ХАЧИДОГОВ Руслан Асланович,

майор полиции, старший преподаватель кафедры огневой подготовки Северо-Кавказского института повышения квалификации,

e-mail: mail@law-books.ru

КИБЕРБЕЗОПАСНОСТЬ: БОРЬБА С ВНЕШНИМИ И ВНУТРЕННИМИ УГРОЗАМИ

Аннотация. *Рассмотрение, анализ и определение путей решения вопросов, связанных с обеспечением кибербезопасности и предупреждением киберпреступлений. Методология исследования – философских, общенаучных и специально-юридических средств и способов познания, обеспечивающих объективность изучения заданной тематики. В результате обосновано отметить, что год за годом в мире становится все больше угроз и происходит все больше утечек данных. Растущие усилия правоохранительных органов и следователей не могут сдержать угрозу вымогательских операций в Интернете. Число жертв увеличивается, а новые киберпреступные группы проявляют высокую мотивацию к достижению своих вредоносных целей. Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина – действия преступников.*

Ключевые слова: *кибербезопасность, киберпреступность, противодействие, обеспечение, предупреждение.*

KHACHIDOGOV Ruslan Aslanovich,

Major of Police, Senior Lecturer at the Department of Fire Training of the North Caucasus Institute for Advanced Studies

CYBERSECURITY: DEALING WITH EXTERNAL AND INTERNAL THREATS

Annotation. *Review, analyze and identify ways to address cybersecurity and cybercrime prevention issues. Research methodology - philosophical, general scientific and special legal means and methods of cognition that ensure objectivity in the study of a given topic. As a result, it is reasonable to note that year after year there are more and more threats in the world and more and more data leaks occur. Growing efforts by law enforcement agencies and investigators are failing to contain the threat of online extortion operations. The number of victims is increasing, and new cybercrime groups are highly motivated to achieve their malicious goals. Most often, medical and government institutions or organizations from the retail sector are subject to data leaks. In most cases, the reason is the actions of criminals. Some organizations attract attackers for a good reason—financial and medical data can be stolen.*

Key words: *cybersecurity, cybercrime, counteraction, provision, prevention.*

Информационная безопасность защищает данные, которые могут храниться как в цифровом виде, так и на бумажных носителях. Специалисты по информационной безопасности борются с внешними и внутренними угрозами. Например, предотвращают последствия случайного изменения данных или нарушений работы системы из-за технических сбоев.

Кибербезопасность относится к защите только цифровой информации и в основном от угроз извне - из интернет-сетей [1].

Кибербезопасность борется с тремя видами угроз, среди которых:

Киберпреступление - действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

Кибератака - действия, нацеленные на сбор информации, в основном политического характера.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы –

ниже мы приводим самые распространенные [2]

Вредоносное программное обеспечение (далее ПО). Вредоносное ПО может быть самым разным, вот некоторые распространенные виды: вирусы, троянцы, шпионское, рекламное, ботнеты, SQL-инъекция, фишинг, атаки, man-in-the-middle, DoS-атаки, троянец Dridex, мошенничество на сайтах и в приложениях для знакомств, Emotet [3].

Противостоять киберугрозам помогают технологии защиты информации, например антивирусные программы, криптографические методы шифрования данных, брандмауэры и программы для выявления подозрительной активности вроде EDR и IDS-систем.

Пользователи могут защитить свои персональные данные от киберугроз в сети интернет, если будут соблюдать правила кибербезопасности. Перечислим основные:

- Использовать разные и сложные пароли для аккаунтов и устройств. Сложными считаются пароли, которые состоят из букв, цифр и знаков препинания. Их тяжело угадать, а подбирать — долго.
- Включить двухфакторную аутентификацию для доступа к аккаунтам.
- Использовать лицензионные антивирусные программы и регулярно запускать сканирование устройства.
- Не переходить по подозрительным ссылкам на веб-страницах и не скачивать файлы из непроверенных интернет-ресурсов, электронных писем или сообщений в мессенджере от незнакомых отправителей.
- Не переходить по ссылкам из SMS-сообщений, которые пришли без запроса. Например, SMS-сообщение со ссылкой для восстановления доступа к аккаунту на сайте или соцсети.
- Проверять адрес отправителя электронного письма, прежде чем переходить по ссылкам из него, чтобы не стать жертвой фишинга.
- Использовать VPN при подключении к Wi-Fi сети в общественных местах вроде кафе и поездов.
- Отключать Bluetooth, когда он не используется. Не принимать запросы на подключение от незнакомых людей.
- Настроить резервное копирование данных, чтобы восстановить их в случае пропажи.
- Не игнорировать доступные обновления систем и браузеров. В них обычно исправляют обнаруженные проблемы кибербезопасности.

Киберугрозы постоянно присутствовали в жизни человечества все 50 лет технологических изменений. С появлением интернета и цифровой трансформации понятие кибербезопасности стало привычным в профессиональной и личной жизни. После распространения вирусов в 1990-х годах, 2000-е годы ознаменовались институционализацией киберугроз и кибербезопасности, которую сегодня изучают в школах и институтах.

Кибербезопасность – это практика защиты критически важных систем и конфиденциальной информации от цифровых атак. Меры кибербезопасности, известные как безопасность информационных технологий, предназначены для борьбы с угрозами [4] в отношении сетевых систем и приложений, независимо от того, исходят ли эти угрозы из организации или извне.

Развитие цифровых технологий привело к появлению большого количества цифровых угроз в интернете. Например, кража персональных данных пользователей или атаки хакеров на информационные системы компании с целью вывести их из строя. В ответ на угрозы появилась область знаний, которая занимается разработкой и внедрением технологий защиты информационных систем от них, - кибербезопасность. Специалисты по кибербезопасности изучают преступления и угрозы в цифровой среде и разрабатывают способы противостоять им.

Список литературы:

[1] Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: автореферат диссертации на соискание ученой степени к.ю.н. / Н.С. Зиновьева. – Краснодар: Краснодарский университет МВД России, 2021.

[2] Михайленко Е.В. Введение в программирование: учебное пособие / Е.В. Михайленко. - Краснодар: Краснодарский университет МВД России, 2020.

[3] Правовая защита информации: учебное пособие / сост. В.Н. Цимбал. – Краснодар: Краснодарский университет МВД России, 2020.

[4] Машекуашева М.Х. Некоторые аспекты использования в преступных целях искусственного интеллекта. Право и управление. 2024. № 8. С. 376-378.

Spisok literatury:

[1] Zinovieva N.S. Computer information transformed by cryptographic methods in solving and investigating crimes: abstract of a dissertation for the degree of Ph.D./N.S. Zinovieva. - Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia, 2021.

[2] E.V. Mikhailenko. Introduction to programming: a textbook/E.V. Mikhailenko. - Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia, 2020.

[3] Legal protection of information: tutorial/comp. V.N. Tsimbal. - Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia, 2020.

[4] Mashekuasheva M.Kh. Some aspects of the use of artificial intelligence for criminal purposes. Law and governance. 2024. № 8. S. 376-378.