УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ: ОСНОВНЫЕ УГРОЗЫ И ПУТИ ИХ ПРЕДОТВРАЩЕНИЯ

Розумец Владислав Сергеевич, Писклова Ангелина Владимировна

студенты 2 курса факультета

СПО ГБОУ ВО СГПИ

Научный руководитель: Проскурин Николай Николаевич:

Страший преподаватель кафедры начальной военной подготовки и безопасности жизнидеятельности ГБОУ ВО СГПИ

Аннотация. В статье рассматриваются актуальные проблемы обеспечения кибербезопасности в современном информационном обществе. Анализируются основные виды киберугроз, особенности их распространения и последствия для государства, организаций и отдельных пользователей. Особое внимание уделяется мерам профилактики киберпреступлений и формированию культуры информационной безопасности.

Ключевые слова: кибербезопасность, информационная безопасность, киберугрозы, киберпреступность, защита информации.

CYBER SECURITY IN THE MODERN WORLD: MAIN THREATS AND WAYS TO PREVENT THEM

Rozumets Vladislav Sergeevich, Pisklova Angelina Vladimirovna

Scientific adviser: Proskurin Nikolai Nikolaevich

Abstract: The article examines current issues of ensuring cybersecurity in the modern information society. The main types of cyber threats, the specifics of their spread, and

the consequences for the state, organizations, and individual users are analyzed. Particular attention is paid to measures for preventing cybercrime and fostering a culture of information security.

Keywords: cybersecurity, information security, cyber threats, cybercrime, information protection.

Современное общество характеризуется стремительным развитием информационных технологий. Цифровизация практически всех сфер деятельности человека привела к значительному увеличению объема информации, циркулирующей в глобальных сетях. Вместе с тем развитие информационного пространства сопровождается ростом различных угроз безопасности данных и информационных систем.

Проблема обеспечения кибербезопасности становится одной из ключевых задач как для отдельных государств, так и для международного сообщества в целом. По мнению исследователей, рост числа кибератак связан с увеличением количества пользователей сети Интернет и расширением цифровой инфраструктуры [1, с. 15].

В настоящее время киберпреступность представляет собой сложное социально-техническое явление, которое затрагивает экономические, политические и социальные процессы. В этой связи особую актуальность приобретает анализ основных угроз в киберпространстве и разработка эффективных механизмов противодействия им [2, с. 37].

Одной из наиболее распространенных угроз являются вредоносные программы. К данной категории относятся вирусы, трояны, шпионские программы и другие типы вредоносного программного обеспечения,

которые предназначены для получения несанкционированного доступа к данным или нарушения работы информационных систем.

Не менее опасной угрозой является фишинг. Данный метод предполагает получение конфиденциальной информации пользователей посредством поддельных сайтов или электронных писем. Исследования показывают, что значительная часть успешных кибератак осуществляется именно благодаря социальной инженерии [3, с. 52].

Еще одной серьезной проблемой являются атаки типа «отказ в обслуживании» (DDoS). Они направлены на перегрузку серверов большим количеством запросов, что приводит к невозможности нормальной работы веб-ресурсов. Такие атаки могут нанести значительный экономический ущерб организациям и государственным структурам [4, с. 61].

В условиях цифровой трансформации государственные структуры также сталкиваются с угрозами в киберпространстве. Информационные системы органов власти, банковских организаций и крупных предприятий становятся объектами целенаправленных кибератак.

Особую опасность представляют атаки на критическую информационную инфраструктуру. Нарушение работы таких систем может привести к серьезным последствиям для функционирования экономики и безопасности государства [5, с. 74].

Кроме того, распространение киберпреступности оказывает влияние на социальную сферу. Утечка персональных данных, мошенничество в сети Интернет и распространение вредоносного контента формируют новые риски для пользователей информационных технологий [2, с. 89].

Для эффективного противодействия киберугрозам необходимо применение комплексного подхода. Он включает технические, организационные и образовательные меры.

К техническим мерам относятся использование антивирусных программ, систем обнаружения вторжений, шифрование данных и регулярное обновление программного обеспечения. Данные методы позволяют значительно снизить вероятность успешной атаки на информационные системы [3, с. 101].

Организационные меры предполагают разработку политики информационной безопасности, регламентацию доступа к данным и контроль за использованием информационных ресурсов.
Важную роль также играет повышение квалификации специалистов в области кибербезопасности.

Не менее значимым направлением является формирование культуры безопасного поведения в сети Интернет. Пользователи должны обладать базовыми знаниями о возможных угрозах и способах защиты персональной информации [1, с. 122].

Таким образом, кибербезопасность является важнейшим элементом функционирования современного информационного общества. Рост числа киберугроз требует постоянного совершенствования методов защиты информации и разработки новых механизмов противодействия киберпреступности.

Эффективная система обеспечения кибербезопасности должна включать взаимодействие государства, организаций и пользователей информационных

технологий. Только комплексный подход позволит снизить уровень рисков и обеспечить устойчивое развитие цифровой среды [4, с. 140].

Для эффективного противодействия подобным угрозам критически важно не только постоянно совершенствовать системы безопасности, но и активно отслеживать любую подозрительную активность в сети, обучать население основам кибербезопасности, а также налаживать партнерские отношения с другими государствами.

Такие меры позволят надежно защитить конфиденциальные данные и ключевые ресурсы от возможных атак как существующих, так и потенциальных угроз. Киберпреступность, включая атаки на государственные системы и частный бизнес, несет в себе риск серьезных экономических потерь и может спровоцировать социальные и политические кризисы.

Для эффективного решения подобных задач необходимо, чтобы государственные органы располагали всеми необходимыми ресурсами и полномочиями. Создание мер по предотвращению будущих инцидентов и наказание за совершенные преступления являются ключевыми задачами государства. Кроме того, для обеспечения защиты критически важных информационных ресурсов госорганы должны активно внедрять технологии мониторинга интернет-трафика, выявления аномалий в поведении сети и оперативного реагирования на обнаруженные угрозы.

Список источников

1. Касперский Е.В. Компьютерные угрозы и защита информации. – М.: Информационная безопасность, 2021. – 256 с.

2. Смирнов А.А. Основы информационной безопасности. – СПб.: Питер, 2020. – 320 с.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем. – М.: Форум, 2019. – 416 с.

4. Лопатин В.Н. Кибербезопасность и киберпреступность. – М.: Юрайт, 2022. – 280 с.

5. Кузнецов П.А. Защита информации в информационных системах. – М.: Академия, 2021. – 240 с.