УДК 349:004.056

Саидов Давид Николаевич, бакалавр, Сургутский государственный университет, Г.Сургут

НАУЧНАЯ СТАТЬЯ НА ТЕМУ: «ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК»

Аннотация

В статье рассматриваются организационно-правовые аспекты защиты от сетевых атак в условиях цифровизации. Проанализированы основные виды киберугроз и законодательная база в сфере информационной безопасности. Особое внимание уделено внутренним регламентам, политике безопасности и ответственности персонала. Обоснована необходимость комплексного сочетания правовых, управленческих и технических мер для минимизации ущерба от киберинцидентов.

Ключевые слова: информационная безопасность, сетевые атаки, организационно-правовая защита, политика безопасности, киберугрозы, законодательное регулирование.

Annotation

The article examines the organizational and legal aspects of protection against network attacks in the context of digitalization. The main types of cyber threats and the legislative framework in the field of information security are analyzed. Special attention is paid to internal regulations, security policy, and personnel responsibility. The necessity of a comprehensive combination of legal, managerial, and technical measures to minimize damage from cyber incidents is substantiated.

Key words: information security, network attacks, organizational and legal protection, security policy, cyber threats, legislative regulation.

ВВЕДЕНИЕ

В эпоху тотальной цифровизации, когда информационные системы становятся основой функционирования бизнеса, государственных структур и общества в целом, вопросы обеспечения кибербезопасности выходят на передний план

стратегического управления. Сетевые атаки перестали быть уделом лишь крупных корпораций или финансового сектора — сегодня любая организация, имеющая подключение к интернету, является потенциальной мишенью для злоумышленников. Если ранее основной акцент в борьбе с киберугрозами делался исключительно на технические средства защиты (файрволы, антивирусы, системы шифрования), то современные реалии доказывают недостаточность одних лишь «технических барьеров».

Возрастающая изощренность атак, использование методов социальной инженерии и эксплуатация человеческого фактора требуют смещения фокуса в сторону организационно-правового регулирования. Именно четкая правовая база, внутренние регламенты компании и выстроенная система ответственности персонала формируют тот фундамент, на котором базируется устойчивость всей технической инфраструктуры. В данной статье подробно рассматриваются ключевые аспекты организационно-правовой защиты от сетевых атак, анализируется актуальное законодательство и предлагаются практические механизмы, позволяющие выстроить эффективную систему противодействия киберинцидентам на уровне управления предприятием.

НАУЧНАЯ СТАТЬЯ

1.ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК

В современном цифровом мире киберугрозы становятся все более изощрёнными и масштабными, что требует от организаций комплексного подхода к обеспечению информационной безопасности. Сетевые атаки способны нанести значительный ущерб как финансовому положению компаний, так и их репутации, а также привести к утечке конфиденциальных данных. В связи с этим особое внимание уделяется организационно-правовой защите, которая включает в себя разработку внутренних регламентов, соблюдение законодательных норм и внедрение эффективных процедур реагирования на инциденты.

Организационно-правовая защита от сетевых атак представляет собой совокупность мер, направленных на создание правовой базы и управленческих механизмов для предотвращения и минимизации последствий киберинцидентов. Она охватывает вопросы ответственности сотрудников, договорные отношения с внешними партнёрами, а также взаимодействие с государственными органами в сфере информационной безопасности. В статье рассмотрим ключевые аспекты данной защиты и практические рекомендации по её реализации в корпоративной среде.

2.ВВЕДЕНИЕ В ПРОБЛЕМУ СЕТЕВЫХ АТАК И ИХ ВЛИЯНИЕ НА ОРГАНИЗАЦИЮ

Современные организации сталкиваются с постоянно растущей угрозой сетевых атак, которые могут привести к значительным финансовым потерям, утечке конфиденциальных данных и подрыву репутации. Сложность и разнообразие методов атак, таких как фишинг, DDoS-атаки, вредоносное ПО и целевые взломы, создают серьезные вызовы для обеспечения безопасности информационных систем. Внедрение эффективных организационно-правовых механизмов защиты становится ключевым элементом в формировании устойчивой кибербезопасности. Эти механизмы включают разработку внутренней политики безопасности, регламентации доступа к информации,

проведение обязательного обучения сотрудников и установление ответственности за нарушение правил. Кроме того, своевременное реагирование и сотрудничество с правоохранительными органами способствуют минимизации последствий атак и предотвращению их повторения. В условиях цифровизации бизнес-процессов организациям необходимо осознавать не только технические, но и юридические аспекты противодействия киберугрозам для обеспечения долгосрочной стабильности и доверия клиентов.

3.ОСНОВНЫЕ ВИДЫ СЕТЕВЫХ АТАК И ИХ ХАРАКТЕРИСТИКА

Сетевые атаки представляют собой разнообразные методы воздействия на информационные системы с целью нарушения их работы, кражи данных или получения несанкционированного доступа. Среди основных видов сетевых атак выделяются следующие категории. Первое — атаки отказа в обслуживании (DoS и DDoS), при которых с помощью большого объёма запросов пытаются перегрузить сервер или сеть, делая их недоступными для легитимных пользователей. Второе — фишинг, цель которого — обманным путём заставить пользователя раскрыть конфиденциальную информацию, например пароли или банковские реквизиты, посредством поддельных сайтов или сообщений. Третье — атаки с применением вредоносного программного обеспечения (вирусы, трояны, шпионские программы), внедряющие вредоносный код и нарушающие целостность системы. Четвёртое — межсайтовое скриптование (XSS) и SQL-инъекции, направленные на эксплуатацию уязвимостей веб-приложений для получения несанкционированного доступа к данным. Каждая из этих атак требует соответствующих организационно-правовых мер для своевременного обнаружения и пресечения угроз.

4.ЗАКОНОДАТЕЛЬНАЯ БАЗА И НОРМОТИВНЫЕ АКТЫ ПО ЗАЩИТЕ ОТ СЕТЕВЫХ АТАК

Современная защита от сетевых атак основывается на комплексном регулировании, включающем законодательные и нормативные акты,

направленные на обеспечение информационной безопасности. В Российской Федерации ключевую роль играет Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который устанавливает основные принципы обработки и защиты данных. Дополнительно значим Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», регламентирующий меры защиты систем, обеспечивающих функционирование жизненно важных отраслей. В международной практике важны нормативные документы, такие как Общий регламент по защите данных (GDPR) и стандарты ISO/IEC 27001, направленные на управление информационной безопасностью. Помимо законов, нормы устанавливаются подзаконными актами, постановлениями и отраслевыми стандартами, которые определяют технические и организационные меры противодействия кибератакам. Таким образом, законодательная база представляет собой многоуровневую систему, обеспечивающую правовую основу для разработки и внедрения эффективных средств защиты информационных систем от сетевых угроз.

5.ОРГАНИЗАЦИОННЫЕ МЕРЫ И ПОЛИТИКА БЕЗОПАСНОСТИ В ПРЕДОТВРАЩЕНИИ СЕТЕВЫХ АТАК

Организационные меры и политика безопасности играют ключевую роль в предотвращении сетевых атак, создавая системный подход к защите информационных ресурсов. В основе таких мер лежит разработка и внедрение комплексных правил и процедур, регулирующих поведение пользователей и сотрудников при работе с сетью и данными. Важно обеспечить регулярное обучение персонала вопросам информационной безопасности, чтобы повысить их осведомленность о потенциальных угрозах и методах защиты. Политика безопасности должна включать требования к использованию сложных паролей, контролю доступа, обновлению программного обеспечения и своевременному реагированию на инциденты. Организационные меры предусматривают также регулярный аудит систем безопасности и оценку

уязвимостей, что позволяет выявлять и устранять слабые места до их эксплуатации злоумышленниками. Важным аспектом является формирование культуры безопасности в компании, где каждый сотрудник понимает ответственность за сохранность корпоративных данных. Такой подход обеспечивает слаженную работу технических средств и человеческого фактора, что значительно снижает вероятность успешных сетевых атак и минимизирует потенциальный ущерб.

6.ПРАКТИЧЕСКИ РЕКОМЕНДАЦИИ ПО ВНЕДРЕНИЮ ПРАВОВЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

Для эффективной защиты от сетевых атак необходимо комплексное применение как правовых, так и технических мер. Во-первых, организация должна разработать и утвердить внутренние нормативные документы, регламентирующие правила информационной безопасности, ответственность сотрудников и порядок обработки инцидентов. Важно провести обучение персонала, повысив его правовую грамотность в сфере кибербезопасности, что позволит своевременно выявлять и предотвращать угрозы. С технической стороны рекомендовано внедрение современных средств защиты: межсетевых экранов, систем обнаружения и предотвращения вторжений, а также регулярное обновление программного обеспечения для устранения уязвимостей. Для юридической защиты следует обеспечить регистрацию контрафактных доменов и использовать механизм правовой блокировки источников атак. Кроме того, заключение соглашений с провайдерами услуг и правоохранительными органами ускоряет реакции на инциденты. Внедрение комплексного подхода позволит минимизировать риски и повысить устойчивость к сетевым угрозам.

ЗАКЛЮЧЕНИЕ

Подводя итог, можно с уверенностью утверждать, что организационно-правовая защита от сетевых атак является не просто вспомогательным элементом, а критически важной составляющей общей стратегии кибербезопасности. Технические средства, какими бы совершенными они ни были, не способны полностью нивелировать риски без наличия проработанной нормативной базы и строгого соблюдения регламентов со стороны сотрудников. Правовые нормы, закрепленные как на уровне федерального законодательства, так и в локальных актах компании, создают не только рамки дозволенного, но и механизмы неизбежности ответственности за нарушения, что существенно повышает дисциплину в обращении с информационными ресурсами.

Комплексный подход, объединяющий в себе регулярное обучение персонала, аудит уязвимостей, своевременное обновление политик безопасности и активное взаимодействие с регуляторами и правоохранительными органами, позволяет выстроить эшелонированную оборону. В условиях, когда методы сетевых атак постоянно эволюционируют, статичная защита обречена на провал. Поэтому организационно-правовые механизмы должны находиться в процессе непрерывного совершенствования, адаптируясь к новым вызовам цифровой среды. Только синергия права, менеджмента и технологий способна обеспечить долгосрочную стабильность бизнеса, сохранность конфиденциальных данных и доверие клиентов в современном киберпространстве.

ЛИТЕРАТУРА

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
5. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
6. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: Учебное пособие. — М.: РИОР, 2020.
7. Кузнецов П. У. Информационное право: учебник для вузов. — М.: Юрайт, 2023.
8. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. — М.: Форум, 2017.

LITERATURE

1. Federal Law of July 27, 2006, No. 149-FZ "On Information, Information Technologies, and Information Protection."
2. Federal Law of July 26, 2017, No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation."
3. RF Government Resolution of November 1, 2012, No. 1119 "On Approval of Requirements for the Protection of Personal Data When Processed in Personal Data Information Systems."
4. GOST R ISO/IEC 27001-2021. Information Technology. Security Methods and Tools. Information Security Management Systems. Requirements.
5. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
6. Baranova, E.K., Babash, A.V. Information Security and Information Protection: A Tutorial. Moscow: RIOR, 2020.
7. Kuznetsov, P.U. Information Law: A Textbook for Universities. Moscow: Yurait, 2023.
8. Shan'gin, V.F. Information Security of Computer Systems and Networks: A Tutorial. Moscow: Forum, 2017.