Отчет о прохождении курса Stepik

Дашкина Анита Тагировна

Содержание

1 Цель работы.....3

2 Выполнение работы.....4

3 Выводы.....6

1 Цель работы

Ознакомиться с основами кибер безопасности по нескольким пунктам, а именно:

1. Безопасность в сети
2. Защита ПК/Телефона
3. Криптография

2 Выполнение работы

1. Безопасность в сети

Безопасность в сети — это в первую очередь защита от хакеров, вирусов и мошенников, которые могут украсть ваши данные, деньги или личные файлы. Основные угрозы — это перехват паролей в публичных Wi-Fi сетях, фишинговые сайты, поддельные письма с просьбой ввести логин, а также вредоносные программы, скрытые в скачанных файлах. Чтобы обезопасить себя, используйте сложные пароли (не «123456»!) и двухфакторную аутентификацию, избегайте входа в важные аккаунты через открытые сети без VPN, проверяйте адреса сайтов (особенно банков и соцсетей) и установите антивирус. Если заметили подозрительную активность — сразу меняйте пароли, отключайте сомнительные приложения и сканируйте устройство. Главное правило: если что-то кажется странным (например, письмо «от банка» с ошибками или сайт с подозрительным адресом), лучше перепроверить — это может быть ловушка. Для более глубокого понимания основ кибербезопасности стоит пройти специализированные курсы, но даже эти простые меры значительно снизят риски.

2. Защита ПК/Телефона

Защита компьютера и телефона — это как установка надежных замков на цифровую дверь вашей жизни. Начните с антивируса — он как базовый щит от вирусов и троянов, причем даже бесплатные версии (типа Avast или Kaspersky Free) уже дают защиту. Не забывайте про обновления — они "латают дыры" в системе, через которые могут пролезть злоумышленники. Ставьте приложения только из официальных магазинов (Google Play, App Store) и внимательно читайте, какие права запрашивает программа (если фонарик просит доступ к вашим контактам — это повод насторожиться). Резервные копии — ваш спасательный круг: если телефон украдут или данные повредят вирусы, вы восстановите фото и документы из "облака" или с жесткого диска. Для особо важных данных используйте шифрование (например, встроенные функции BitLocker на Windows или FileVault на Mac). И главное — не кликайте на подозрительные ссылки, даже если их прислал "друг" (его аккаунт могли взломать). Эти простые правила сведут риски к минимуму без необходимости быть IT-экспертом.

3. Криптография

Криптография на практике — это не магия, а реальные инструменты для защиты данных. Всё просто: шифрование превращает ваши сообщения и файлы в "тарабарщину" для посторонних, а ключи (как пароли) позволяют только вам и получателю их расшифровать. Например, мессенджеры вроде WhatsApp используют сквозное шифрование — даже компания не может прочитать ваши сообщения. Для паролей применяйте хеширование (это "одностороннее" шифрование, чтобы даже взломанная база не раскрыла ваши пароли в чистом виде). Цифровые подписи подтверждают, что файл не подделан, а VPN и HTTPS шифруют интернет-соединение, защищая данные в пути. Главное правило: надёжные алгоритмы (AES, RSA) и секретные ключи — ваши лучшие друзья, а самодельные "шифры" из головы — рискованная игра. Даже базовые знания криптографии помогут избежать утечек и сохранить конфиденциальность.

4 Вывод

В результате выполнения работы этот курс научил, как защищаться от цифровых угроз в современном мире. Я узнал, что такое кибербезопасность и почему она важна для каждого. Раздел криптографии объяснит, как работают шифрование и цифровые подписи, чтобы ваши сообщения и данные оставались конфиденциальными. В части защиты сетей расскажут, как безопасно пользоваться Wi-Fi, распознавать фишинг и защищаться от хакерских атак с помощью VPN и фаерволов. Веб-безопасность научит избегать опасных сайтов и защищать свои аккаунты от взлома. Раздел защиты ПК и телефонов даст практические советы: ставить антивирусы, вовремя обновлять программы и не качать подозрительные файлы. Вы поймете, как социальная инженерия манипулирует людьми (например, через фальшивые звонки "из банка"), и научитесь не попадаться на уловки мошенников. Если что-то пошло не так, раздел реагирования на инциденты подскажет, как действовать при утечке данных или заражении вирусом. Курс также затрагивает законы о персональных данных и этические вопросы — чтобы вы не только защищали себя, но и не нарушали чужие права. Главный вывод: безопасность начинается с простых шагов — сложных паролей, критического мышления и базовых цифровых привычек.