупные производители уже предлагают клиентам покрытие убытков до 1–3 млн $, если их решения не предотвратят атаку [8]. Аналогичные предложения появляются и на российском рынке: большие интеграторы, операторы и банки готовы компенсировать потери клиентов при сбоях

своих сервисов [8]. Это стимулирует более строгое отношение к качеству и тестированию средств защиты, а также требует тщательного включения гарантий в договоры.

В сочетании эти меры позволяют существенно снизить риски ИБ. Однако важно помнить, что защиты должны быть встроены в ежедневные процессы компании – от блокировки экрана до проверки получателей перед отправкой конфиденциальных файлов. Только комплексный подход, объединяющий технологии, процессы и людей, обеспечивает действительно высокую стойкость к современным угрозам [2][5].

ЗАКЛЮЧЕНИЕ

Проведённый анализ показал, что проблематика информационной безопасности и конфиденциальности остаётся крайне актуальной и многогранной. С одной стороны, усложнение цифровых технологий и растущий объём персональных данных создают новые уязвимости. С другой – динамика угроз диктует необходимость комплексных ответов: от современных ИТ-решений (автоматизация, машинное обучение, SASE, Zero Trust и др.) до усиленного правового контроля и подготовки персонала [4][2]. Законодательство (ФЗ-152, закон о КИИ и др.) формирует обязательный минимум требований безопасности [2][9], но практика показывает, что риск-ориентированный подход (адекватная оценка рисков и их устранение) является залогом надёжной защиты. В конечном счёте, безопасность ИТ-систем и защита приватности становятся ключевыми факторами устойчивости и доверия – как для бизнеса, так и для общества в целом.

ЛИТЕРАТУРА

1. Что такое приватность данных?. — Текст : электронный // kaspersky : [сайт]. — URL: https://www.kaspersky.ru/resource-center/threats/internet-and-individual-privacy-protection (дата обращения: 24.12.2025).
2. Топ кибервызовов 2025–2026: главные тренды в ИБ от «Лаборатории Касперского». — Текст : электронный // Ведомости.Технологии : [сайт]. — URL: https://www.vedomosti.ru/technologies/special/2025/12/24/top-kibervizovov-20252026-glavnie-trendi-v-ib-ot-laboratorii-kasperskogo-erid-2VfnxxvgiQ1 (дата обращения: 24.12.2025).
3. Что такое конфиденциальность информации. — Текст : электронный // Гладиаторы ИБ : [сайт]. — URL: https://glabit.ru/blog/chto-takoe-konfidencialnost-informacii (дата обращения: 24.12.2025).
4. Ключевые тренды в сфере информационной безопасности (ИБ) на ближайшие годы: что изменится?. — Текст : электронный // MONS : [сайт]. — URL: https://mons.ru/klyuchevye-trendy-v-sfere-informacionnoj-bezopasnosti (дата обращения: 24.12.2025).
5. Какие угрозы информационной безопасности наиболее опасны в 2025 году и как бизнесу защититься от утечек, атак и сбоев. — Текст : электронный // KT Team : [сайт]. — URL: https://www.kt-team.ru/blog/cybersecurity-threats-2025 (дата обращения: 24.12.2025).
6. Эксперты заявили о смене фокуса хакеров на уничтожение инфраструктуры компаний. — Текст : электронный // Forbes : [сайт]. — URL: https://www.forbes.ru/tekhnologii/552750-eksperty-zaavili-o-smene-fokusa-hakerov-na-unictozenie-infrastruktury-kompanij (дата обращения: 24.12.2025).
7. Актуальные угрозы информационной безопасности. — Текст : электронный // GARTEL : [сайт]. — URL: https://www.gartel.ru/articles/aktualnye-ugrozy-informatsionnoy-bezopasnosti/ (дата обращения: 25.12.2025).
8. Кибербезопасность 2025-2026. Год в кибершторме — настанет ли затишье?. — Текст : электронный // Хабр : [сайт]. — URL: https://habr.com/ru/companies/pt/articles/975040/ (дата обращения: 24.12.2025).
9. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) "О персональных данных". — Текст : электронный // КонсультантПлюс : [сайт]. — URL:

https://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/ (дата обращения: 24.12.2025).

10. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 4-е изд., стер. — Москва : ФЛИНТА, 2022. — 184 с. — ISBN 978-5-9765-1904-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/232457 (дата обращения: 24.12.2025). — Режим доступа: для авториз. пользователей.

11. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130 (дата обращения: 24.12.2025). — Режим доступа: для авториз. пользователей.

12. Бирюков, А. А. Информационная безопасность: защита и нападение : руководство / А. А. Бирюков. — 3-е изд. — Москва : ДМК Пресс, 2023. — 440 с. — ISBN 978-5-93700-219-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/455351 (дата обращения: 24.12.2025). — Режим доступа: для авториз. пользователей.

13. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ / А. С. Кечеджиев, A. S. Kechedzhiev, О. Л. Цветкова, O. L. Tsvetkova // Молодой исследователь Дона. — 2023. — № 2 (41). — С. 23-27. — ISSN 2500-1779. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/354917 (дата обращения: 26.12.2025). — Режим доступа: для авториз. пользователей.

14. Ванина, А. Г. Гуманитарные проблемы обеспечения информационной безопасности : курс лекций : учебное пособие / А. Г. Ванина, Т. В. Минкина. — Ставрополь : СКФУ, 2021. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/386570 (дата обращения: 26.12.2025). — Режим доступа: для авториз. пользователей.

15. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности / Н. Ш. Козлова, N. S. Kozlova, В. А. Довгаль, V. A. Dovgal // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2023. — № 3 (326). — С. 65-72. — ISSN 2410-3225. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/journal/issue/347516 (дата обращения: 26.12.2025). — Режим доступа: для авториз. пользователей.