65. КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ ЦИФРОВОЙ ЭКОНОМИКИ: ВЫЗОВЫ И РЕШЕНИЯ

Герасименя В.В., студентка гр. 378104, Раптунович О. М., магистрант группы 376741, Липницкая Н.И., ассистент кафедры ЭИ

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Ефремов А.А. – канд. экон. наук, доцент каф. ЭИ

Аннотация. Данное исследование посвящено изучению и анализу текущего состояния кибербезопасности в сфере цифровой экономики. Исследование показало активное возникновение новых угроз и вызовов для кибербезопасности. В результате были предложены инновационные решения для защиты информации.

В современной цифровой экономике кибербезопасность становится неотъемлемой частью нашей повседневной жизни. Все большее число людей зависит от цифровых технологий, таких как мобильные устройства. В них хранится значительное количество личных данных и осуществляется множество операций, включающих обмен сообщениями и совершение финансовых транзакций. Злоумышленники могут попытаться получить доступ к этой информации. Разберемся, какие основные угрозы существуют и какие меры по предотвращению и реагированию на кибератаки существуют.

Актуальность исследования связана с увеличением рисков и угроз в сфере кибербезопасности. Необходимость повышения безопасности информации и сетевой инфраструктуры становится неотъемлемой для обеспечения надежного функционирования цифровой экономики и защиты интересов организаций и пользователей.

Главная цель исследования заключается в изучении и анализе кибербезопасности в контексте цифровой экономики с задачей определения вызовов и поиска решений для предстоящих кибератак.

Для достижения цели были поставлены следующие задачи:

- Оценить важность проблемы кибербезопасности в контексте цифровой экономики.
- Исследовать основные вызовы, с которыми сталкиваются организации в области кибербезопасности.
- Выявить основные проблемы, с которыми сталкиваются организации и пользователи.
- Разработать рекомендации по внедрению современных методов и технологий.

Объектом исследования является взаимосвязь между кибербезопасностью и цифровой экономикой. Предметом – роль и значимость кибербезопасности в контексте цифровой экономики.

Вопрос кибербезопасности стал актуален с тех пор, когда только появились компьютеры и начали развиваться информационные технологии. В 1988 году была совершена первая кибератака червя Morris. Он стал одним из первых крупным и масштабным компьютерным червем и заразил несколько тысяч компьютеров. После такой крупной атаки разработчики приняли решение применить меры безопасности в сети для защиты данных в компьютерных системах.

Кибербезопасность – система определенных практик, используемых для защиты компьютерных систем, сетей и данных от повреждений и утечек. Кибербезопасность обеспечивает конфиденциальность и целостность информации, поступающей на сервера. Кибератака – попытка или акт несанкционированного проникновения в компьютерные системы или сети с целью получить доступ к информации, повредить, совершить кражу данных, а также нарушить стабильное функционирование системы.

Одни из первых разработок для решения вопросов кибербезопасности были написаны и введены в действия до 2000-х годов. Разработка антивирусных программ – одна первых мер по защите от вредоносных программ. Они сканировали компьютеры и сети на предмет вирусов, после чего, в случае обнаружения, удаляли, изолировали или обезвреживали вирусы. Брандмауэры были разработаны для контроля и фильтрации сетевого трафика с целью предотвращения вторжения из внешних сетей и предоставления несанкционированного доступа к данным. Брандмауэры устанавливали правила доступа к сети или Интернет-ресурсам, а также разрешали или блокировали соединения с компьютерами в другой сети. Шифрование данных использовалось для защиты конфиденциальности информации во время передачи ее по сети или хранении на различных устройствах. Технологии шифрования позволяли обеспечить безопасную передачу данных между серверами или сервером и клиентом.

С течением времени решения и разработки в области кибербезопасности совершенствовались и создавались новые варианты для обеспечения защиты. В данный момент в это понятие включается широкий спектр технических и иных особенностей, решающих проблему и обеспечивающих надежную защиту от киберугроз. Появление искусственного интеллекта повлияло на разработки и решения в данной области. Искусственный интеллект – область компьютерных наук, которая занимается созданием программ и систем, способных выполнять задачи, используя данные и алгоритмы. Данные

разработки позволяют автоматизировать процессы обнаружения, анализа и устранения угроз. Параллельно решениям проводилось обучение пользователей. Люди получают информацию о потенциальных угрозах, информацию о том, как необходимо устанавливать и использовать пароли, распознавать мошеннические схемы и иные методы попыток завладения персональных данных. Блокчейн-технологии оказывают большое влияние на обеспечение кибербезопасности. Блокчейн-технология – это распределенная база данных, которая записывает транзакции и события в виде блоков, которые затем связываются в цепочку. Данная разработка надежна и невозможно изменить информацию, хранящуюся в ней, без согласия большинства участников сети.

Проблемы, связанные с существующими решениями и разработками: увеличение атак в цифровой среде; быстрое развитие технологий; различная архитектура, протоколы и интерфейсы систем и платформ; недостаток единых стандартов; нехватка квалифицированных специалистов; недостаточная прозрачность и отчетность; недостаточная реакция на кибератаки; отсутствие поддержки инноваций и исследований; недостаточное исспользование средств автоматизации и аналитики.

Гипотезы, которые могут улучшить функционирование системы кибербезопасности в цифровой экономике. Гипотеза 1. Внедрение обязательного аудита безопасности для организаций, занимающихся обработкой и хранением больших объемов данных, улучшит функционирование кибербезопасности в цифровой экономике. Гипотеза 2. Создание глобального стандарта отчетности о мерах по кибербезопасности и инцидентах. Стандарт, который примут и будут применять все организации. Гипотеза 3. Внедрение системы непрерывного мониторинга и обнаружения нарушений безопасности с использованием искусственного интеллекта позволит оперативно выявлять и реагировать на киберугрозы, улучшая защиту в цифровой экономике. Гипотеза 4. Обязательное включение обучения по кибербезопасности в учебные программы и повышение осведомленности пользователей о современных угрозах поможет создать более безопасную цифровую экономику. Гипотеза 5. Внедрение строгих санкций и наказаний для нарушителей кибербезопасности будет служить отпугивающим фактором и снизит уровень киберпреступности, повышая общую безопасность в цифровой экономике.

По результатам исследований можно сделать вывод, что вопрос кибербезопасности является актуальным с самого появления компьютеров и развития информационных технологий. Кибербезопасность включает систему практик, направленных на защиту компьютерных систем, сетей и данных от повреждений и утечек. Она обеспечивает конфиденциальность и целостность информации. Разработки в области кибербезопасности включают антивирусные программы и шифрование данных. Они были разработаны для обнаружения и устранения угроз, контроля сетевого трафика и защиты конфиденциальности данных. С течением времени решения и разработки в области кибербезопасности совершенствовались. Однако существуют проблемы, связанные с решениями и разработками. Для улучшения функционирования системы кибербезопасности в цифровой экономике предлагаются несколько гипотез.

Таким образом, кибербезопасность в цифровой экономике имеет важное значение и требует постоянного внимания. Развитие информационных технологий и цифровых систем приводит к возрастанию угроз и рисков, связанных с безопасностью данных, сетей и компьютерных систем. Результаты научных исследований могут использоваться для разработки рекомендаций и стандартов безопасности, которые помогут организациям и пользователям защитить свои данные и системы. Исследования способствуют развитию защитных мер и рекомендаций, повышают осведомленность пользователей и способствуют разработке политики и законодательства в этой области.

Список использованных источников:

1. Безкоровайный М. М., Лосев С. А., Татузов А. Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. – 2011. – №. 6. – С. 27-32.

2. Кусков Н.А. Исследование способов несанкционированного доступа к информации // Научный вестник Московского государственного технического университета гражданской авиации. – 2013г. - № 6 (192). – С. 127 – 129.

3. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. - 2015. - № 13. - С. 96-99.

4. Никишова М.И. Перспективы применения технологий искусственного интеллекта в корпоративном управлении в условиях перехода к цифровой экономике // Управленческие науки в современном мире, 2018. – Т. 1. – № 1. – С. 233-237.