DOI 10.37882/2223-2966.2025.02.13

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ СОТРУДНИКОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

CYBERSECURITY AND EMPLOYEE DATA PROTECTION IN THE CONTEXT OF DIGITALIZATION

O. Ivanchina

Summary. In conditions of economic instability and political tension, modern Russian enterprises pay special attention to safety. Cybersecurity is becoming especially important due to the active digitalization in the Russian economy, which increases the risk of cyber-attacks and data leakage. Statistics show an increase in the number of cyber-attacks in Russia annually over the past 5 years [1]. The article discusses approaches to defining the concept of «cybersecurity» according to the points of view of various authors, the dynamics of the number of cyber-attacks in Russia over the past five years, which tends to increase. The types of cyber threats for a modern enterprise are also systematized: malicious software, phishing, denial of service attacks, vulnerability attacks, internal threats, data theft, extortionate software, supply chain attacks, social engineering. Possible protection and prevention measures are presented for each of them. An important part of cybersecurity is training employees in the basics of data security. The author concludes that modern information systems are becoming more complex and integrated, which creates new vulnerabilities and requires more advanced protection measures.

Keywords: security, cybersecurity, data protection, digitalization, cyberattack, cybersecurity measures.

Иванчина Ольга Викторовна
кандидат экономических наук, доцент, Приволжский государственный университет путей сообщения
ivanchina_o@mail.ru

Аннотация. В условиях экономической нестабильности и политической напряженности на современных российских предприятиях особое внимание уделяют безопасности. Кибербезопасность становится особенно важной из-за активной цифровизации в экономике России, увеличивающей риск кибератак и утечки данных. Статистика свидетельствует о росте количества кибератак в России ежегодно за последние 5 лет [1]. В статье рассмотрены подходы к определению понятия «кибербезопасность» по точкам зрения различных авторов, динамика количества кибератак в России за последние пять лет, которая имеет тенденцию к росту. Также систематизированы виды киберугроз для современного предприятия: вредоносное программное обеспечение, фишинг, атаки типа «отказ в обслуживании», атаки с использованием уязвимостей, внутренние угрозы, кража данных, вымогательское программное обеспечение, атаки на цепочку поставок, социальная инженерия. По каждому из них представлены возможные меры по защите, а также профилактике. Важной частью кибербезопасности является обучение сотрудников основам безопасности данных. Автор приходит к выводу, что современные информационные системы становятся все более сложными и интегрированными, что создает новые уязвимости и требует более продвинутых мер защиты.

Ключевые слова: безопасность, кибербезопасность, защита данных, цифровизация, кибератака, меры обеспечения кибербезопасности.

Введение

С развитием технологий и увеличением количества данных, обрабатываемых и хранящихся в цифровом формате, растет и число кибератак. Компании становятся мишенями для хакеров, что делает важным наличие эффективных мер защиты. Кибератаки могут привести к значительным финансовым потерям как из-за прямых убытков (например, кража денег), так и из-за косвенных (например, потеря клиентов, снижение доверия инвесторов). Утечки данных и успешные кибератаки могут нанести серьезный ущерб репутации компании, что в долгосрочной перспективе может оказаться еще более разрушительным, чем финансовые потери. Поэтому исследование основ кибербезопасности помогает компаниям не только защитить свои активы и данные, но и обеспечить долгосрочную устойчивость бизнеса в условиях растущих киберугроз.

Материалы и методы исследования

Исследование основано на научных статьях российских и иностранных авторов, аналитических исследованиях экспертов компании РБК и Positive Technologies. К методам исследования относятся сравнение, сопоставление, аналогия, графический и табличный метод исследования.

Результаты и обсуждения

В условиях цифровизации кибербезопасность и защита данных сотрудников становятся критически важными аспектами управления персоналом. Обзор источников показал, что нет общепринятого определения кибербезопасности. Можно выделить три подхода к трактовке данного понятия в источниках, в том числе в зарубежном стандарте (рис. 1).

Следовательно, кибербезопасность является частью информационной безопасности и направлена на защиту систем, подключенных к Интернету, от кибератак. Она обеспечивает защиту сетей от несанкционированного доступа. По сути, кибербезопасность стремится к созданию состояния, в котором информационные системы

Рис. 1. Подходы к определению понятия «кибербезопасность»

Источник: составлено автором поданным [3, 5, 6, 8, 10]

защищены от угроз. Главная цель этих мер — защитить информацию, предотвращая или снижая риски кибератак, утечек и повреждений данных.

Киберугрозы для предприятий могут быть разнообразными, их систематизация представлена в таблице 1.

Представленное разнообразие киберугроз требует от предприятий разработки и внедрения комплексных стратегий по кибербезопасности для защиты своих данных и инфраструктуры.

Статистика свидетельствует о росте количества кибератак в России ежегодно за последние 5 лет (рис. 2).

Повышение риска киберпреступности и утечки данных обусловлено тем, что активно внедряемые в последнее время цифровые системы хранят большое количество личных данных сотрудников, включая номера социального страхования, банковские реквизиты и контактную информацию. Защита этой информации от утечек и несанкционированного доступа крайне важна для сохранения доверия сотрудников и соблюдения законодательных требований. С ростом цифровизации увеличивается и число кибератак. Компании должны внедрять надежные системы защиты, такие как антивирусное программное обеспечение, брандмауэры и системы обнаружения вторжений, чтобы предотвратить потенциальные угрозы [1, 2]. В таблице 2 представлены меры по защите от разных видов кибератак.

Важной частью кибербезопасности является обучение сотрудников основам безопасности данных. Это включает в себя информирование о фишинговых атаках, обучении созданию сложных паролей и безопасному использованию корпоративных систем. При этом постоянный мониторинг и регулярное обновление программного обеспечения и систем безопасности необходимы для

Таблица 1.

Виды киберугроз для предприятия

Вид угрозы	Характеристика
Вредоносное ПО	Программы, которые могут повредить системы, украсть данные или дать злоумышленникам доступ к сети
Фишинг	Мошеннические попытки получить конфиденциальную информацию, такие как пароли или данные кредитных карт, через поддельные электронные письма или сайты
Атаки типа «отказ в обслуживании» (DDoS)	Перегрузка серверов предприятия большим количеством запросов, что приводит к недоступности услуг
Атаки с использованием уязвимостей	Эксплуатация известных или неизвестных слабых мест в программном обеспечении для доступа к системам
Внутренние угрозы	Недобросовестные или неосторожные действия сотрудников, которые могут привести к утечке информации или другим проблемам
Кража данных	Незаконное получение конфиденциальной информации, такой как данные клиентов или интеллектуальная собственность
Вымогательское ПО	Блокировка доступа к данным или системам с требованием выкупа за восстановление доступа
Атаки на цепочку поставок	Внедрение вредоносного ПО или выполнение атак через уязвимости в программном обеспечении поставщиков
Социальная инженерия	Манипуляция людьми для получения конфиденциальной информации или доступа к системам

Источник: составлено автором по данным [1, 2, 6, 9]

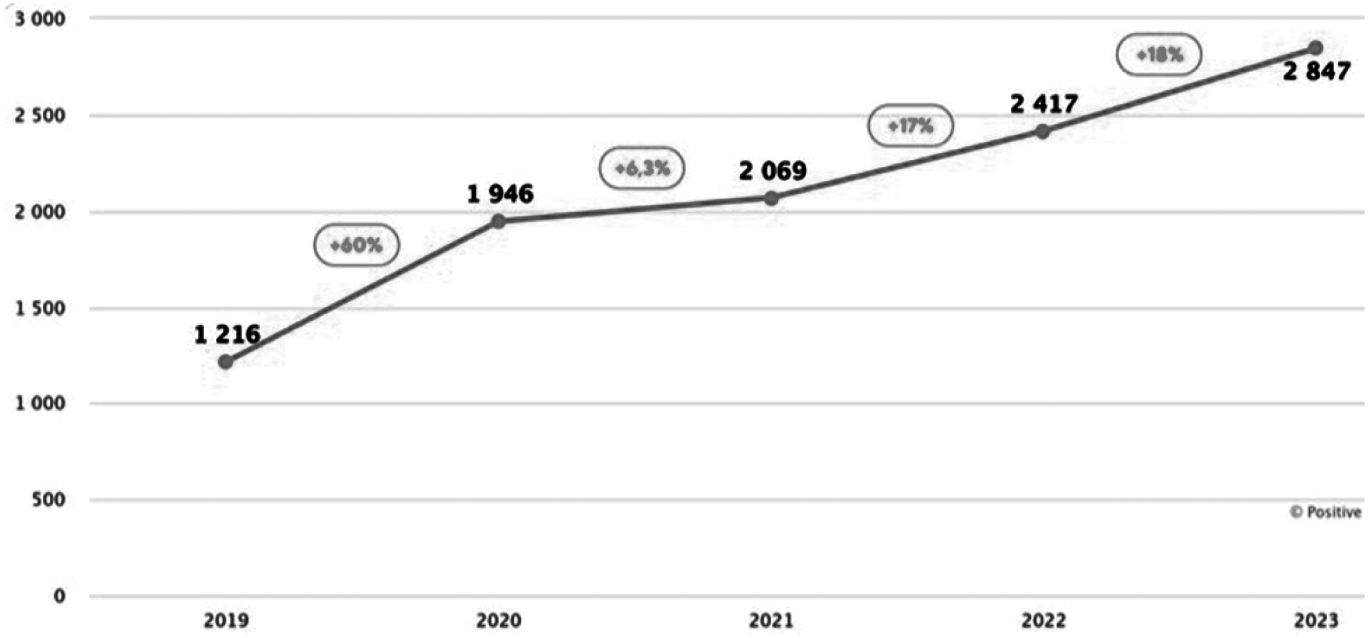

Рис. 2. Динамика количества успешных кибератак на организации в России в 2019–2023 гг.

Источник: [1]

Таблица 2.

Меры по защите от разных видов кибератак

Вид угрозы	Меры по защите
Вредоносное ПО	Использование антивирусного и антишпионского программного обеспечения. Регулярное обновление программного обеспечения и операционной системы. Ограничение прав доступа пользователей к установке программ.
Фишинг	Проведение обучения сотрудников по распознаванию фишинговых атак. Внедрение фильтров спама и фишинга в электронной почте. Использование двухфакторной аутентификации для доступа к системам.
Атаки типа «отказ в обслуживании» (DDoS)	Использование сетевых фильтров и систем предотвращения DDoS-атак. Регулярное обновление и тестирование систем защиты. Сотрудничество с интернет-провайдерами для фильтрации трафика
Атаки с использованием уязвимостей	Регулярное проведение аудитов безопасности и тестирования на проникновение. Патчинг и обновление уязвимых программных компонентов. Внедрение системы управления уязвимостями.
Внутренние угрозы	Проведение проверок сотрудников и контроль доступа к конфиденциальной информации. Установление четких политик безопасности и их соблюдение. Мониторинг действий сотрудников и выявление аномалий.
Кража данных	Шифрование данных и использование систем управления идентификацией и доступом. Внедрение механизмов быстрого обнаружения и реагирования на инциденты. Регулярное резервное копирование данных.
Вымогательское ПО	Регулярное резервное копирование данных и хранение копий в безопасном месте. Обучение сотрудников распознаванию подозрительных файлов и ссылок. Использование инструментов для предотвращения и обнаружения вымогательского ПО.
Атаки на цепочку поставок	Проведение аудитов и оценка безопасности поставщиков. Установление строгих критериев безопасности для партнеров и поставщиков. Мониторинг и контроль взаимодействия с поставщиками
Социальная инженерия	Обучение сотрудников методам социальной инженерии и способам их предотвращения. Установление строгих процедур проверки личности при запросах на доступ к данным. Регулярные тренировки и тесты на устойчивость к социальным манипуляциям.

Источник: составлено автором по данным [2, 4, 7, 8, 9]

защиты от новых уязвимостей и угроз, что способствует своевременному выявлению и устранению потенциальных рисков. Все это способствует созданию безопасной цифровой среды, защищающей как данные сотрудников, так и репутацию компании.

Таким образом, представленные меры помогают минимизировать риски и защитить организацию от различных киберугроз.

Выводы

В статье рассмотрены подходы к определению понятия «кибербезопасность» по различным источникам, динамика количества кибератак в России за последние пять лет, которая имеет тенденцию к росту. Также систематизированы виды киберугроз для современного предприятия, по каждому из них представлены возможные меры по защите. Исследование основ кибербезопасности помогает компаниям не только защитить свои активы и данные, но и обеспечить долгосрочную устойчивость бизнеса в условиях растущих киберугроз.

ЛИТЕРАТУРА

1. Готовы ли российские компании противостоять кибератакам? // Positive Technologies. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/are-russian-companies-well-prepared-to-fend-off-cyberattacks/#id1 (дата обращения: 10.12.2024).
2. Как обеспечить кибербезопасность своего бизнеса в 2024 году // РБК Компании. — URL: https://companies.rbc.ru/news/wUFvbgOC3I/kak-obespechit-kiberbezopasnost-svoego-biznesa-v-2024-godu/?ysclid=m4v0pt9uxi325948404 (дата обращения: 10.12.2024).
3. Ковалев О.Г., Семенова Н.В. Кибербезопасность современной России: теоретические и организационно-правовые аспекты // Столыпинский вестник. — 2021. — №3. — С. 14–19.
4. Количество кибератак на российский бизнес по итогам 2024 года выросло в четыре раза — подсчитали эксперты // Cyber Media. — URL: https://securitymedia.org/news/kolichestvo-kiberatak-na-rossiyskiy-biznes-po-itogam-2024-goda-vyroslo-v-chetyre-raza-podschitali-ek.html?ysclid=m4v1l4j8x4670856853 (дата обращения: 10.12.2024).
5. Мартынюк М.С. Организационно-управленческие механизмы обеспечения кибербезопасности российских компаний // Финансовые рынки и банки. — 2023. — №6. — С. 5–9.
6. Платунина Г.П., Ермоленко Д.С. Кибербезопасность: искусная защита цифровой экономики // Экономика и качество систем связи. — 2021. — №2. — С. 30–40.
7. Сафонова М.Ф., Ципляева С.А. Кибербезопасность: проблемы и решения // Естественно-гуманитарные исследования. — 2019. — №24(2). — С. 63–68.
8. Шевко Н.Р., Казанцев С.Я. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. — 2020. — №5. — С.185-189.
9. Aldorisio J. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist] // Securityscorecard. — URL: https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit (date of application: 10.12.2024).
10. DS DS/ISO/IEC 27032-2012 Information technology — Security techniques — Guidelines for cybersecurity. Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности: Международный (зарубежный) стандарт от 11 сентября 2012. — URL: https://docs.cntd.ru/document/431889511 (date of application: 10.12.2024).

Журнал «Современная наука: актуальные проблемы теории и практики»