УДК 004.056

ТЕХНОЛОГИИ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ

А. В. Кондакова

студентка направления «Бизнес-информатика», Минский филиал Российского экономического университета им. Плеханова, г. Минск, Беларусь, e-mail: kondakovaanastasia278@gmail.com

Научный руководитель: **С. К. Комаров**

кандидат технических наук, доцент кафедры информационных технологий и социально-гуманитарных дисциплин, Минский филиал Российского экономического университета им. Плеханова, г. Минск, Беларусь, e-mail: skkomarow@gmail.com

В данной статье дается понятие кибербезопасности в ИТ-сфере, а также сформулированы основные тенденции развития технологий в и рассмотрены основные методы защиты информации в эпоху цифровизации. С развитием инновационных технологий в обществе появляются новые понятия в области информационной безопасности. Статья призвана дополнить соответствующие знания о новейших технологиях кибербезопасности и дать им полную характеристику в соответствии с имеющейся информацией.

Ключевые слова: информационная безопасность; кибербезопасность; информационные технологии.

CYBERSECURITY TECHNOLOGIES IN THE ERA OF DIGITALIZATION

A. V. Kondakova

student of Business Informatics, Minsk Branch of the Plekhanov Russian University of Economics, Minsk, Belarus, e-mail: kondakovaanastasia278@gmail.com

Supervisor: **S. K. Komarov**

PhD in Technical Sciences, Associate Professor of the Department of Information Technologies and Social and Humanitarian Disciplines, Minsk Branch of the Plekhanov Russian University of Economics, Minsk, Belarus, e-mail: skkomarow@gmail.com

In this article, the concept of cybersecurity in the IT sphere is given, as well as the main trends in the development of technologies in and the main methods of information protection in the era of digitalization are formulated. With the development of innovative

technologies, new concepts in the field of information security appear in society. The article is recognized to supplement the relevant knowledge about the latest cybersecurity technologies and give them a full description in accordance with the available information.

Keywords: information security; cybersecurity; information technology.

Когда современный мир с каждым годом претерпевает изменения, связанные с развитием информационных технологий, встает вопрос о том, а как же сохранить все те данные, которые были накоплены годами и десятилетиями? Как не допустить потерю информации? Ведь с ростом использования цифровых технологий возрастает риск утечки информации и угрозы безопасности данных с изменением целостности инфраструктур.

Информационная безопасность, она же кибербезопасность, стала одной из важных областей в ИТ-сфере. Как для крупного, так и для малого бизнеса кибербезопасность играет огромную роль, связанную с защитой компьютеров, различных программных приложений и сетей. Компании используют цифровые системы и высокоскоростное подключение, чтобы обеспечивать эффективное обслуживание клиентов и экономичные бизнес-операции, а также применяют различные стратегии информационной безопасности, которые бы сводили к минимуму нежелательные последствия кибератак [1].

С каждым днем специалисты со всего мира разрабатывают технологии в области кибербезопасности. Ведь кибератаки, как и человек, эволюционируют по мере развития технологий. И каждый раз, когда создаются новые инструменты и программы для защиты данных, злоумышленники придумывают новые способы и стратегии, например, для получения незаконного доступа к различным системам [1].

Однако, несмотря на это, искусственный интеллект, как один из новейших технологий в области кибербезопасности, охватил все информационное пространство и по праву считается открытием XX века. Искусственный интеллект выявляет несвойственное поведение злоумышленников в базах данных или в сетевых конфигурациях, что облегчает выявление постороннего доступа к информации и может полностью предотвратить этот несанкционированный доступ к важной информации [2].

Системы идентификации и аутентификации, как методы предотвращения утечки информации, помогают удостоверить личность пользователя и гарантировать, что он имеет право на доступ к требуемой информации. На сегодняшний день существует различные методы аутентификации, которые мы используем в повседневной жизни. Это голосовое распознавание речи, пароли, распознавание по биометрическим данным: отпечатки пальцев, рисунки сетчатки глаза, геометрия лица и им подобные.

Кроме существования таких методов безопасности, как искусственный интеллект и системы идентификации и аутентификации, специалисты выделяют еще один метод – это Open Source Software. Дословно переводится, как программное обеспечение с открытым исходным кодом. Исходный код таких программ доступен для просмотра, изучения или изменения, что дает возможность убедиться в отсутствии проблем, уязвимостей и неприемлемых для пользователя функций. Например, скрытого слежения за пользователем программы. Данный код доступен всем, он позволяет компаниям создавать свои кибербезопасные решения [3; 4].

Важно понимать, что кибербезопасность не ограничивается только технологиями искусственного интеллекта, системами идентификации и аутентификации и программного обеспечения с открытым исходным кодом. Это комплексная проблема, которая требует комплексного решения. Например, общего взаимодействия технических мер безопасности, организационных стратегий, образования и поддержки со стороны общества. Системы защиты должны быть обязательно гибкими, многоуровневыми, способными адаптироваться к новым угрозам и уязвимостям [5].

Сегодня информационная безопасность – это одним из самых актуальных тем в современном мире. Своего рода кибербезопасность – это бизнес-модель любой компания, фирмы или предприятия, часть стратегий, планирования и управления во всех стадиях бизнес-операций, дизайна и разработки систем и доступности для пользователей. Без кибербезопасности не сможет существовать компания. Это культура, к которой необходимо прислушиваться, так как в первую очередь это меры предосторожности к цифровым атакам.

Библиографические ссылки

1. Абдуллаев Э. А. Кибербезопасность: вызовы и стратегии защиты в цифровую эпоху // Молодой ученый. 2023. № 33(480). С. 8–9. URL: https://moluch.ru/archive/480/105493/ (дата обращения: 23.09.2023).

2. Информационная безопасность в эпоху цифровизации [Электронный ресурс]. URL: https://dzen.ru/a/ZIRU6ZSvqls4MuNE (дата обращения: 23.09.2023).

3. Кибербезопасность в эпоху цифровизации: вызовы и решения [Электронный ресурс]. URL: https://dzen.ru/a/ZI9PVdcpHwHpcGMy (дата обращения: 23.09.2023).

4. Открытое программное обеспечение [Электронный ресурс] // Википедия. URL: Открытое программное обеспечение – Википедия (wikipedia.org) (дата обращения: 23.09.2023).

5. Open source [Электронный ресурс] // Skillfactory Media. URL: https://blog.skillfactory.ru/glossary/open-source/?ysclid=lmwh9pdd1f928459068 (дата обращения: 23.09.2023).