Частное профессиональное образовательное учреждение
«АНАПСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лекцию подготовил:
Омельченко И. Н.

Защита информации

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность (ИБ) - это комплекс мер и средств, направленных на защиту конфиденциальности, целостности и доступности информации

Утечка данных

Утечка данных – это получение доступа к конфиденциальной, личной или защищаемой информации лицом, не имеющим соответствующего разрешения.

К утечке данных могут привести следующие факторы:

технологические уязвимости

поведение пользователей





Взлом

Взлом - это несанкционированный доступ к вашим данным, устройствам или аккаунтам с целью получения выгоды, кражи информации, распространения вредоносного ПО или осуществления мошенничества

Как происходит взлом?

Взлом паролей

Заражение устройств вредоносными программами

Использование небезопасных беспроводных сетей

Обходные пути доступа

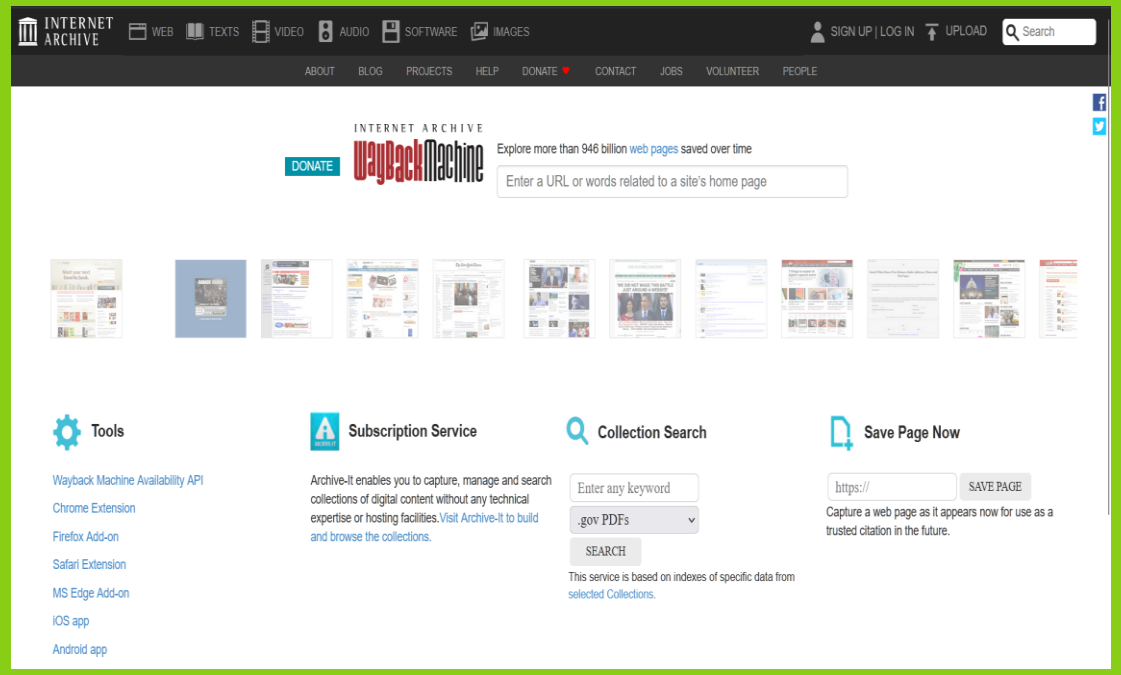
Перехват электронной почты

Отслеживание нажатия клавиш

Создание зомби-компьютеров



Пример утечек данных/взлома в Мире



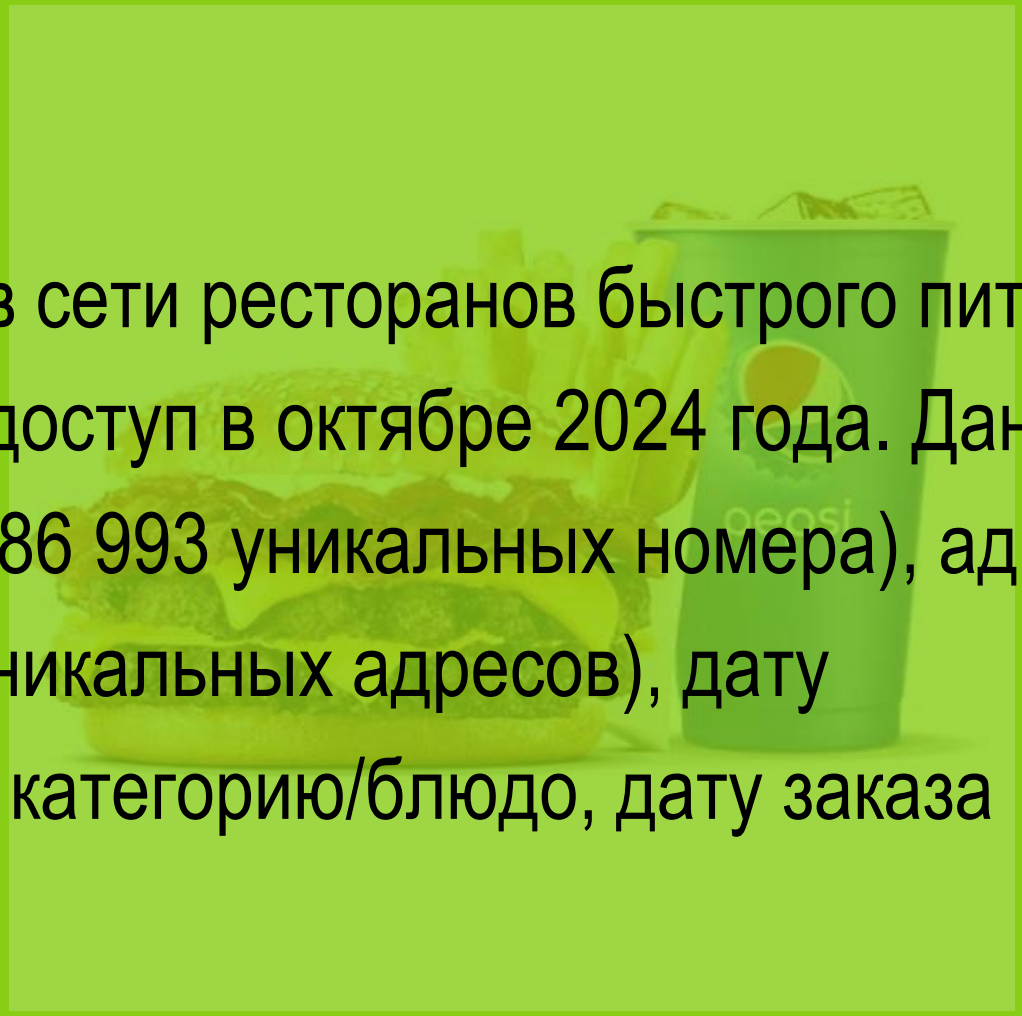
Кейс - Internet Archive

На сайт web.archive.org, принадлежащий некоммерческой организации Internet Archive, произошла хакерская атака в октябре 2024 года. По информации СМИ, произошла утечка данных более 31 млн пользователей.

Пример утечек данных/взлома в России

Кейс – Burger King

Персональные данные клиентов сети ресторанов быстрого питания Burger King попали в открытый доступ в октябре 2024 года. Данные содержат имена, телефоны (4 886 993 уникальных номера), адреса электронной почты (3 163 628 уникальных адресов), дату рождения, пол, город, любимую категорию/блюдо, дату заказа клиентов.



Что/Кто осуществляет информационную безопасность в РФ

В России защита персональных данных регулируется статьей 152-ФЗ "О персональных данных" и главой 14 Трудового кодекса РФ (для работников), а также статьей 137 Уголовного кодекса РФ и статьей 13.11 Кодекса об административных правонарушениях.

А также государственные структуры: Роскомнадзор, ФСТЭК, ФСБ

Вредоносные программы

Вредоносные программы - это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам.



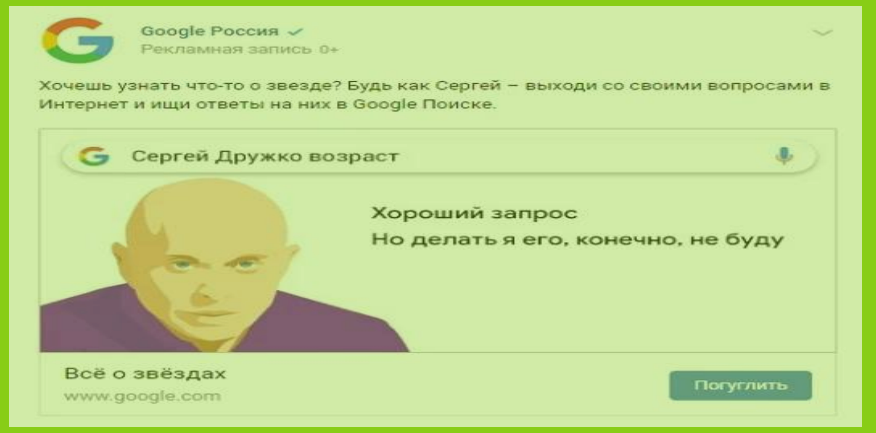


Типы вредоносных программ



Рекламные программы - это программы, которые демонстрируют нежелательную рекламу на вашем устройстве, всплывающие окна и перенаправляют вас на рекламные сайты, а иногда и собирают ваши данные для персонализированной рекламы.







Типы вредоносных программ

Шпионские программы - это разновидность вредоносных программ, скрывающихся на устройстве, отслеживающих активность и осуществляющих кражу конфиденциальной информации: финансовых данных, учетных записей, данных для входа и прочих данных.



Типы вредоносных программ

Программы-вымогатели – это вредоносные программы, осуществляющие блокировку или отказ доступа пользователей к системе или данным до момента выплаты выкупа.

Программы-шифровальщики – это тип программ-вымогателей, выполняющих шифрование пользовательских файлов и требующих оплаты в определенный срок и часто в цифровой валюте, например, в биткойнах.



Типы вредоносных программ

Майнер - вредоносный код использует мощность вашего ПК с целью добычи криптовалюты.

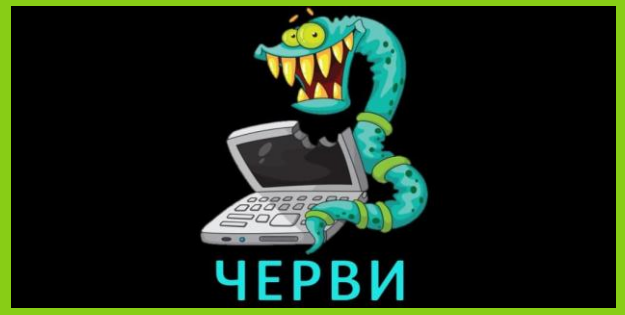




Типы вредоносных программ

Троянские программы - это тип вредоносного программного обеспечения, которое маскируется под легитимное или полезное приложение, чтобы обманным путем попасть на устройство пользователя. После установки троянец не способен самостоятельно распространяться, но предоставляет злоумышленникам скрытый доступ к системе для кражи личных данных, слежки, несанкционированных изменений или даже полного контроля над устройством.





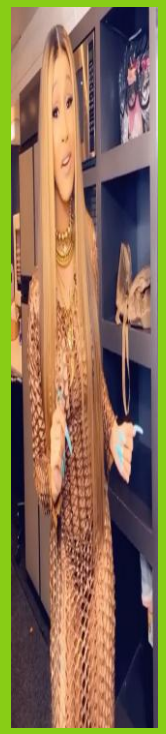
Типы вредоносных программ

Черви - это один из наиболее часто встречающихся типов вредоносных программ, распространяющихся по компьютерным сетям, используя уязвимости операционной системы. Черви представляют собой отдельные программы, распространяющиеся путем самокопирования с целью заражения других компьютеров, при этом никаких действий со стороны пользователей или злоумышленников не требуется.



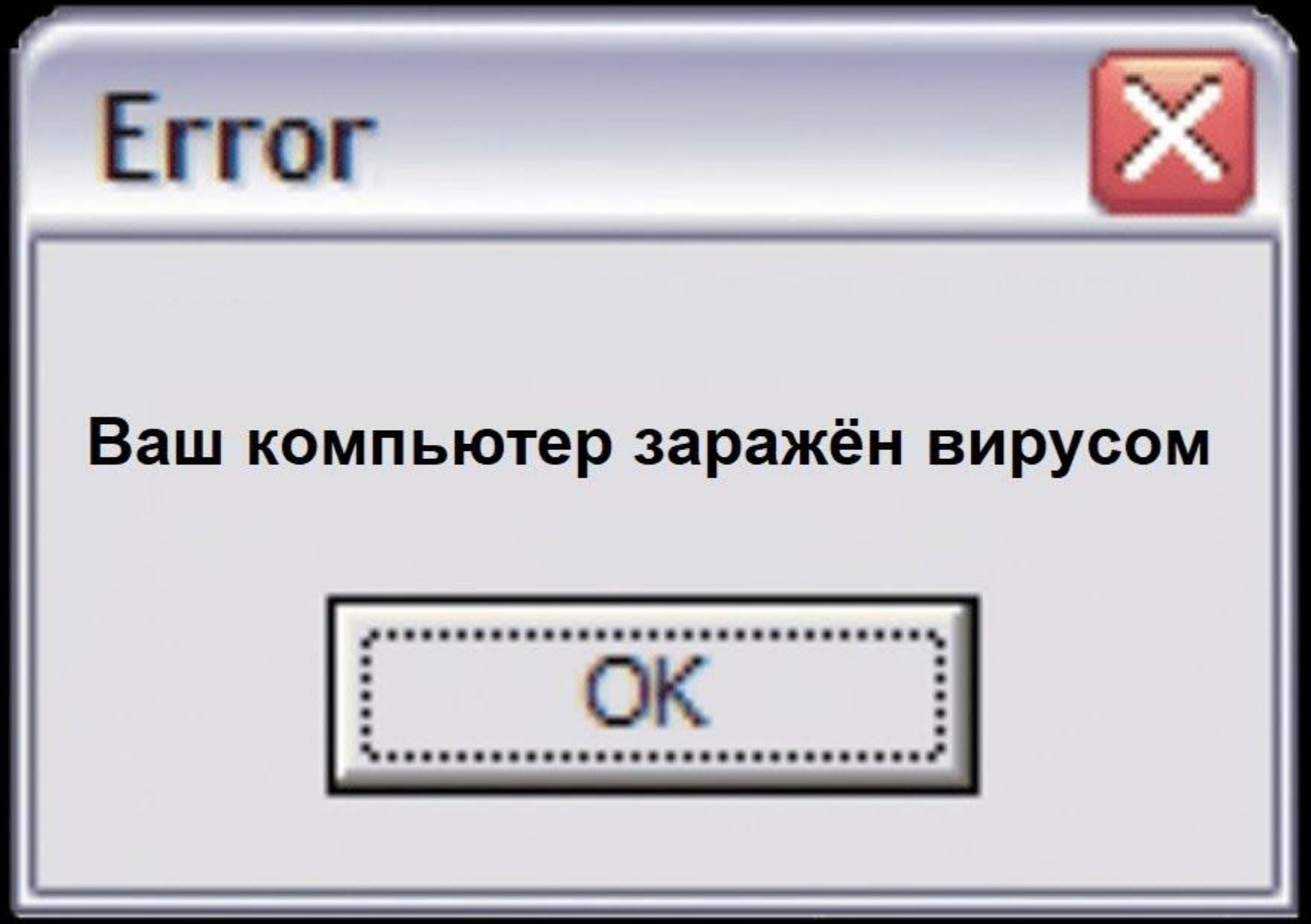
Типы вредоносных программ





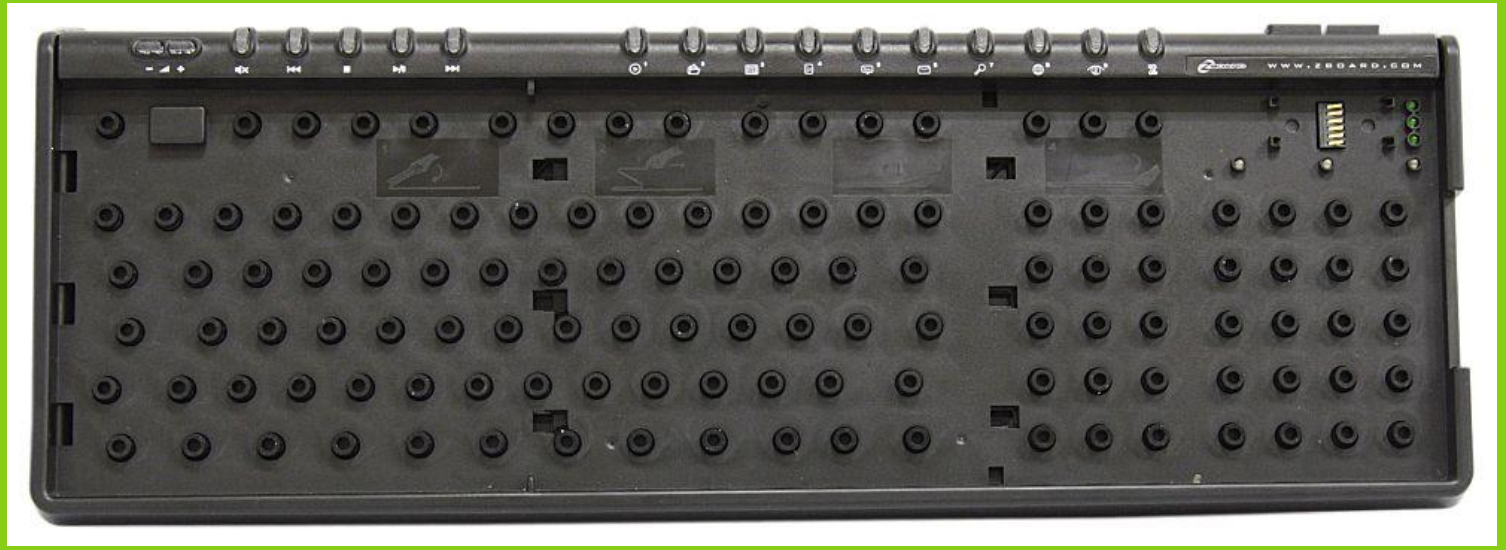
Вирус - это фрагмент кода, который вставляется в приложение и запускается при его запуске. Попав в сеть, вирус может использоваться для кражи конфиденциальных данных, запуска DDoS-атак или атак программ-вымогателей. Обычно вирус распространяется через зараженные веб-сайты, при совместном доступе к файлам, при загрузке зараженных вложений электронной почты. Вирус бездействует до момента активации зараженного файла или программы. После этого вирус начинает распространяться в системе.




Error
Ваш компьютер заражён вирусом
OK

Типы вредоносных программ

Клавиатурные шпионы - это разновидность шпионских программ, отслеживающих активность пользователей. Злоумышленники могут использовать клавиатурные шпионы для кражи паролей, банковских данных и прочей конфиденциальной информации. Клавиатурные шпионы могут попасть систему в результате фишинга, социальной инженерии или вредоносных загрузок.



Типы вредоносных программ

Бот – это компьютер, зараженный вредоносной программой, которым злоумышленники могут управлять удаленно. Боты, иногда называемые зомби-компью спользоваться для запуска атак, а также стать частью б ра ботов, объединенных в сеть. Ботнеты могут включа стройств, как правило, они распространяются незамет воляют злоумышленникам совершать различные вред вия: DDoS-атаки, рассылку спама и фишинговых сообщ аспространять другие типы вредоносных программ.



Антивирусные программы

Антивирусные программы - это специализированное программное обеспечение, предназначенное для защиты компьютеров и других устройств от вредоносных программ (вирусов, троянов, шпионского ПО и др.), обеспечивая их обнаружение, блокировку, удаление и нейтрализацию.

Примеры антивирусные программы



Антивирусные программы

Обновление баз антивируса необходимо для обнаружения новых угроз, так как они содержат описания вредоносных программ. Для большинства антивирусных программ, таких как Kaspersky и Microsoft Defender, обновления происходят автоматически через интернет, но могут быть и ручные способы.

Безопасность в Интернете

Сетевые угрозы - это действия или события, которые могут нарушить конфиденциальность, целостность или доступность информации и систем в сети, включая вредоносное ПО, фишинг, DDoS-атаки, социальную инженерию и несанкционированный доступ, а также физические угрозы, такие как кража оборудования.

Безопасность в Интернете

Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям).



Безопасность в Интернете



Спам - массовая рассылка корреспонденции (чаще всего рекламы) лицам, не выражавшим желания её получить. Распространителей спама называют **спамерами.**







Безопасность в Интернете



Социальная инженерия в ИБ - это вид манипуляции людьми с целью получения конфиденциальной информации или доступа к системам. Злоумышленники используют психологическое воздействие, чтобы заставить жертву совершить определенные действия (например, предоставить пароль), обходя при этом технические средства защиты. Распространенные методы социальной инженерии включают фишинг (email-рассылки), вишинг (телефонные звонки) и смсинг (SMS-сообщения).

Безопасность в Интернете

Фейковые страницы - это поддельные профили в социальных сетях, на форумах или веб-сайтах, созданные от чужого имени или с использованием фальшивых данных. Их создают для различных целей: мошенничества, распространения дезинформации, травли, а также из-за желания анонимности или для пародийных целей.



Меры информационной безопасности при работе в сети интернет

Использование антивируса

Работа с надежными сайтами

Создание сложных паролей

Регулярное обновление программ

Не открывать подозрительные письма / ссылки

Быть внимательным при загрузке файлов

Тренды и прогнозы развития цифровых технологий

Как данные инструменты возможно использовать в ИБ?

Искусственный интеллект

Интернет вещей

Облачные сервисы

Кибервойны и атаки на инфраструктуру