Котенев Павел Павлович
ФГБОУ “Нижневартовский государственный университет”
Пшеничников Алексей Антонович
ФГБОУ “Нижневартовский государственный университет”
Бармин Александр Юрьевич
ФГБОУ “Нижневартовский государственный университет”
Фатеев Кирилл Алексеевич
ФГБОУ “Нижневартовский государственный университет”
kotenevp35@mail.ru

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ. ЗАЩИТА ЛИЧНЫХ ДАННЫХ В ИНТЕРНЕТЕ

Аннотация. В статье рассматриваются современные подходы к защите личных данных в условиях, цифровизации и роста киберугроз. Проведен анализ правовых, организационных и технических мер кибербезопасности, включая шифрование, многофакторную аутентификацию, системы обнаружения и предотвращения вторжений, а также обучение пользователей. Особое внимание уделено международным и российским нормативным актам (GDPR, ФЗ №152-ФЗ) и их влиянию на практику защиты данных. Представлено сравнение эффективности различных методов по критериям уровня защиты, производительности и затрат. Сделан вывод о необходимости комплексного подхода, сочетающего технологические решения и организационные меры, а также о важности адаптации стратегий безопасности к изменяющимся угрозам и специфике деятельности организации.

Ключевые слова: Кибербезопасность, Защита личных данных, Шифрование, Многофакторная аутентификация, GDPR, ФЗ №152-ФЗ, Киберугрозы, IDS/IPS, Информационная безопасность, Цифровизация.

Практические методики и алгоритмы защиты

В условиях стремительного роста количества угроз в интернете, разработка алгоритмов защиты личных данных становится важной задачей для организаций. Существует множество методов для защиты, и в данной части работы рассматривается несколько наиболее эффективных методов.

Шифрование – это самый важный метод защиты данных. Оно значительно повышает безопасность, так как превращает читаемую информацию в нечитаемую. В основном используют симметричное шифрование. Это когда один ключ используется для шифрования и дешифрования. Самые популярные примеры шифрования это AES и RSA, которые применяются при защите онлайн платежей.

Также существует аутентификация. Аутентификация – это подтверждение личности, например паролем или биометрическим способом [3].

Самые популярные методы защиты от вторжений это IDS (метод обнаружения вторжений) и IPS (метод предотвращения вторжений). Они позволяют идентифицировать и предотвращать угрозы в реальном времени.

Для организаций также важно осуществлять регулярное обновление программного обеспечения, так как устаревшие версии программ могут содержать уязвимости, которыми злоумышленники могут пользоваться для доступа к информации.

Также важным фактором защиты является обучение сотрудников организации. Множество утечек информации происходит из-за ошибок сотрудников, которые не знают ничего о кибербезопасности. Поэтому

обучение сотрудников значительно снизят риски утечек информации.

Эффективная защита персональных данных в интернете требует комплексного подхода, то есть необходимо интегрировать все средства защиты информации в одну систему, для повышения уровня безопасности [5].

Нормативные акты кибербезопасности

GDPR - нормативный акт, устанавливающий строгие требования к обработке персональных данных. Вступил в силу в 2018 году [6]. Основная цель GDPR - обеспечение прозрачности обработки данных и защита персональных данных.

Ключевой принцип регламента это документальное подтверждение соблюдения установленных правил. Организации обязаны вести реестры обработки данных и внедрять методы защиты данных в разработку продуктов [7].

GDPR предоставил пользователям новые возможности контроля над своими данными. Пользователи получили право запрашивать информацию об обработке своих данных, требовать их исправления или полного удаления. Данные возможности создали дополнительные обязательства для организаций, обрабатывающих персональные данные.

Также важной частью регламента являются требования к безопасности данных и обязанность по уведомлению о нарушениях. Компании обязаны сообщать об утечках персональных данных в надзорные органы в течении 72 часов с момента происшествия. Примером серьезных последствий нарушений может послужить штраф компании “Meta” в 2023

году. За утечку персональных данных им пришлось выплатить штраф в размере 1.3 миллиарда долларов.

Регламент установил строгие правила по международной передачи персональных данных. Передача данных за пределы ЕС разрешена только при условии обеспечения серьезного уровня защиты.

Федеральный закон №152-ФЗ “О персональных данных” - это основной нормативный акт, регулирующий обработку персональных данных в Российской Федерации. Принят в 2006 году. Устанавливает требования к операторам, среди которых необходимость получения согласия пользователя на обработку его данных, а также обеспечение конфиденциальности [8]. Закон также предусматривает обязательную локализацию баз данных граждан на территории РФ [9].

ФЗ-152, в отличие от GDPR, не предусматривает право на переносимость данных, но дает пользователям ряд прав, включая право на доступ к своим персональным данным и содержит более детализированные требования к мерам защиты информации [10].

В законе также предусмотрена административная и уголовная ответственность за несоблюдение требований по защите персональной информации.

При сравнении GDPR и ФЗ-152 стоит отметить, что российский закон больше направлен на защиту государственных интересов, а GDPR направлен на права физических лиц в целом.

Анализ и сравнение эффективности различных методов защиты

Для кибербезопасности ключевыми являются анализ и сравнение эффективности методов защиты личных данных. В условиях новых угроз важно не только разработать надежные методы, но и оценить их действенность по заранее установленным критериям. Критериями же в таком случае являются уровень защиты, скорость обработки, затраты на внедрение и эксплуатацию, а также, что немаловажно, простота использования.

Один из главных критериев оценки методов защиты — это уровень защиты. Он определяется способностью системы предотвращать или минимизировать последствия кибератак. Для тестирования этого показателя проводятся сравнительные испытания, где результаты применения различных методов фиксируются в условиях реальных угроз. Например, в одном исследовании, проведенном в 2022 году, были протестированы системы шифрования AES и RSA, а также многофакторная аутентификация. Результаты показали, что системы, использующие многофакторную аутентификацию, значительно более устойчивы к попыткам несанкционированного доступа, по сравнению с обычными паролями. Соответственно и случаи успешного взлома в таких системах были сведены к минимуму [1].

Разумеется уровень защиты не самый главный критерий. Немаловажным аспектом является скорость обработки данных и влияние методов защиты на производительность системы. Например, если шифрование замедляет передачу данных, это может быть критично для сервисов с высокой нагрузкой, таких как онлайн-банкинг или облачные сервисы. Исследования привели к выводу, что использование алгоритмов, таких как AES, обеспечивает не только высокий уровень защиты, но и

требует значительно меньше ресурсов системы по сравнению с другими методами, такими как Blowfish или DES. Таким образом, можно с уверенностью сказать, что нельзя проводить оценку эффективности метода защиты без особого внимания на обеспечение необходимой скорости работы сервисов. В условиях высокой конкуренции на рынке это утверждение принимает особо большое значение [2].

Конечно же нельзя забывать и о затратах на внедрение и эксплуатацию технологий, таких как многофакторная аутентификация. Подобные решения могут быть невыполнимыми для малых и средних предприятий. Однако качественная защита, на долгое время ограждающая компанию от финансовых потерь из-за утечек данных и кибератак, полностью оправдывает затраты. Достаточно простой интерфейс использования, также снижает риск применения слабо защищенных паролей, что несомненно делает его важным. Как итог анализа подтверждается необходимость комплексного подхода к выбору стратегий безопасности. В том числе включая грамотное управление и мониторинг методов защиты. Это требует как организационного, так и технологического подхода для своевременного приспособления к постоянным изменениям в сфере защиты от киберугроз. Системный подход к оценке эффективности методов защиты данных снижает риски кибератак и утечек до минимума.

Заключение

В ходе проведенного исследования были изучены современные проблемы защиты личных данных в интернете на основе этих данных, были получены выводы, что ситуация становится все сложнее с каждым годом. На практике видно, как компании сталкиваются с новыми видами

мошенничества и утечек, при этом многие до сих пор недооценивают риски. Была выделена главная проблема, она заключается в том, что в современном обществе защита информации перестала быть сугубо технической задачей - теперь это комплексный вызов, требующий пересмотра всей бизнес-стратегии [4].

Из полученного опыта работы с различными организациями можно выделить ключевые моменты. Первым является то, что технологии важны, но они не работают без грамотного процесса и надлежащего персонала.

Сколько раз были зафиксированы случаи. когда дорогая система защиты показывала свою неэффективность из-за банальной халатность или пренебрежения основами безопасности. Вторым выступает отсутствие универсального решения то, что идеально подходит крупному банку, может быть избыточным для небольшого интернет-магазина. Третье, защита данных не может быть разовым решением, это процесс постоянной адаптации к растущим и меняющимся угрозам.

На данный момент часто совершается ошибка когда компания тратит огромный бюджет на “модные” решения, забывая при этом про базовые вещи вроде контроля доступа или регулярного процесса обновления ПО. Рекомендуется всегда начинать с аудита реальных рисков, а только потом выбирать инструменты. Необходимость обучать сотрудников. Простой пример: внедрение двухфакторной аутентификации снижает риски взлома на 80%, однако такая система будет работать только если сотрудники понимают, зачем это нужно и как правильно эксплуатировать.

Подводя итог, защита персональных данных сегодня это вопрос не просто соблюдения законодательства государства, но и сохранение репутации бизнеса. Рост внимания клиентов к цифровой безопасности

повышает риски для бизнеса. Серьезная утечка данных способна нанести непоправимый ущерб репутации компании, которую выстраивали годами. В этих условиях грамотная и системная защита информации перестанет быть дополнительной опцией. Она становится обязательным требование для выживания и конкурентоспособности любого предприятия на современном рынке.

Список литературы

1. Э. Халтен. Кибербезопасность с момента «рождения» цифровой информации. DOI 10.22184/1992-4178.2019.182.1.18.20 // ELECTRONICS Science Technology Business. 04.02.2019 URL: http://www.electronics.ru/journal/article/7206 (дата обращения: 09.08.2025).
2. Андрей В. Манойло. Текущие стратегии кибербезопасности и киберзащиты НАТО. DOI 10.31249/ape/2020.03.08 // Urgent Problems of Europe. 01.01.2020 URL: https://upe-journal.ru/article.php?id=312 (дата обращения: 09.08.2025).
3. Юрий Воронин, Анна Дмитриева, Татьяна Кухтина. ВЗАИМОДЕЙСТВИЕ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ И ЦИФРОВОЙ БЕЗОПАСНОСТИ: СТРАНОВОЙ АНАЛИЗ. DOI 10.14529/law220302 // Bulletin of the South Ural State University series Law. 01.01.2022 URL: https://vestnik.susu.ru/law/article/view/12404 (дата обращения: 09.08.2025).
4. М.С. Кобышева, Андрей Володин, Методий Иванов, Татьяна Феофилова, Т.М. Манасерян. Риски и угрозы экономической безопасности России в условиях цифровой трансформации. DOI 10.17513/vaael.1597 // Bulletin of the Altai Academy of Economics and law. 01.01.2021 URL: https://vaael.ru/article/view?id=1597 (дата обращения: 09.08.2025).

5. Тигран Л. Оганесян. Право на защиту персональных данных: исторический аспект и современная концептуализация в эпоху больших данных. DOI 10.12737/jflcl.2020.010 // Journal of Foreign Legislation and Comparative Law. 29.05.2020 URL: https://jzsp.ru/articles/article-2988.pdf (дата обращения: 09.08.2025).

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) // Official Journal of the European Union. 2016. L 119. P. 1-88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 09.08.2025).

7. European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3): Version 2.0: Adopted 12 November 2019. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en (дата обращения: 09.08.2025).

8. Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных" (ред. от 24.02.2021). Ст. 6, 9 // Собрание законодательства РФ. 2006. №31 (1 ч.). Ст. 3451.

9. Приказ Роскомнадзора от 05.09.2013 №996 "Об утверждении требований и методов по обезличиванию персональных данных" // Российская газета. 2013. №228.

10. Постановление Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // Собрание законодательства РФ. 2012. №45. Ст. 6257.