Столыпинский вестник

Научная статья

Original article

УДК 338.1

ВЫЗОВЫ И РЕШЕНИЯ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

CHALLENGES AND SOLUTIONS IN THE FIELD OF CYBER SECURITY IN THE AGE OF DIGITAL TRANSFORMATION

Назарова Александра Дмитриевна, студент, Уральский государственный экономический университет, Екатеринбург, Россия, alya.nazarova.02@inbox.ru

Шведов Владислав Витальевич, кандидат исторических наук, доцент кафедры государственного и муниципального управления, Уральский государственный экономический университет, Екатеринбург, Россия, shvedoff@mail.ru

Nazarova Alexandra Dmitrievna, student, Ural State University of Economics, Yekaterinburg, Russia, alya.nazarova.02@inbox.ru

Sulimin Vladimir Vlasovich, Candidate of Historical Sciences, Associate Professor, Department of State and Municipal Administration, Ural State University of Economics, Yekaterinburg, Russia, shvedoff@mail.ru

Аннотация. Кибербезопасность в эпоху цифровизации является одной из наиболее актуальных проблем современности. Развитие технологий и переход к цифровым технологиям приводит к тому, что все больше информации о людях и компаниях хранится в сети. Однако это также увеличивает риски для нашей

безопасности. В статье рассматривается тема кибербезопасности в эпоху цифровизации. Анализируются вызовы, связанные с угрозами безопасности в сети, рассмотрена роль веб-аналитики, а также предлагаются решения для защиты информации и предотвращения кибератак. Также отмечается важность обеспечения безопасности информации в компаниях и организациях. Кроме того, статья подчеркивает, что кибербезопасность - это задача не только отдельных пользователей, но и государственных органов и международного сообщества в целом. Только совместными усилиями мы можем обеспечить безопасность в сети и защитить свою конфиденциальную информацию.

Abstract. Cybersecurity in the era of digitalization is one of the most pressing problems of our time. The development of technology and the transition to digital technologies lead to the fact that more and more information about people and companies is stored on the network. However, this also increases the risks to our security. The article deals with the topic of cybersecurity in the era of digitalization. The challenges associated with network security threats are analyzed, the role of web analytics is considered, and solutions are proposed for protecting information and preventing cyber attacks. The importance of ensuring the security of information in companies and organizations is also noted. In addition, the article emphasizes that cybersecurity is not only a task for individual users, but also for government agencies and the international community as a whole. Only by working together can we ensure online security and protect our confidential information..

Ключевые слова: кибербезопасность, цифровизация, угрозы безопасности, защита информации, кибератаки, веб-аналитика.

Keywords: cyber security, digitalization, security threats, information security, cyber-attacks, web analytics.

Современный мир стал все более зависим от цифровых технологий. Многие аспекты жизни, включая банковские операции, покупки, коммуникацию и работу, теперь проходят через интернет и хранятся в цифровом виде. Это

приводит к тому, что кибербезопасность становится важнее, чем когда-либо ранее. Угрозы безопасности в сети становятся все более изощренными, и без должной защиты любая компания, организация или частное лицо может стать жертвой кибератак.

Перейдём к определению. Кибербезопасность – это условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться нежелательными [1, с. 216].

Одним из главных вызовов области кибербезопасности является то, что технологии и угрозы постоянно меняются, и защитные меры должны быть адаптированы под эти изменения. Некоторые из наиболее актуальных угроз включают в себя кибератаки на Интернет вещей (IoT), социальную инженерию, фишинг и мошенничество с использованием искусственного интеллекта.

Киберпреступники используют различные методы, чтобы получить доступ к конфиденциальной информации или заразить компьютеры вредоносным ПО. Одним из методов является фишинг. Фишинг − это атака, при которой злоумышленник отправляет ложные электронные письма, которые выглядят так, будто они были отправлены от имени надежной организации. Такая атака является относительно новым видом мошенничества [3, с.58]. В этих письмах часто просится предоставить личную информацию, такую как пароль или номер кредитной карты. Целью таких атак является получение доступа к конфиденциальным данным.

Еще одним вызовом является Малварь. Малварь (Malware) − вредоносное программное обеспечение, имеющее своей целью в той или иной форме нанести ущерб пользователю или компьютеру и его содержимому [2]. Малварь может использоваться для сбора личной информации, в том числе паролей, банковских данных и других конфиденциальных данных.

Вредоносные программы создают множество проблем пользователю − от маленьких почти незаметных неудобств до серьезного финансового вреда:

меняют настройки браузера и не дают изменить их пользователю (например, устанавливает новую домашнюю страницу или поиск по умолчанию); устанавливают рекламные программы на компьютер, такие как всплывающие окна и баннеры, которые работают даже без подключения к интернету и т.д.

Другим вызовом является DDoS-атака. DDoS-атака - это атака на сервер, при которой используется большое количество компьютеров для создания высокой нагрузки на сервер. Целью такой атаки может быть отказ в обслуживании, что приводит к недоступности сайта или сервиса.

Для решения вызовов, связанных с угрозами безопасности в сети, необходимы соответствующие меры безопасности. Одним из наиболее эффективных методов является использование шифрования данных. Шифрование позволяет защитить данные от несанкционированного доступа и предотвратить их утечку. Также важным методом является установка антивирусного ПО, которое обеспечивает защиту от вредоносных программ и других угроз безопасности [2].

Обучение пользователей также является важным. Пользователи должны знать, какие методы используют киберпреступники, и как их избежать. Они должны знать, какой вид информации можно безопасно передавать через Интернет, а какой следует хранить локально. Кроме того, компании и организации должны обеспечить безопасность своей информации, устанавливая политики безопасности и обучая своих сотрудников.

Кроме того, государства и международные организации также играют важную роль в обеспечении кибербезопасности. Они должны разрабатывать соответствующие законы и политики для защиты данных и борьбы с киберпреступностью. Также важно, чтобы они сотрудничали в этой области и обменивались информацией о новых угрозах безопасности в сети [3].

Кибербезопасность в эпоху цифровизации − это сложный вопрос, который требует внимания со стороны пользователей, компаний, организаций, государственных органов и международного сообщества в целом. Современный мир зависит от цифровых технологий, и защита от угроз безопасности в сети становится важнее, чем когда-либо ранее. Киберпреступники используют различные методы, чтобы получить доступ к конфиденциальной информации или заразить компьютеры вредоносным ПО. Фишинг, малварь и DDoS-атаки − это некоторые из главных вызовов, связанных с безопасностью в сети.

Решение этих вызовов может включать различные методы, включая использование шифрования и многофакторной аутентификации для защиты личных данных, мониторинг сетевых активностей для обнаружения потенциальных угроз и разработку стратегий обучения и просвещения пользователей для повышения осведомленности о кибербезопасности.

Однако, для решения этих вызовов необходимо больше, чем просто технические решения. Необходимо улучшить культуру кибербезопасности, включая обучение пользователей о том, как обезопасить свои данные и устройства, а также сотрудников организаций о том, как предотвратить утечку конфиденциальных данных.

Для обеспечения кибербезопасности в веб-аналитике, компании должны использовать безопасные протоколы и шифрование данных, а также внедрять механизмы аутентификации и авторизации, чтобы предотвратить несанкционированный доступ к системам.

Шифрование данных и установка антивирусного ПО − это только некоторые из методов, которые можно использовать для защиты информации и предотвращения кибератак. Однако, также важно обучать пользователей и устанавливать соответствующие политики безопасности в компаниях и организациях.

Кроме того, государства и международные организации также играют важную роль в обеспечении кибербезопасности. Они должны разрабатывать

соответствующие законы и политики для защиты данных и борьбы с киберпреступностью. Также важно, чтобы они сотрудничали в этой области и обменивались информацией о новых угрозах безопасности в сети.

Все вышеперечисленные методы и рекомендации имеют целью обеспечить безопасность в сети. Но, необходимо отметить, что киберпреступность и угрозы безопасности в сети продолжают развиваться и становятся все более сложными и изощренными. Это означает, что защита от кибератак и обеспечение кибербезопасности является непрерывным процессом, который требует постоянного мониторинга и анализа новых угроз. Поэтому, важно не только применять соответствующие меры безопасности, но и постоянно совершенствовать их, чтобы быть готовыми к новым угрозам.

Наконец, мы должны понимать важность кибербезопасности и ее роль в обеспечении безопасности в целом. В цифровом мире, где данные являются ключевым активом, защита от киберугроз должна быть приоритетом для каждого человека, компании или организации. Необходимо осознавать, что кибербезопасность − это общественная задача, и только совместными усилиями мы можем обеспечить безопасность в сети и защитить свою конфиденциальную информацию. Обеспечение экибербезопасности в веб-аналитике является необходимым условием для защиты данных пользователей и уверенной работы компании на рынке.

Однако, кибербезопасность не должна стать препятствием для инноваций и развития технологий. Необходимо найти баланс между безопасностью и комфортом использования технологий. Кроме того, важно помнить о значимости этики в сети и уважать права других людей на приватность и безопасность.

Таким образом, кибербезопасность в эпоху цифровизации − это сложный вопрос, который требует внимания со стороны всех участников цифрового сообщества. Мы должны постоянно совершенствовать меры безопасности, обучать пользователей и сотрудничать в борьбе с киберпреступностью. Только так мы сможем обеспечить безопасность в сети и сохранить конфиденциальность

информации в эпоху цифровизации.

Литература:

1. Алексеевна, С. Л. Принципы функционирования модели интегрированной отраслевой ису сектором национальной кибербезопасности / С. Л. Алексеевна // . – 2020. – № 3-1(59). – С. 75-85. – EDN FQDDZO.
2. Безделов, А. Д. Инновационные формы управления и кибербезопасность безналичных расчетов в условиях цифровизации банковской экосистемы / А. Д. Безделов, Е. В. Логинова // Научные исследования и разработки. Экономика фирмы. – 2020. – Т. 9, № 3. – С. 25-31. – DOI 10.12737/2306-627X-2020-25-31. – EDN NAUDDS.
3. Гулак, А. М. О влиянии GDPR на состояние кибербезопасности в Великобритании / А. М. Гулак // Матрица научного познания. – 2022. – № 6-1. – С. 45-47. – EDN ADNMHX.
4. Гулак, А. М. О влиянии GDPR на состояние кибербезопасности в Великобритании / А. М. Гулак // Матрица научного познания. – 2022. – № 6-1. – С. 45-47. – EDN ADNMHX.
5. Демироглу, Н. Б. Автоматизация бизнес-процессов как условие эффективности малого бизнеса / Н. Б. Демироглу // Вестник Алтайской академии экономики и права. – 2020. – № 11-2. – С. 212-216. – DOI 10.17513/vaael.1413. – EDN BWQRWV.
6. Ерыгин, Д. В. Цифровизация как инструмент социально-экономического развития / Д. В. Ерыгин, Е. С. Куликова // Приоритетные направления инновационной деятельности в промышленности : Сборник научных статей IV международной научной конференции, Казань, 29–30 апреля 2021 года. Том Часть 1. – Казань: Общество с ограниченной ответственностью "КОНВЕРТ", 2021. – С. 214-215. – EDN HTZKPI.
7. Мийзамов, А. А. Актуальные вопросы кибербезопасности / А. А. Мийзамов, В. М. Енин, И. А. Матющенко // International Journal of Advanced Studies in Computer Engineering. – 2021. – № 1. – С. 17-21. – EDN SPMATC.

8. Сулимин, В. В. Риски развития цифровой экономики / В. В. Сулимин, А. В. Голубева // Мир в эпоху глобализации экономики и правовой сферы: роль биотехнологий и цифровых технологий : Сборник научных статей по итогам VIII международной научно-практической конференции, Москва, 15–16 августа 2021 года. – Москва: Общество с ограниченной ответственностью "КОНВЕРТ", 2021. – С. 47-48. – EDN YOGSUO.
9. Халниязова, Д. С. Проблемы обеспечения кибербезопасности при осуществлении банковской деятельности / Д. С. Халниязова // Теория права и межгосударственных отношений. – 2022. – Т. 1, № 5(25). – С. 233-239. – EDN DWZDRZ.

References

1. Alekseevna, S. L. Principy funkcionirovaniya modeli integrirovannoj otraslevoj isu sektorom nacional'noj kiberbezopasnosti / S. L. Alekseevna // . – 2020. – № 3-1(59). – S. 75-85. – EDN FQDDZO.
2. Bezdelov, A. D. Innovacionnye formy upravleniya i kiberbezopasnost' beznalichnyh raschetov v usloviyah cifrovizacii bankovskoj ekosistemy / A. D. Bezdelov, E. V. Loginova // Nauchnye issledovaniya i razrabotki. Ekonomika firmy. – 2020. – T. 9, № 3. – S. 25-31. – DOI 10.12737/2306-627X-2020-25-31. – EDN NAUDDS.
3. Gulak, A. M. O vliyanii GDPR na sostoyanie kiberbezopasnosti v Velikobritanii / A. M. Gulak // Matrica nauchnogo poznaniya. – 2022. – № 6-1. – S. 45-47. – EDN ADNMHX.
4. Gulak, A. M. O vliyanii GDPR na sostoyanie kiberbezopasnosti v Velikobritanii / A. M. Gulak // Matrica nauchnogo poznaniya. – 2022. – № 6-1. – S. 45-47. – EDN ADNMHX.
5. Demiroglu, N. B. Avtomatizaciya biznes-processov kak uslovie effektivnosti malogo biznesa / N. B. Demiroglu // Vestnik Altajskoj akademii ekonomiki i prava. – 2020. – № 11-2. – S. 212-216. – DOI 10.17513/vaael.1413. – EDN BWQRWV.

6. Erygin, D. V. Cifrovizaciya kak instrument social'no-ekonomicheskogo razvitiya / D. V. Erygin, E. S. Kulikova // Prioritetnye napravleniya innovacionnoj deyatel'nosti v promyshlennosti : Sbornik nauchnyh statej IV mezhdunarodnoj nauchnoj konferencii, Kazan', 29–30 aprelya 2021 goda. Tom CHast' 1. – Kazan': Obshchestvo s ogranichennoj otvetstvennost'yu "KONVERT", 2021. – S. 214-215. – EDN HTZKPI.
7. Mijzamov, A. A. Aktual'nye voprosy kiberbezopasnosti / A. A. Mijzamov, V. M. Enin, I. A. Matyushchenko // International Journal of Advanced Studies in Computer Engineering. – 2021. – № 1. – S. 17-21. – EDN SPMATC.
8. Sulimin, V. V. Riski razvitiya cifrovoj ekonomiki / V. V. Sulimin, A. V. Golubeva // Mir v epohu globalizacii ekonomiki i pravovoj sfery: rol' biotekhnologij i cifrovyh tekhnologij : Sbornik nauchnyh statej po itogam VIII mezhdunarodnoj nauchno-prakticheskoj konferencii, Moskva, 15–16 avgusta 2021 goda. – Moskva: Obshchestvo s ogranichennoj otvetstvennost'yu "KONVERT", 2021. – S. 47-48. – EDN YOGSUO.
9. Halniyazova, D. S. Problemy obespecheniya kiberbezopasnosti pri osushchestvlenii bankovskoj deyatel'nosti / D. S. Halniyazova // Teoriya prava i mezhgosudarstvennyh otnoshenij. – 2022. – T. 1, № 5(25). – S. 233-239. – EDN DWZDRZ.

Для цитирования: Назарова А.Д., Шведов В.В. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации // Научный сетевой журнал «Столыпинский вестник» № 5/2023