Государственное автономное образовательное учреждение
«БАЛАШОВСКИЙ ТЕХНИКУМ МЕХАНИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА»

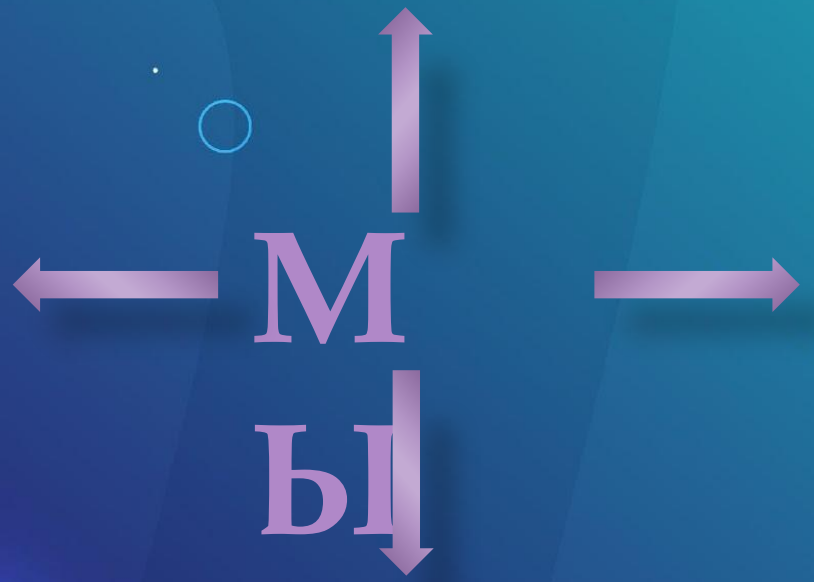
Выполнил студент 3 курса
Специальности 09.02.07
Информационные системы и программирование
Давыдов Алексей
Руководители: Судатова Ю.А, Жаворонкова

Балашов,

Интернет прочно вошел в нашу жизнь

Работаем

Учимся в интернете



Общаемся в интернете с друзьями

Организуем свой досуг

Возможности Глобальной сети безграничны ……

Но в Интернете как в реальной жизни присутствует много опасностей и, чтобы не попасть в неприятность

нужно соблюдать определенные правила безопасности.

ОТ НАС ХОТЯТ

- ✔ **Деньги** (платные подписки, обман при покупке/продаже, в переписке, благотворительность и т.д.).
- ✔ **Информация** (для подмены личности, атаки на вас, близких, для рекламы, слежки).
- ✔ **Эксплуатация устройства** (майнинг, DDoS-атаки, скрытая накрутка рекламы).

ГЛАВНАЯ ОПАСНОСТЬ ДЛЯ НАС

- ✔ Иметь слабые пароли.
- ✔ Заразить устройство вредоносной программой.
- ✔ Ввод пароля в поддельном окне.
- ✔ Отсутствие резервных копий.
- ✔ Доверие (без проверки).

ПАРОЛИ

81% вторжений хакеров связаны со слабыми или украденными паролями пользователей.

- ✔ Взлом почты — позволяет восстановить все пароли к привязанным аккаунтам.
- ✔ Взлом банковских приложений — лишает вас средств на счетах.
- ✔ Взлом гос. услуг — делает возможным **установить электронную подпись** и открывает доступ к полному перечню государственных услуг, например, переоформление недвижимости.
- ✔ Взлом соц.сетей — позволяет манипулировать близкими, заражать вирусами через посты и сообщения, похитить все файлы из переписок и т.д.
- ✔ Базы данных воруются, их методично расшифровывают и массово перебирают все аккаунты на популярных сайтах.

Ненадежные пароли делают бесполезной любую систему безопасности.

В современном мире не нужно запоминать все пароли — только один!

Хранение паролей:

- ✔ минимум 25 знаков на все пароли (сочетайте цифры, знаки и буквы разного РеГи
- ✔ пароль не должен включать в себя реально существующие слова или известные ф
- ✔ меняйте пароли обязательно — раз в 3 месяца;
- ✔ на "секретный вопрос" — давайте ложные ответы (но помните их!).

ПОЧТА

Почта — ключ ко всему!
Завладев вашей почтой, можно сбросить пароли вашего банка, гос. услуг или соцсетей и захватить аккаунты.

Опасные действия (к которым вас призывают письма мошенников):

- ✔ отправка данных;
- ✔ отправка денег;
- ✔ открытия вложения;
- ✔ установка приложения;
- ✔ переход по ссылки на сайт (сразу можно загрузить вредоносный код).

Создайте для себя домашнюю почту, рабочую, для сайтов, для мусора).
Не будет спама и риск взлома снизится.
Для удобства можно настроить пересылку всех писем на один из аккаунтов.
В идеале хорошо бы иметь и отдельный «мусорный» номер телефона.

БАНКОВСКАЯ КАРТА

Никому и никогда нельзя пересылать **фотографию** или **скан карты**.

- ✔ Зная номер карты, можно узнать Имя и Фамилию из соцсетей и подобрать механическим образом дату окончания действия карты. Теперь Интернет-магазины открыты для покупок.
- ✔ Заведите спец. карту с нулевым балансом только для получения переводов (в своём же банке).
- ✔ Установите **суточный лимит** по выводу и переводу средств (так вы обезопасите большую часть денег на счёте).
- ✔ Подключите **SMS-оповещение** о фактах списания (мошенники пользуются тем, что интернет-магазины позволяют делать покупки на небольшие суммы без кодового подтверждения по SMS, даже если подключена двухфакторная аутентификация).
- ✔ При списании средств без вашего ведома — успейте подать заявление в **первые сутки**!
- ✔ Там, где возможно, не оставляйте реквизиты карты (интернет-магазины, электронные кошельки).

При оплате онлайн покупок проверяйте подлинность платежного сайта.

WEB

Самые распространенные ошибки пользователей — лень и спешка. Эти две вещи, несомненно, ставят под удар нашу безопасность.

Признаки опасного сайта

- Опасным может быть абсолютно любой сайт. Покиньте сайт при появлении первых подозрений в подделки.
- Перед вводом своих данных на любом сайте — обязательно проверяйте его на подлинность (https://, внешний вид, сам адрес, пробив на фишинг).

Ссылки

- Каждая ссылка несёт потенциальную опасность.
- Нужно доверять только официальным сайтам (обращайте пристальное внимание на доменное имя (адрес сайта), если оно отличается — вас пытаются обмануть).

ПО

- Устанавливайте ПО только с официального сайта (адрес см. в Википедии) или у офиц. дистрибьютора (ссылка на загрузку сразу ведёт на скачивание файла, а не на файл-обменник или торрент).

Файлы

- При загрузке из Интернета музыки, видео, книг, документов — обязательно обращайте внимание на расширение (формат файла). Их открытие может привести к установке вредоносного ПО.

Браузер

- Расширения для браузера (они же плагины, приложения, утилиты) в магазине браузера — это программы, такие же, как и любые исполняемые файлы. Среди них часто выявляются вредоносные.

Облако

- Необходим надёжный пароль и особое внимание к ссылкам, которые вы раздаёте (настройка прав доступа к файлам). Проверяйте ссылки лично.

Торрент

- При любой возможности найдите какую-либо информацию без использования торрент-форумов и сайтов.
- Под видом файла .torrent вы можете скачать вредоносное ПО.
- С помощью файла .torrent вы можете скачать вредоносное ПО уже непосредственно через торрент-трекер.
- Если решились, то используйте торрент-программу только этих брендов и только на их официальном сайте (uTorrent, BitTorrent, BitComent, MediaGet).
- Выбирайте раздачу с наибольшим кол-вом сидов (пользователей, которые скачали весь файл до конца), читайте отзывы и комментарии под раздачей. Используйте сайты только с регистрацией (закрытые сообщества), там есть хоть какая-то административная проверка файлов.

СОЦСЕТИ

Потеря аккаунта
Открывает доступ ко всем ресурсам (где вы регистрировались с помощью соцсети).
Создаются зеркала (удаленная привязка и наблюдение). Регулярная смена пароля — хорошее средство от незаметного присутствия незнакомца.
От вашего имени **выпрашивают** деньги у ваших друзей, а потом стирают эти сообщения в переписки (вы даже не узнаете об этом).
Скачиваются моментально все **документы** из переписок (используют фильтр или спец. программу).
Логинятся от вашего имени на сомнительных сайта, не оставляя следов (DarkNet).
Меньше личной информации о себе
Не стоит публиковать
Номер своего телефона
Номера документов, любую **финансовую** информацию
Домашний адрес и когда вас нет дома.
Запрещенный контент (обнажёнка, призыв
к насилию, оскорбления)
Билеты на самолет.
Помните, что **любую информацию из ваших публикаций** могут использовать против вас.
Документы
Не используйте **мессенджер** соцсети для пересылки документов. Мошенники получат доступ ко всем документам, которые вы отправляли или получали от других людей.
Фото
Фото содержат **метаданные (**время и дата съемки, марка и модель фотокамеры) и, если на устройстве включена геолокация, то ещё указывается широта и долгота того места, где была снята фотография (отключите геолокацию).
Загрузка
При загрузке из социальной сети **музыки, видео, книг, документов** — обязательно обращайте внимание на расширение.
При загрузке любого файла обязательно проверяйте его антивирусом (даже от друзей и знакомых).
Существует две методики мошенничества
Угнать или **сымитировать аккаунт** реального человека (друга, коллеги, знакомого), обращаясь от его имени.
Втереться в доверие под видом незнакомого персонажа (организатора лотереи, матери больного ребенка и так далее).
Общие правила
Критически относитесь к любым **неожиданным** письмам и сообщениям — как от знакомых, так и от незнакомых людей.
Если призыв к действиям выглядит правдоподобно — свяжитесь с источником по другому каналу. Если просьба настоящая, уточняющий звонок никого не обидеть.
Вводите пароль от соцсети только на сайте и в приложении.
Всё, что попадает в Сеть — остаётся там навсегда!

БЕЗОПАСНОСТЬ КОМПЬЮТЕРА

- Физический доступ
Установите сложный пароль на компьютере. Никто не сможет получить доступ к документам, фотографиям, проектам, паролям из браузера, установить следящее ПО, отформатировать жесткий диск или ваш ребенок случайно не сможет удалить папку и т.д. А ещё ноутбук можно потерять или его украдут.
Антивирус
Регулярно обновляйте операционную систему (ОС) и браузер (то есть перезапускайте компьютер хотя бы раз в неделю).
Вредоносное ПО
Вредоносное ПО — главный враг вашего компьютера.
Любое отклонение от работы вашего компьютера — может быть признаком вредоносного ПО.
Абсолютное большинство вредоносных программ не может появиться на вашем компьютере без вашего участия. (Ваша задача вовремя распознать обман и остановиться).
USB-устройства
Отключите опцию **автозапуска** для всех носителей и устройств. Некоторые вирусы, особенно черви, распространяются автоматически.
Веб-камера и микрофон
Выключайте, прикрывайте или **заклеивайте веб-камеру**, когда не используете её.
Отключайте физически внешне подключаемую камеру, когда не используете (там встроенный микрофон).
Если вы заметили, что диод камеры мигнул хотя бы на несколько секунд — сразу же отключите Интернет, запустите антивирус (возможно следящее ПО). При выключенной камере он не должен ни гореть, ни мигать ни при каких обстоятельствах.
Отключите микрофон в меню настроек ОС (Диспетчер устройств - Звуковые, игровые и видеоустройства - Микрофон - Драйвер или правой кнопкой мыши "Отключить").
Отключите микрофон — вставьте любой обрезанный штекер в гнездо микрофона.
Резервное копирование
Регулярно делайте резервные копии важной информации (ПК можно залить водой, забыть, его могут зашифровать, украсть).

БЕЗОПАСНОСТЬ МОБИЛЬНОГО УСТРОЙСТВА

Файлы

Никогда **не открывайте файлы**, приложенные к сообщениям (которых вы не ждёте).

Нужно помнить, что **расширение исполняемых программ** для Android - .apk, а для iOS - .ipa.

Никогда не загружайте исполняемые файлы ни из каких сообщений.

Приложения

Загружайте только из официальных магазинов приложений.

Если приложение в официальном магазине платное — никаких бесплатных версий где-либо ещё быть не может (мошенничество).

В App Store и Google Play проникает вредоносное ПО.

Странные разрешения — ещё один признак подозрительного приложения (Контакты для фонарика).

Обновляйте систему и браузер как можно скорее (закрываются лазейки). Чем современнее ПО и браузер, тем выше уровень вашей защиты. Не игнорируйте уведомления или делайте все вручную, просто перезагружая телефон.

Отключайте Bluetooth, когда не используете его.

USB-устройства

Не используйте смартфон в качестве USB-носителя (можно заразить вредоносным ПО или самим стать носителем).

Резервное копирование

Регулярно создавайте резервные копии данных на смартфоне (особенно если используете устройство для работы или храните на нём важные документы или файлы). Могут зашифровать, украсть или просто разбить.

Настройте удаленный доступ к устройству на случай его потери или кражи, включите геолокацию (можно отследить местоположение, заблокировать устройство, стереть все данные или вывести на экран контактную информацию; можно включить автодозвон — устройство будет звонить регулярно и максимально громко, даже на беззвучном режиме).

Остерегайтесь фишинга по телефону

10 ЗАКОНОВ БЕЗОПАСНОСТИ (от Microsoft)

- Закон №1. Если вы запустили на своем компьютере **приложение злоумышленника**, это больше не ваш компьютер.
- Закон №2. Если злоумышленник внес **изменения в операционную систему** вашего компьютера, это больше не ваш компьютер.
- Закон №3. Если у злоумышленника есть неограниченный **физический доступ** к вашему компьютеру, это больше не ваш компьютер.

Закон №4. Если злоумышленник смог загрузить **приложения на ваш сайт**, это больше не ваш сайт.
Закон №5. **Ненадежные пароли** делают бесполезной любую систему безопасности.
Закон №6. Безопасность компьютера напрямую зависит от **надежности администратора**.

Закон №7. Безопасность зашифрованных данных напрямую зависит от того, насколько защищен **ключ расшифровки.**
Закон №8. Устаревшее **антивирусное приложение** лишь немногим лучше, чем его отсутствие.
Закон №9. Абсолютная **анонимность** недостижима ни в жизни, ни в Интернете.
Закон №10. **Технология** не является панацеей.

ЗАКЛЮЧЕНИЕ

- Мы можем заранее подумать о нашей информации и осознать, что, даже если наши действия кажутся нам безобидными, публикуя фотографию, забывая сменить пароли (установленные по умолчанию), используя рабочий телефон для совершения личного звонка или создавая учетную запись Facebook для наших маленьких детей, мы принимаем решения, последствия которых **будем ощущать ВСЮ ЖИЗНЬ**. Поэтому действовать нам следует, исходя из этих соображений.

~ Кевин Митник. Самый известный хакер на планете, а ныне самый востребованный специалист по кибербезопасности

СПАСИБО ЗА ВНИМАНИЕ