УДК 004.056.5

БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ЭПОХУ ЦИФРОВИЗАЦИИ

А. С. Наумик[1)], Т. Д. Юрковец[2)]

[1)] *студент факультета экономики и управления, Гродненский государственный университет им. Янки Купалы, г. Гродно, Республика Беларусь, e-mail: naumikanna2@gmail.com*
[2)] *студент факультета экономики и управления, Гродненский государственный университет им. Янки Купалы, г. Гродно, Республика Беларусь, e-mail: taniau-2901@mail.ru*

Научный руководитель: **Е. В. Михолап**

магистр экономических наук, преподаватель кафедры экономики и управления на предприятии, Гродненский государственный университет имени Янки Купалы, г. Гродно, Республика Беларусь, e-mail: elizaveta.miholap@mail.ru

С каждым годом возрастает уровень угроз со стороны хакеров в связи с ростом их навыков и появлению новых путей взлома систем. Традиционная профилактика и устранение последствий ИТ-взломов остаются критически важными видами деятельности, но осведомленность и обучение сотрудников не менее важны. Организациям необходимо разрабатывать и внедрять новые стратегии управления и руководства информационной безопасностью, начиная с профилактики, обнаружения, управления устранением последствий взломов. Целью является объяснение важности об информировании сотрудников об ИТ-безопасности; об использовании новых систем защиты информации; о предотвращении ИТ-взломов при помощи поиска информации в Интернете и темной паутине.

Ключевые слова: ИТ-безопасность; защита информации; хакеры; системы защиты.

INFORMATION SECURITY AND PROTECTION IN THE ERA OF DIGITALIZATION

A. S. Naumik[1)], T. D. Yurkovets[2)]

[1)] *students of the faculty of economics and management, Grodno State University named after Yanka Kupala, Grodno, Republic of Belarus, e-mail: naumikanna2@gmail.com*
[2)] *students of the faculty of economics and management, Grodno State University named after Yanka Kupala, Grodno, Republic of Belarus, e-mail: taniau-2901@mail.ru,*

Academic supervisor: **E. V. Mikholap**

MA in economics, lecturer of the department of economics and management at the enterprise, Grodno State University named after Yanka Kupala, Grodno, Republic of Belarus, e-mail: elizaveta.miholap@mail.ru

Threats from hackers increase every year due to their growing skills and the emergence of new ways to break into systems. Traditional IT hacking prevention and remediation remain critical activities, but employee awareness and training are just as important. Organizations need to develop and implement new information security management and governance strategies, starting with hack prevention, detection, and remediation management. The goal is to explain the importance of educating employees about IT security; using new information security systems; and preventing IT hacks by searching the Internet and the dark web.

Keywords: IT security; information protection; hackers; protection systems.

Угрозы информационной безопасности организаций возрастают под воздействием ряда факторов: рост числа устройств, подключенных к сети, увеличение числа взаимодействий между работниками и устройствами, а также усиление профессионального уровня атак безопасности.

Массово распространились атаки с использованием социальной инженерии, и они становятся все умнее и умнее. Кроме того, наблюдается массовое распространение мобильных устройств, которые все чаще используются как в личной жизни, так и в бизнесе. Все это создает огромную проблему в сфере ИТ-безопасности.

Если хакеры захотят проникнуть в сеть организации, они смогут это сделать – вопрос лишь в том, сколько усилий и времени он приложит.

Нужно пересмотреть приоритеты в области безопасности, чтобы больше внимания уделять обнаружению и реагированию, а не только предотвращению.

Стратегии ИТ-безопасности:

- Наличие хорошей и современной защиты от вирусов, потому что она предотвращает 90 процентов атак.

- Повысить осведомленность сотрудников о рисках, связанных с ИТ-безопасностью. Это требует правильной методологии, ресурсов, интеграций в обучение и практику.

- Раннее обнаружение планов на взлом системы организации (находить информацию в Интернете и темной паутине, на сайтах с обсуждениями).

ИТ-специалисты обычно могут заметить, что в их сети происходит что-то ненормальное, но характер атак изменился и теперь ИТ-отдел может проработать 200–250 дней, не имея ни малейшего представления о том, что в сети кто-то есть. Именно здесь требуется другой механизм для обнаружения активности в сети.

Ранее ИТ-безопасность составляла 99 % информационной безопасности, сейчас это около 60 %. Поэтому необходимо защищать информацию в системе, способствовать образованию и осведомленности персонала, а также предотвращать вторжения и утечки [1].

В некоторых отраслях, таких как финансовые услуги и здравоохранение, организации более жестко регулируются из-за огромных объемов персональных данных и конфиденциальных данных, которыми они владеют. Это делает эти отрасли главной мишенью для хакеров.

Данные, которые эти организации хранят, требуют инвестиций в обучение персонала и технологии по защите информации, что еще больше усложняет задачи по защите данных [2].

За последние несколько лет в секторе финансовых услуг произошел резкий рост инновационных технологий, и, несмотря на стремление к конфиденциальности, кажется, что существует нехватка цифровых решений.

Таким образом, в современную эпоху цифровизации следует уделять внимание не только на сами системы защиты данных и на устранение последствий утечки информации, используя опыт и заполняя пробелы в системах, но и на информирование и обучение самих сотрудников организации, клиентов и поставщиков [3].

Библиографические ссылки

1. Cyber/Information Security in the Digital Age [Электронный ресурс]. – URL: https://digitalstrategies.tuck.dartmouth.edu/wp-content/uploads/2017/10/Cyber-Info-Security-in-the-Digital-Age-Roundtable-Overview.pdf (дата обращения: 08.10.2022).

2. Why Data Security and Privacy in the digital age are crucial [Электронный ресурс]. – URL: https://www.imperva.com/blog/why-data-security-and-privacy-in-the-digital-age-are-crucial/ (дата обращения: 08.10.2022).

3. Угрозы информационной безопасности [Электронный ресурс]. – URL: https://www.anti-malware.ru/threats/information-security-threats (дата обращения: 08.10.2022).