УДК 621.762.4

Безопасное использование компьютерных сетей

Бабицкая Э. С., студент,
Каминская И. В., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: канд. техн. наук, доцент Дробыш А. А.

Аннотация:
В статье представлены основные понятия и виды компьютерных сетей. Так же рассмотрены часто встречаемые виды киберугроз, правила как безопаснее использовать глобальную сеть Интернет. Тема достаточная актуальна на данный момент, так как появилось очень много продвинутых мошенников, которые шифруют вредоносные угрозы на различных сайтах, впоследствии которых многие пользователи теряют свои персональные данные.

Сеть – это совокупность объектов, имеющих определенные общие признаки и определенным образом связанных между собой.

Компьютерные сети – это совокупность компьютеров, объединенных каналами связи и обеспеченных коммуникационным оборудованием и программным обеспечением для совместного использования данных и оборудования [1].

Рассмотрим основные виды компьютерных сетей:

– локальные (Local Area Network – LAN) – сосредоточенные на территории радиусом не более 1–2 км, локальные компьютерные сети построены с использованием дорогих высококачественных линий связи, позволяющих достигать высоких скоростей обмена данными порядка 10000 Мбит/с, данные передаются в цифровом формате;

– глобальные (Wide Area Network – WAN) – объединяют компьютеры, рассредоточенные на расстоянии 100 и 1000 км. Более низкие, чем в локальных сетях, скорости передачи данных (единицы и десятки мегабит в секунду);

– беспроводные локальные (Wireless Local Area Network – WLAN);

– локальные сети на основе технологии беспроводной связи Wi-Fi. Такая сеть связывает два или более устройств с помощью беспроводной связи для формирования локальной сети (LAN) в пределах

ограниченной области, например дома, в университете, в учебном заведении или общественном здание и т. д.;

– региональные (Metropolitan Area Network – MAN) – при достаточно больших расстояниях между узлами (десятки километров) они качественные линии связи и достигают высоких скоростей обмена, иногда даже более высоких, чем в классических локальных сетях;

– персональные (Personal Area Network – PAN) – объединяет персональное электронное оборудование пользователя (телефоны, ноутбуки, карманные персональные компьютеры и т. д.) преимущественно через беспроводную связь Bluetooth или Wi-Fi, предусматривает ограниченное количество абонентов (до 8 участников) и небольшой радиус действия (до 30 м);

– нательная компьютерная сеть (Body Area Network – BAN) - объединяет надеваемые или имплантированные компьютерные устройства, такие как умные часы, мониторы давления и т. п. [1].

Безопасность – это защита устройств от угроз, которые преступники могут спрятать (зашифровать) в программах/сайтах/приложениях.

Безопасность компьютерных сетей (кибербезопасность) – это действие по защите компьютерных сетей от различных угроз.

Мы рассмотрим подробно безопасность в глобальной компьютерной сети Интернет.

Интернет – это глобальная компьютерная сеть, объединяющая миллионы компьютеров в единую информационную систему [2].

Чтобы сохранить конфиденциальность пользователя и безопасность в интернете, важно знать о различных типах интернет-атак:

1. Фишинг – это кибератака с использованием поддельных писем. Злоумышленники пытаются обмануть получателей электронной почты, убедив их в подлинности и актуальности сообщения. Например, они маскируют письма под запросы из банка или сообщения от друзей, чтобы пользователи переходили по ссылкам. Цель атаки состоит в том, чтобы обманным путем заставить пользователей раскрыть личную информацию или загрузить вредоносные программы.

2. Взлом и удаленный доступ. Злоумышленники используют уязвимости частной сети или системы для кражи конфиденциальной информации и данных. Технология удаленного доступа предоставляет им дополнительные возможности. Программное обеспечение для удаленного доступа позволяет пользователям получать доступ к ком-

пьютеру и управлять им удаленно. Протокол, позволяющий пользователям удаленно управлять компьютером, подключенным к интернету, называется RDP. Злоумышленники используют различные методы выявления и эксплуатации уязвимостей RDP, чтобы получить полный доступ к сети и ее устройствам.

3. Вредоносные программы и вредоносная реклама. Вредоносные программы – это все вирусы, трояны и т. д., которые злоумышленники используют для нанесения ущерба и кражи конфиденциальной информации. Любое программное обеспечение, предназначенное для повреждения компьютера, сервера или сети, может расцениваться как вредоносное. Вредоносная реклама – это онлайн-реклама, которая распространяет вредоносные программы. Интернет-реклама – это сложная экосистема, включающая веб-сайты рекламодателей, рекламные биржи, рекламные серверы, сети ретаргетинга и сети доставки контента. Злоумышленники используют эту сложность для размещения вредоносного кода там, где рекламодатели и рекламные сети не всегда могут его обнаружить. Пользователи, взаимодействующие с вредоносной рекламой, могут загрузить вредоносные программы на свое устройство или перейти на вредоносные веб-сайты.

4. Ботнеты – сеть компьютеров, специально зараженных вредоносным ПО с целью выполнения автоматических задач в интернете без разрешения владельцев этих компьютеров.

5. Опасности в публичных и домашних сетях Wi-Fi. Использование публичных сетей Wi-Fi сопряжено с рисками, поскольку уровень безопасности в таких местах низкий или защита полностью отсутствует. Это позволяет киберпреступникам просто отслеживать действия пользователей в интернете и красть их пароли, личную информацию. Также есть опасность прослушивания сети, взламывания точки доступа с перехватом данных и точка доступа в виде обманки для сбора личных данных [3].

Существует достаточное множество угроз и вредоносных программ, но как же все-таки защитить свои данные. Предложу несколько советов:

1. Обновите ПО и ОС. Используя новое ПО, вы получаете улучшенную систему безопасности.

2. Используйте антивирусные программы. Необходимо иметь на каждом устройстве антивирусник, т. к. он автоматически будет следить за безопасности вашего устройства, а также при скачивании какого-либо продукта, он будет оповещать вас при нахождении вредоносных носителей.

3. Используйте надежные пароли. Не применяйте комбинации, которые легко подобрать или угадать, а также не используйте одинаковый пароль на всех программах, так как вас очень легко будет взломать и украсть личную информацию.

4. Не открывайте почтовые вложения от неизвестных отправителей, так как они могут быть заражены вредоносным ПО.

5. Не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов. Это один из стандартных путей распространения вредоносного ПО.

6. Избегайте незащищенных сетей Wi-Fi в общественных местах. Так как в них вы сильно уязвимы.

Из-за большого количества кибератак/угроз, и частого использования сети Интернет, у человека могут очень быстро и легко украсть его личные данные. Поскольку большое количество информации мы храним на наших устройствах. Чтобы избежать этого рекомендуется следовать советам по безопасному использованию представленных в статье.

Список использованных источников

1. Компьютерные сети [Электронный ресурс] // www.polnaja-jenciklopedija.ru – 2019 – Режим доступа: https://www.polnaja-jenciklopedija.ru/nauka-i-tehnika/kompyuternye-seti.html – Дата доступа: 19.03.2022.

2. Глобальная компьютерная сеть Интернет [Электронный ресурс] // www.polnaja-jenciklopedija.ru – 2018 – Режим доступа: https: //www.polnaja-jenciklopedija.ru/nauka-i-tehnika/globalnaya kompyuternaya-set-internet.html – Дата доступа: 19.03.2022.

3. Что такое кибербезопасность? [Электронный ресурс] // www.kaspersky – 2021 – Режим доступа: https://www.kaspersky. ru/resource-center/definitions/what-is-cyber-security – Дата доступа: 20.03.2022.