**Литература**

1. Сколько мирового электричества тратят на майнинг. [Электронный ресурс] Режим доступа: https://devby.io/news/maining.amp, свободный.

2.Чёрный майнинг.[Электронный ресурс] Режим доступа: https://lifehacker.ru/chernyj-majning/, свободный.

УДК 338.2

## ИСТОРИЯ КИБЕРУГРОЗ И КИБЕРБЕЗОПАСНОСТИ: ОСНОВНЫЕ ЭТАПЫ

Литвинюк К.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Кибербезопасность – это защита компьютерных систем от кражи или повреждения их оборудования, программного обеспечения или данных, а также от отказа или нарушения предоставляемых ими услуг. История киберугроз начинается с первых шагов информационных технологий, когда создаваемые вирусы были простыми и не представляли серьезной угрозы. Однако со временем, как и технологии, методы кибератак стали усложняться. Это способствовало постоянному развитию методов кибербезопасности, направленных на нейтрализацию угроз. Понимание этапов развития кибербезопасности помогает осознавать текущие вызовы и прогнозировать будущие угрозы.

Ранние годы развития киберугроз и кибербезопасности, охватывающие 1970-е и начало 1980-х годов, являются ключевым периодом в истории информационных технологий, отмеченным зарождением первых компьютерных вирусов и началом осознания необходимости защиты информационных систем. Этот этап характеризуется началом широкого использования компьютеров не только в академических и военных целях, но и в коммерческих организациях, а также появлением первых сетевых технологий, которые способствовали быстрому распространению вредоносного программного обеспечения.

Одним из первых вирусов, оказавших заметное влияние на развитие кибербезопасности, был Creeper, появившийся в 1971 году. Эта экспериментальная программа, созданная Реем Томлинсоном, могла самостоятельно перемещаться по сети ARPANET, выводя на экраны пользователей сообщение: "I'm the creeper, catch me if you can!" В ответ на эту угрозу был

разработан Reaper – программа, которая искала и уничтожала Creeper, ставшая первым в истории антивирусом. [1]

Конец 1970-х и начало 1980-х годов ознаменовались не только ростом числа персональных компьютеров, но и увеличением их функциональности, что сопровождалось осознанием потенциальной уязвимости про-граммного обеспечения для вредоносных атак. В 1983 году ученый Фред Коэн в своих экспериментах формализовал термин "компьютерный вирус", продемонстрировав, как программы могут заражать компьютеры и ис-пользовать их ресурсы для копирования себя, что стало поворотным мо-ментом в понимании механизмов распространения вирусов.

Развитие сетевых технологий, таких как ARPANET, и расширение числа компьютерных сетей по всему миру увеличили актуальность угроз безопасности. Вирусы стали распространяться быстрее и становиться более разрушительными, что привело к необходимости разработки более совершенных методов защиты. Это включало создание первых коммерческих антивирусных программ и политик безопасности, которые начали формировать основу для современных мер защиты информационных систем. [2]

Также в этот период началось формирование законодательства, регулирующего использование и защиту информационных технологий, что отражало растущее осознание важности информационной безопасности на государственном уровне. Политики безопасности включали ограничение доступа к важной информации, использование паролей и других мер идентификации для обеспечения защиты данных.

Таким образом, период 1970-х – начала 1980-х годов заложил фундамент для современной кибербезопасности, сформировав основные принципы защиты информации и предоставив первый опыт борьбы с киберугрозами. Этот этап показал, что развитие технологий неразрывно связано с ростом киберугроз, что требует непрерывного усиления мер безопасно-сти.

В 1990-е годы, с появлением и распространением интернета, мир столкнулся с новой волной киберугроз, которые стали более масштабными и разрушительными. Этот период ознаменовался расцветом вирусов и червей, которые могли быстро распространяться через электронную почту и другие сетевые механизмы. Самыми известными примерами являются вирусы ILOVEYOU и Melissa, которые поразили миллионы компьютеров по всему миру, вызвав значительные экономические потери. [2]

Эта эпоха также стала свидетелем начала использования сложных механизмов кибератак, таких как DDoS-атаки и фишинг, что сделало оче-видной необходимость в развитии более продвинутых средств защиты. В ответ на растущие угрозы, были разработаны новые антивирусные программы, системы обнаружения вторжений и файерволы. Также началось формирование первых комплексных политик кибербезопасности, направленных на

защиту индивидуальных пользователей и организаций. Этот период показал, что кибербезопасность требует глобального подхода и сотрудничества на всех уровнях общества.

В 2000-е годы, на фоне бурного развития цифровой экономики и всеобщего перехода на онлайн-технологии, мир столкнулся с новой волной киберпреступности. Этот период характеризуется заметным ростом финансовых махинаций в интернете, включая фишинг, спуфинг и атаки с использованием вредоносного ПО, направленные на кражу банковских данных и личной информации.

Киберпреступники стали использовать сложные многоэтапные схемы для проведения мошеннических операций, что потребовало от организаций усиления мер безопасности. В ответ на это были разработаны новые стандарты и технологии защиты, включая шифрование данных и многофакторную аутентификацию, а также международные нормативы, такие как PCI DSS для защиты платежной информации и GDPR в Европе для за-щиты данных пользователей.

В этот период также активизировалась работа по созданию национальных и международных законодательных и нормативных рамок, направленных на борьбу с киберпреступностью. Усиление киберзащиты стало приоритетной задачей не только для IT-специалистов, но и для управленческих структур на всех уровнях, подчеркивая необходимость комплексного и системного подхода к обеспечению кибербезопасности.

С 2010-х годов до настоящего времени кибербезопасность сталкивается с новыми и более сложными вызовами. Распространение облачных технологий, интернета вещей (IoT) и мобильных устройств привело к увеличению количества кибератак, таких как распространение вредоносного ПО, рэнсомвар и утечки данных. Кроме того, значительные угрозы представляют организованные группы хакеров и государственно-поддерживаемые кибератаки, нацеленные на критически важные инфраструктуры и корпоративные сети.

В ответ на эти угрозы происходит активное внедрение новых технологий защиты, включая искусственный интеллект и машинное обучение для предсказания и нейтрализации атак, а также усиление мер по защите персональных и корпоративных данных. Важным направлением стала разработка правовых и технических норм, направленных на усиление кибер-безопасности на национальном и международном уровнях. Этот период подчеркивает, что эффективное противодействие киберугрозам требует комплексного подхода и глобального сотрудничества. [1]

В заключение, история киберугроз и кибербезопасности демонстрирует постоянную эволюцию угроз и ответных мер. От простых вирусов первых компьютерных сетей до сложных многоуровневых атак современности,

каждый новый этап технологического развития приводит к новым вызовам в области защиты информации. Эффективное противодействие киберугрозам требует не только применения передовых технологий и строгих процедур, но и постоянного обучения специалистов, а также сотрудничества на международном уровне. Только комплексный и интегрированный подход к кибербезопасности может обеспечить надежную защиту в условиях постоянно меняющегося ландшафта угроз.

**Литература**

1. Clarke, C. A. (2001). Cyberwar: The Next Threat to National Security. Potomac Books Inc.

2. Denning, D. E. (2018). The Invisible Governance Frontier: Defending Democracy in the Age of Cyber Threats. Oxford University Press.

## РАСШИРЕНИЕ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ В ТАМОЖЕННОЙ СФЕРЕ

Литвинюк К.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В современном мире вопросы обеспечения безопасности государственных границ и упрощения таможенных процедур становятся особенно актуальными. Эффективность функционирования таможенных органов напрямую зависит от применяемых технологий, среди которых особое место занимает биометрическая идентификация. Эта технология позволяет ускорить процесс проверки документов, уменьшить вероятность ошибок и обеспечить высокий уровень защиты от нелегальной иммиграции и контрабанды.

Цель данной научной работы заключается в изучении перспектив и возможностей расширения использования биометрической идентификации в таможенной сфере Республики Беларусь. В работе будут рассмотрены современные подходы и технологии биометрической идентификации, анализ их применимости в таможенных процессах, а также возможные пути интеграции данных систем в существующую инфраструктуру.

Биометрическая идентификация в таможенной сфере может включать использование отпечатков пальцев, радужной оболочки глаза, лицевого распознавания и других уникальных биологических и поведенческих характеристик личности. Введение таких систем предполагает ряд технических и