ВЫХОДНЫЕ ДАННЫЕ СТАТЬИ: ДЕМБРОВСКИЙ Н.Ю. КИБЕРБЕЗОПАСНОСТЬ: ОСНОВНЫЕ УГРОЗЫ И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ / Н.Ю. ДЕМБРОВСКИЙ // МОЛОДОЙ ИССЛЕДОВАТЕЛЬ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ: СБ. СТ. ПО МАТЕРИАЛАМ CCCLXIX МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «МОЛОДОЙ ИССЛЕДОВАТЕЛЬ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ». – № 31(369). – М., ИЗД. «ИНТЕРНАУКА», 2024.

СТАТУС: ПОДГОТАВЛИВАЕТСЯ К ИЗДАНИЮ.

КИБЕРБЕЗОПАСНОСТЬ: ОСНОВНЫЕ УГРОЗЫ И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Дембровский Николай Юрьевич
студент, Владивостокский государственный университет,
Россия, г. Владивосток

Кибербезопасность является одной из самых актуальных и обсуждаемых вопросов в современном мире. В связи с быстрым развитием информационных и цифровых технологий по всем сферам деятельности увеличивается и угроза информационной безопасности пользователя в режиме онлайн.

Кибербезопасность - это практика защиты сетей, устройств, приложений, систем и данных от киберугроз. Общая цель заключается в предотвращении атак, которые пытаются получить доступ к данным или уничтожить их, вымогать деньги или нарушать нормальные бизнес-операции, будь то внутри организации или за ее пределами [1]. С развитием интернета все больше хранится и передается информации через сеть. Именно это дает возможность киберпреступникам или хакерам завладеть личной информацией пользователя и использовать против него. Также опасность грозит и компаниям, у которых слабая система информационной безопасности. Хакер - человек, превосходно разбирающийся в устройстве и функционировании вычислительных систем, умеющий быстро найти и элегантно устранить ошибки в их работе [2].

Основными угрозами в сфере кибербезопасности являются чаще всего вирусы или троянские программы, которые могут заразить компьютер для того, чтобы украсть личную или конфиденциальную информацию. Также существуют и рэнсомверы, они предназначены для блокировки доступа к необходимым данным и требуют выкуп за разблокировку. Чаще всего, в мире кибербезопасности, принято называть мошеннические попытки фишингом, с помощью которых хакеры пытаются получить личную информацию пользователя. Есть еще один способ мошенничества, с которым люди очень часто сталкиваются, особенно сильная опасность грозит детям и пенсионерам. Такой способ осуществляется с помощью звонков на обычный телефон, где

мошенники могут представляться государственными организациями, например, банком и запросить личные данные вашей карты. По статистике на такие уловки ведутся пожилые люди, которые только осваиваются с новыми цифровыми технологиями и часто доверяют таким звонкам, и дети, которые вовсе могут не понимать или не придавать значения звонку и сделать то, что скажет посторонний человек по телефону.

Чтобы понимать, как работает кибербезопасность, необходимо построить структуру с основными этапами. Данная структура представлена на рисунке 1. Первым этапом предотвращения угроз личной информации является идентификация, где рассчитываются все риски и происходит управления активами. Далее осуществляются защита информации, используя защитные технологии, контроль доступа и т.д. После идет постоянный мониторинг безопасности и обнаруживаются какие-либо угрозы и риски. Далее происходит анализ угрозы, улучшение системы. Заключительным этапом является восстановление, во время которого происходит постоянное улучшение всех информационных технологий, которые были или могут подвергаться различным угрозам.

Рисунок 1. Структура кибербезопасности

Для предотвращения угроз информационной безопасности существуют несколько способов. Первым является обновление программного обеспечения

на всех устройствах. ПО - это совокупность программ на компьютере или другом устройстве. Еще так называют сами программы [3]. Второй способ заключается в использовании сложной двухфакторной аутентификацией для защиты конфиденциальности данных. Также в компаниях используются специальные ПО, которые обнаруживают все угрозы и своевременно их предотвращает.

Кибербезопасность является одной из важных тем в информационном обществе, так как от безопасности информации зависит работоспособность всех цифровых технологий и систем. Необходимо регулярно развивать навыки сотрудникам по борьбе с киберпреступниками, чтобы эффективно и быстро предотвращать и уничтожать все киберугрозы, так как с каждым днем появляются новые кибератаки, которые могут значительно повредить систему компании или нести угрозу обычным пользователям.

Список литературы:

1. Что такое кибербезопасность? [Электронный ресурс]. – Режим доступа: https://www.sap.com/central-asia-caucasus/products/financial-management/what-is-cybersecurity.html (дата обращения: 28.07.24)
2. Хакер [Электронный ресурс]. – Режим доступа: https://blog.skillfactory.ru/glossary/haker/ (дата обращения: 28.07.24)
3. Программное обеспечение [Электронный ресурс]. – Режим доступа: https://blog.skillfactory.ru/glossary/programmnoe-obespechenie/ (дата обращения: 28.07.24)