Как обеспечить личную кибербезопасность в цифровую эпоху

Климов Евгений

Ecom.tech

Почему это важно?

- Резкий рост киберпреступности.
- Цифровая трансформация = новые уязвимости: Все больше аспектов жизни (общение, финансы, работа, госуслуги) переходят в онлайн.
- Последствия для частных лиц: Кража личных данных (ФИО, паспорт, СНИЛС, ИНН), финансовые потери (взлом онлайн-банкинга, мошенничество), ущерб репутации.
- Пример: История о крупной утечке данных из популярного онлайн-сервиса и ее последствиях для пользователей.

Почему это критически важно для юристов?

- **Адвокатская тайна и конфиденциальность клиентских данных**: Юристы работают с особо чувствительной информацией (детали дел, финансовая информация клиентов, коммерческая тайна).
- **Репутационные риски**: Утечка данных может разрушить доверие клиентов и нанести непоправимый ущерб репутации юриста или фирмы.
- **Риски компрометации цифровых доказательств**: Важность сохранения целостности и подлинности электронных документов и переписки.
- **Юридическая ответственность**: Ответственность за несоблюдение законодательства о защите персональных данных.
- **Профессиональная этика**: Обязанность юриста принимать все разумные меры для защиты информации клиента.
- **Пример**: "Взлом почты юридической фирмы X привел к утечке информации о готовящейся сделке M&A, что сорвало переговоры и повлекло финансовые потери для клиента".

Цели мастер-класса

- **Понять ландшафт угроз**: Разобраться, какие киберугрозы наиболее актуальны сегодня и как они эволюционируют.
- **Освоить практические навыки**: Научиться защищать свои устройства (компьютеры, смартфоны), аккаунты (почта, соцсети, мессенджеры) и данные.
- **Быть в курсе новых технологий**: Узнать о рисках, связанных с ИИ, дипфейками, метавселенными и другими трендами.
- **Сформировать «безопасное мышление»**: Выработать привычку критически оценивать цифровую среду и принимать осознанные решения для своей защиты.
- **Знать, что делать**: Понимать алгоритм действий при киберинциденте и правовые аспекты.

План мастер-класса

- **Основные киберугрозы**: Знать врага в лицо.
- **Крепость на замке**: Защита устройств и аккаунтов.
- **Цифровые следы**: Безопасное поведение в сети.
- **На гребне волны**: Новые технологии и связанные с ними киберугрозы.
- **Закон и порядок**: Правовые аспекты и реагирование на инциденты.
- Обсуждение и ответы на вопросы.

Основные киберугрозы

Что такое киберугроза?

Определение:

Любое потенциально опасное событие или действие, которое может нанести ущерб информационным системам, данным или пользователям.

Что такое киберугроза?

Основные категории угроз:

- Вредоносное ПО (Malware)
- Социальная инженерия (манипуляция людьми)
- Сетевые атаки (DDoS, перехват трафика)
- Атаки на веб-приложения (SQL-инъекции, XSS)
- Инсайдерские угрозы (умышленные или случайные действия сотрудников)

Мотивация злоумышленников:

- Финансовая выгода (самая частая)
- Шпионаж (государственный, корпоративный)
- Хактивизм (политические или социальные мотивы)
- Кибертерроризм
- Месть, самоутверждение

Вредоносное ПО (Malware)

Виды:

- **Вирусы**: Прикрепляются к программам, самокопируются.
- **Черви**: Распространяются по сети самостоятельно.
- **Трояны**: Маскируются под легитимное ПО, выполняют скрытые вредоносные функции.
- **Шпионское ПО** (Spyware): Собирает информацию о пользователе без его ведома.
- **Рекламное ПО** (Adware): Показывает навязчивую рекламу.
- **Клавиатурные шпионы** (Keyloggers): Записывают нажатия клавиш.

Методы распространения:

Email-вложения, вредоносные ссылки, зараженные веб-сайты, USB-накопители, пиратское ПО.

Пример для юристов:

Троян, замаскированный под шаблон юридического документа или обновление специализированной правовой программы, который крадет учетные данные от систем электронного документооборота

Программы-вымогатели (Ransomware)

- **Механизм**: Шифрование файлов на устройстве жертвы или блокировка доступа к системе. Требование выкупа (часто в криптовалюте) за расшифровку или восстановление доступа.
- **Последствия**: Потеря доступа к критически важным данным (дела клиентов, финансовые документы), остановка работы, финансовые убытки (выкуп, восстановление, простои), репутационный ущерб.
- **Актуальность для юристов**: Риск шифрования всей базы дел, что может парализовать работу юридической практики.
- **Пример**: Атака на юридическую фирму, где были зашифрованы все серверы, включая резервные копии. Злоумышленники требовали выкуп, угрожая опубликовать конфиденциальные данные клиентов.
- **Вопрос к аудитории**: Каковы, на ваш взгляд, правовые и этические аспекты уплаты выкупа злоумышленникам? Что бы вы посоветовали клиенту (например, компании) в такой ситуации?

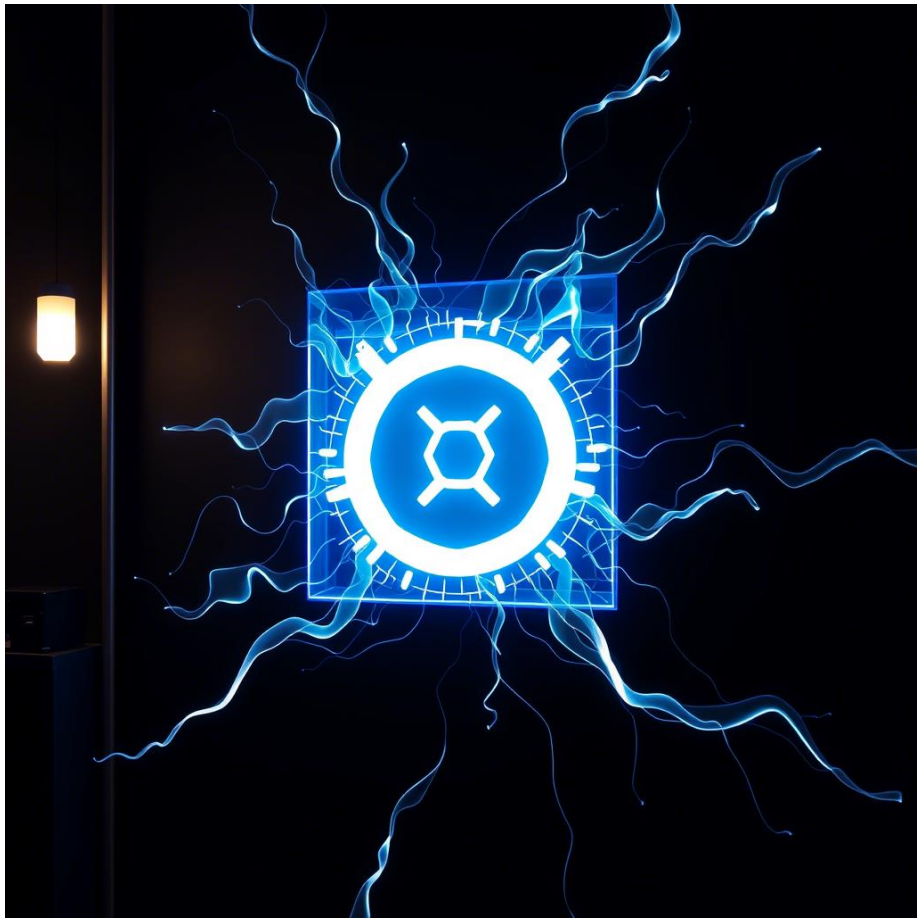
Фишинг и Спирфишинг

- **Фишинг (Phishing)**: Массовая рассылка поддельных писем/сообщений (от имени банков, госорганов, известных компаний) с целью выманивания логинов, паролей, данных банковских карт, установки вредоносного ПО.
- **Спирфишинг (Spear Phishing)**: Целенаправленный фишинг, нацеленный на конкретного человека или организацию. Письма более персонализированы и убедительны.
- **Признаки фишинга**: Неожиданность письма, ошибки в тексте, подозрительный адрес отправителя (даже если похож на настоящий), ссылки, ведущие на поддельные сайты, требования срочно ввести данные.
- **Пример**: Письмо якобы от налоговой инспекции с требованием срочно перейти по ссылке для ознакомления с "новыми поправками" (ссылка ведет на вредоносный сайт или скачивание зараженного файла). Или письмо от "коллеги" с просьбой посмотреть "важный документ по делу" (документ содержит макрос-вирус).

Социальная инженерия

Определение:

Психологическое манипулирование людьми с целью получения конфиденциальной информации или совершения определенных действий. Не технический взлом, а "взлом человека".



Социальная инженерия

- **Претекстинг**: Создание вымышленного сценария (легенды) для получения информации.
- **Вишинг (Vishing)**: Голосовой фишинг (звонки от "службы безопасности банка", "технической поддержки").
- **Смишинг (SMiShing)**: SMS-фишинг.
- **Приманка (Baiting)**: Предложение чего-то заманчивого (например, оставленная "случайно" зараженная флешка).

- **Почему это работает**: Игра на человеческих эмоциях (страх, любопытство, жадность, доверие, желание помочь).
- **Пример**: Звонок "системного администратора" юридической фирмы с просьбой продиктовать пароль для "срочного обновления системы безопасности".
- **Вопрос к аудитории**: Какие психологические слабости людей чаще всего используют социальные инженеры? Как юристу, привыкшему к формальному общению, распознать манипуляцию в неформальном контексте?

DDoS-атаки и взлом аккаунтов

DDoS-атаки (Distributed Denial of Service):

Атака на отказ в обслуживании. Перегрузка сервера или сетевого канала огромным количеством запросов с множества зараженных компьютеров (ботнет), делая сервис недоступным для легитимных пользователей.

Актуальность для юристов:

Может быть направлена на сайт юридической фирмы, систему электронного правосудия, онлайн-сервисы, которыми пользуются юристы.

Взлом аккаунтов

Причины:

Слабые/повторяющиеся пароли, утечки данных с других сервисов, фишинг, вредоносное ПО.

Последствия:

Доступ к конфиденциальной переписке, документам, финансовая кража, распространение дезинформации от имени жертвы.

Пример:

Взлом электронной почты адвоката с последующим использованием переписки для шантажа или дискредитации клиента.

Угрозы для мобильных устройств

Смартфоны и планшеты хранят огромное количество личной и рабочей информации, часто менее защищены, чем ПК.

Векторы атак:

- **Вредоносные приложения**: Замаскированные под игры, утилиты, часто из неофициальных магазинов.
- **Небезопасные Wi-Fi сети**: Особенно общедоступные точки доступа, где трафик может быть перехвачен.
- **Фишинг и смишинг**: Адаптированы под мобильные устройства.
- **Уязвимости ОС и приложений**: Несвоевременное обновление.
- **Кража или потеря устройства**: Риск несанкционированного доступа к данным.
- **BYOD (Bring Your Own Device)**: Использование личных устройств для работы создает дополнительные риски для корпоративных данных, если устройство юриста скомпрометировано.
- **Пример**: Вредоносное приложение, которое после установки запрашивает доступ к контактам и сообщениям, а затем рассылает спам или фишинговые ссылки от имени владельца.

Инсайдерские угрозы

Определение:

Угрозы, исходящие от лиц, имеющих легитимный доступ к информационным системам и данным организации (сотрудники, подрядчики).

Инсайдерские угрозы

Типы инсайдеров:

- **Злонамеренные**: Действуют с целью навредить компании, украсть данные для личной выгоды или мести.
- **Небрежные/Ошибающиеся**: Нарушают правила безопасности случайно, из-за незнания или невнимательности (например, отправляют конфиденциальный документ не тому адресату).
- **Скомпрометированные**: Учетные данные которых были украдены, и злоумышленник действует от их имени.

Специфика для юридических фирм:

Высокая ценность информации, с которой работают сотрудники (ассистенты, паралигалы, младшие юристы), делает их потенциальными целями или источниками утечек.

Пример:

Недовольный уволенный сотрудник копирует базу клиентов перед уходом. Или юрист случайно отправляет конфиденциальный документ по делу на неправильный email-адрес.

Вопрос к аудитории:

Какие меры, по вашему мнению, должна предпринимать юридическая фирма для минимизации рисков инсайдерских угроз, не создавая при этом атмосферу тотального недоверия?

Защита устройств и аккаунтов

Основы защиты компьютера

Регулярные обновления:

Операционной системы (Windows, macOS, Linux) и всего установленного программного обеспечения (браузеры, офисные пакеты, PDF-ридеры и т.д.). Обновления часто содержат исправления известных уязвимостей.

Антивирусное ПО:

Использование надежного антивируса с актуальными базами. Регулярное сканирование системы.

Файрвол (Межсетевой экран):

Контроль входящего и исходящего сетевого трафика. Использование как программного (встроенного в ОС или антивирус), так и аппаратного (в роутере).

Осторожность при установке ПО:

Скачивание программ только с официальных сайтов разработчиков или из проверенных источников. Внимательное чтение лицензионных соглашений и разрешений при установке.

Учетные записи пользователей:

Работа под учетной записью с ограниченными правами для повседневных задач. Использование учетной записи администратора только при необходимости.

Парольная гигиена: Создание сложных паролей

Почему слабые пароли – это плохо:

Легко подбираются (брутфорс, словарные атаки), часто используются повторно на разных сайтах.

Парольная гигиена: Создание сложных паролей

Критерии надежного пароля:

- **Длина**: Минимум 12-15 символов (чем длиннее, тем лучше).
- **Сложность**: Использование комбинации прописных и строчных букв, цифр и специальных символов (!@#$%^&*()_+-=[]{}|;':",./<>?).
- **Уникальность**: Отдельный пароль для каждого аккаунта.
- **Отсутствие личной информации**: Не использовать имена, даты рождения, клички питомцев, словарные слова.
- **Пассфразы (Passphrases)**: Легче запоминаются и могут быть очень длинными (например, "ЛюблюГрозуВначалеМаяКогдаВесенний ПервыйГром!").
- **Чего избегать**: "123456", "password", "qwerty", имя_жены_год_рождения.
- Практическое задание (мысленно): "Проверьте свои текущие пароли. Соответствуют ли они этим критериям? Можете ли вы сейчас придумать действительно надежный пароль/пассфразу?"

Менеджеры паролей

Проблема: Сложно запомнить десятки уникальных и сложных паролей.

Решение: Менеджеры паролей – программы или сервисы для безопасного хранения и управления паролями.

Как работают: Хранят все пароли в зашифрованном виде. Доступ к базе паролей осуществляется с помощью одного мастер-пароля (который должен быть очень надежным!).

Менеджеры паролей

Преимущества:

- Генерация очень сложных и уникальных паролей.
- Автоматическое заполнение форм входа на сайтах и в приложениях.
- Безопасное хранение (шифрование).
- Синхронизация между устройствами.
- Некоторые менеджеры предупреждают об утечках паролей или слабых паролях.

Важно: Тщательно выбирать менеджер паролей, доверять только проверенным решениям. Надежно хранить мастер-пароль.

Двухфакторная аутентификация (2FA/MFA)

Что это такое?

Метод идентификации пользователя с помощью двух (2FA) или более (MFA) различных типов учетных данных (факторов).

Двухфакторная аутентификация (2FA/MFA)

Факторы аутентификации:

- **Знание** (Something you know): Пароль, PIN-код, ответ на секретный вопрос.
- **Владение** (Something you have): SMS-код на телефон, код из приложения-аутентификатора (упомянуть, что есть много таких приложений), аппаратный токен, смарт-карта.
- **Свойство** (Something you are): Биометрические данные (отпечаток пальца, распознавание лица, сетчатка глаза, голос).

Почему это критически важно?

Даже если злоумышленник украдет ваш пароль, он не сможет войти в аккаунт без второго фактора. Значительно повышает безопасность.

Где использовать: Электронная почта, социальные сети, мессенджеры, онлайн-банкинг, облачные хранилища, любые важные аккаунты.

Пример: При входе в почту после ввода пароля система запрашивает одноразовый код из приложения-аутентификатора на вашем смартфоне.

Вопрос к аудитории: На каких сервисах вы уже используете 2FA? Какие методы 2FA вам кажутся наиболее удобными/безопасными?

Защита мобильных устройств (Смартфоны и Планшеты)

Блокировка экрана

Использовать надежный PIN-код (не 1234, 0000, дата рождения), графический ключ (сложный, не очевидный), пароль или биометрическую аутентификацию (отпечаток пальца, распознавание лица).

Шифрование данных

Включить шифрование устройства (на большинстве современных смартфонов включено по умолчанию, но стоит проверить). Это защитит данные, даже если злоумышленник извлечет карту памяти или получит доступ к файловой системе.

Управление разрешениями приложений

Внимательно проверять, какие разрешения запрашивает приложение при установке и использовании. Отключать ненужные разрешения (доступ к камере, микрофону, местоположению, контактам).

Защита мобильных устройств (Смартфоны и Планшеты)

Установка приложений

Скачивать приложения только из официальных магазинов. Избегать установки из сомнительных источников. Читать отзывы перед установкой.

Обновления

Регулярно обновлять операционную систему и приложения.

Функции "Найти устройство"

Активировать и настроить (стандартные функции ОС). Позволяют удаленно определить местоположение, заблокировать или стереть данные с утерянного/украденного устройства.

Публичный Wi-Fi

Использовать с осторожностью, желательно через VPN.

Шифрование данных

Что такое шифрование?

Процесс преобразования информации (открытого текста) в зашифрованный вид (шифротекст) с помощью криптографического алгоритма и ключа, делая ее нечитаемой для тех, у кого нет ключа для расшифровки.

Зачем это юристу?

Защита конфиденциальной информации клиентов, материалов дел, финансовой документации от несанкционированного доступа при хранении и передаче.

Шифрование данных

Виды шифрования:

- **Шифрование всего диска** (Full-Disk Encryption - FDE): Упомянуть, что такие функции встроены в большинство современных ОС.
- **Шифрование файлов и папок**: Существуют программы для создания зашифрованных контейнеров или шифрования отдельных файлов/папок; также архиваторы с функцией установки пароля на архив.
- **Шифрование электронной почты**: Существуют технологии для шифрования содержимого писем и вложений, а также использования цифровых подписей.
- **Аппаратное шифрование**: Некоторые USB-накопители и внешние диски имеют встроенное аппаратное шифрование.

Важность надежных паролей для шифрования: Пароль – это ключ к вашим зашифрованным данным.

Резервное копирование (Бэкапы)

Зачем нужно?

Защита от потери данных в результате атак программ-вымогателей, сбоев оборудования, случайного удаления, физической утраты устройства.

Правило "3-2-1":

- 3 копии данных: Оригинал и как минимум две резервные копии.
- 2 разных типа носителей: Например, внутренний жесткий диск + внешний жесткий диск, или внешний диск + облачное хранилище.
- 1 копия вне основного местоположения (off-site): Для защиты от локальных катастроф.

Резервное копирование (Бэкапы)

Регулярность: Настроить автоматическое резервное копирование по расписанию.

Проверка бэкапов: Периодически проверять возможность восстановления данных из резервных копий.

Инструменты: Встроенные средства ОС, сторонние программы для резервного копирования, облачные сервисы с функцией бэкапа.

Для юристов: Резервное копирование всей базы дел, документов, переписки – критически важно.

Безопасность Wi-Fi сетей

Риски публичных (открытых) Wi-Fi сетей: Перехват данных, распространение вредоносного ПО.

Безопасность Wi-Fi сетей

Меры предосторожности в публичных Wi-Fi:

- Использовать VPN (Virtual Private Network). VPN создает зашифрованный туннель, защищая ваш трафик.
- Не передавать конфиденциальную информацию.
- Убедиться, что сайты используют HTTPS.
- Отключить автоматическое подключение к открытым сетям.
- Отключить общий доступ к файлам и принтерам.

Безопасность Wi-Fi сетей

Защита домашней/офисной Wi-Fi сети:

- Изменить стандартные имя сети (SSID) и пароль администратора роутера.
- Использовать сильное шифрование: WPA3 (предпочтительно) или WPA2-PSK с надежным паролем.
- Создать гостевую сеть.
- Регулярно обновлять прошивку роутера.

Физическая безопасность устройств

- Не оставлять устройства без присмотра.
- Ноутбуки и мобильные устройства: Использовать сумки и чехлы, не привлекающие внимания; рассмотреть замки для ноутбуков.
- Серверы и стационарные ПК в офисе: Ограничение доступа в серверные.
- USB-флешки и внешние диски: Не подключать неизвестные, шифровать данные на съемных носителях.
- Утилизация старых устройств: Безопасное стирание данных.

Важность для юристов: Устройства часто содержат огромное количество конфиденциальной информации.

Безопасное удаление данных

Простое удаление (в корзину) не стирает данные.

Форматирование диска: Быстрое форматирование также не всегда полностью стирает данные.

Методы безопасного удаления (санитайзинга):

- **Программное уничтожение** (Data Wiping/Shredding): Многократная перезапись секторов диска. Существуют специальные программы для этого.
- **Физическое уничтожение носителя**: Наиболее надежный способ для старых или неисправных носителей.
- **Актуальность для юристов**: При смене компьютеров, утилизации носителей с клиентскими данными необходимо обеспечить их гарантированное уничтожение.

Вопрос к аудитории: Какие процедуры по безопасному удалению данных должны быть внедрены в юридической фирме? Каковы могут быть правовые последствия, если жесткий диск с данными клиентов попадет в чужие руки?

Безопасное поведение в сети

- Электронная почта – основной вектор атак.
- Распознавание фишинговых и вредоносных писем: Адрес отправителя, тема и текст, ссылки, вложения, запросы личной информации.
- Действия при получении подозрительного письма: Не отвечать, не переходить по ссылкам, не открывать вложения. Удалить или сообщить.
- Использование спам-фильтров.

Безопасный веб-серфинг

- **HTTPS и "замочек":** Проверять наличие HTTPS и значка замка.
- **Осторожность при скачивании файлов**: Скачивать только с доверенных источников.
- Вредоносная реклама (Malvertising).
- **Браузерные расширения**: Устанавливать только необходимые и проверенные. Полезные категории: блокировщики рекламы, менеджеры паролей, расширения для принудительного HTTPS.
- **Режим "инкогнито" / "приватный просмотр"**: Что он дает и чего не дает.
- Остерегайтесь всплывающих окон с требованием обновить ПО или сообщением о вирусах.

Социальные сети и приватность

- **Настройки приватности**: Регулярно проверять и настраивать.
- **Овершеринг** (Over-sharing): Не публиковать избыточную личную информацию.
- **Цифровой след** (Digital Footprint): Влияние на репутацию.
- **Специфика для юристов**: Информация из соцсетей может быть использована против вас или ваших клиентов.
- **Геотеги**: Отключать при необходимости.
- **Друзья и подписчики**: Быть избирательным. Остерегаться фейковых аккаунтов.

Пример: Юрист разместил в соцсети фото из отпуска, указав даты. Эта информация была использована для квартирной кражи.

Онлайн-покупки и финансовые операции

- **Проверенные сайты**: Совершать покупки только на известных и надежных сайтах.
- **Фишинговые сайты-клоны**: Остерегаться поддельных сайтов.
- **Данные банковской карты**: Не сохранять данные карты на сайтах без необходимости. Использовать виртуальные карты.
- **3-D Secure**: Дополнительный уровень защиты.
- **Проверка выписок**: Регулярно проверять банковские выписки.
- **Публичный Wi-Fi**: Избегать финансовых операций без VPN.
- **Мобильный банкинг**: Использовать официальные приложения банков.

Цифровая гигиена и критическое мышление

- **Не доверять слепо**: Информация в интернете может быть недостоверной.
- **Проверка источников**: Стараться проверять важную информацию.
- Критическое отношение к "сенсациям" и "слишком выгодным предложениям".
- **Осознанность действий**: Думать, прежде чем кликать.
- Распознавание манипуляций.
- **Регулярная "уборка":** Удалять ненужные аккаунты, файлы, приложения.
- Обучение и информированность.

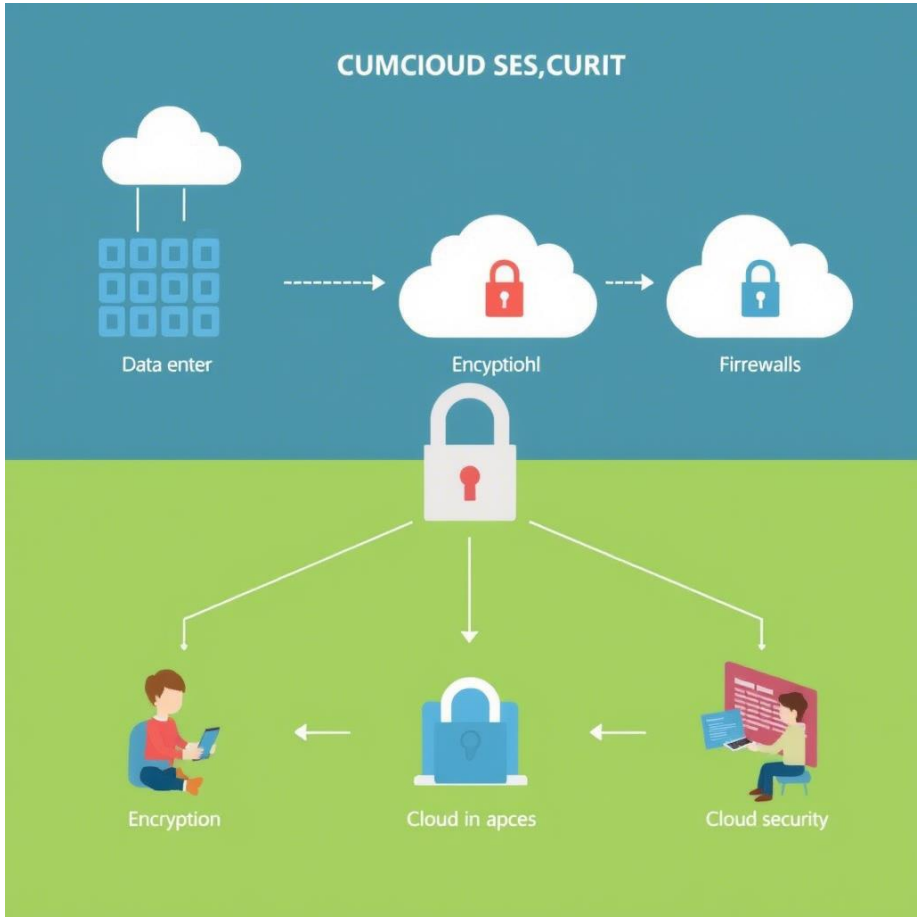
Облачные хранилища и их безопасность

Преимущества:

Доступность данных, удобство совместной работы, резервное копирование.

Риски:

Утечка данных при взломе аккаунта, уязвимости сервиса, доступ к данным со стороны провайдера.



Облачные хранилища и их безопасность

Меры безопасности:

- Выбор надежного провайдера.
- Надежный пароль и 2FA.
- Шифрование на стороне клиента (Client-Side Encryption): Для особо конфиденциальных данных – шифровать файлы перед загрузкой в облако с помощью специальных программ.
- Управление правами доступа.
- Синхронизация: Понимать, какие папки синхронизируются.

Вопрос к аудитории:

Какие облачные сервисы вы используете? Знаете ли вы, какие меры безопасности предлагает ваш провайдер?

Интернет вещей (IoT) и связанные риски

- **Что такое IoT (Internet of Things)**: Умные часы, фитнес-трекеры, умные колонки, бытовая техника, камеры и т.д.
- **Риски безопасности IoT**: Слабые или стандартные пароли, уязвимости в прошивке, сбор данных, использование в ботнетах, несанкционированный доступ.
- **Меры предосторожности**: Менять стандартные пароли, обновлять прошивки, сегментировать сеть, отключать ненужные функции.

Пример: Взлом IP-камеры видеонаблюдения в квартире и трансляция видео в интернет.

Новые технологические тренды и киберугрозы

Искусственный интеллект (ИИ) и машинное обучение (МО) в кибербезопасности

ИИ на службе атакующих:

Создание более убедительных фишинговых писем, автоматизация атак, генерация вредоносного ПО, обход CAPTCHA, адаптивные атаки.

ИИ на службе защиты:

Обнаружение аномалий и угроз, предиктивная аналитика, автоматизация реагирования, улучшение систем аутентификации.

Deepfakes (Дипфейки)

- **Что это такое**: Фото, аудио и видео материалы, реалистично сфабрикованные с помощью ИИ.
- **Технология**: Основана на генеративно-состязательных сетях (GAN).
- **Угрозы**: Дезинформация, шантаж, дискредитация, мошенничество, подделка доказательств.
- **Как распознать** (становится все сложнее): Неестественная мимика, артефакты.
- **Пример**: Дипфейк-видео, где известный политик "признается" в преступлении.

Вопрос к аудитории: Каковы могут быть юридические последствия использования дипфейков? Как юристу работать с цифровыми доказательствами, если существует риск их подделки?

Угрозы в метавселенных и VR/AR

- **Метавселенные**: Конвергенция физической, дополненной (AR) и виртуальной (VR) реальности.
- **Новые векторы атак и риски**: Кража цифровых активов, взлом аккаунтов, социальная инженерия, атаки на VR/AR-устройства, приватность данных, неправомерное поведение, юридическая неопределенность.
- **Пример**: Кража дорогостоящего NFT-артефакта у пользователя в метавселенной.

Квантовые вычисления и их влияние на криптографию

- **Квантовые компьютеры**: Потенциал для решения задач, непосильных для классических компьютеров.
- **Угроза для существующей криптографии**: Алгоритм Шора и его способность взламывать RSA, ECC.
- "Собирай сейчас, расшифровывай потом" (Harvest Now, Decrypt Later).
- Постквантовая криптография (Post-Quantum Cryptography - PQC): Разработка новых криптографических алгоритмов.
- **Перспективы**: Отдаленная, но стратегически важная перспектива.

Безопасность блокчейн-технологий и криптовалют

Угрозы и уязвимости: Атаки на смарт-контракты, биржи, кошельки; фишинг; атака 51%; проблемы приватности.

Меры безопасности для пользователей криптовалют: Использование аппаратных кошельков, надежное хранение приватных ключей, осторожность при работе с биржами, 2FA.

Пример: Пользователь переходит по фишинговой ссылке, имитирующей сайт известной криптобиржи, вводит свои данные, и его средства похищаются.

Этические дилеммы новых технологий и кибербезопасности

- Баланс между безопасностью и приватностью.
- Использование ИИ для слежки и контроля.
- Ответственность за действия автономных систем.
- Цифровое неравенство.
- Этика использования данных.
- **Для юристов**: Важность понимания этих дилемм.

Вопрос к аудитории: "Должны ли правительства иметь возможность получать доступ к зашифрованным сообщениям граждан в целях борьбы с терроризмом и преступностью, даже если это ослабит безопасность для всех остальных?"

Что делать, если вас взломали?

- Важность наличия плана.
- **Немедленные шаги**: Изолировать, не выключать (в некоторых случаях), зафиксировать.
- **Последующие действия**: Идентифицировать, сообщить/эскалировать (IT-отдел, банк, правоохранительные органы, руководство), сменить пароли, проверить на вредоносное ПО, восстановить данные из бэкапа, анализ и извлечение уроков.

Куда обращаться за помощью?

Внутренние ресурсы (IT-отдел/специалист по ИБ).

Внешние ресурсы:

- Банки и платежные системы.
- Правоохранительные органы (специализированные подразделения МВД, СК, Прокуратура).
- Государственные центры реагирования на компьютерные инциденты.
- Производители ПО и оборудования, сервис-провайдеры.
- Специализированные компании по кибербезопасности.

Сбор цифровых доказательств

- Важность для юристов.
- **Основные принципы**: Сохранение целостности, аутентичности, обеспечение сохранности цепочки владения, фиксация метаданных.
- **Что можно собирать**: Лог-файлы, электронная переписка, данные с мобильных устройств, информация из соцсетей, образы дисков.
- **Методы фиксации**: Нотариальное заверение, привлечение специалистов по компьютерной криминалистике.
- **Проблемы**: Быстрое изменение или удаление информации, сложность атрибуции, допустимость доказательств.

Вопрос к аудитории: С какими типичными ошибками при сборе и представлении цифровых доказательств вы сталкивались или можете предположить?

Страхование киберрисков

- **Что это такое**? Вид страхования для защиты бизнеса от финансовых потерь из-за киберинцидентов.
- **Что обычно покрывает полис**: Расходы на реагирование, восстановление данных, убытки от простоя, ответственность перед третьими лицами, расходы на уведомление.
- **Для кого актуально**: Для организаций, работающих с данными, включая юридические фирмы.
- **Важно**: Внимательно изучать условия договора страхования.

Непрерывное обучение и повышение осведомленности

- Кибербезопасность – это процесс, а не результат.
- Важность регулярного обновления знаний.
- Источники информации и самообразования: Специализированные новостные ресурсы по ИБ, профессиональные издания, курсы и тренинги, конференции, внутренние инструктажи.
- Формирование культуры кибербезопасности.

"Золотые правила" кибербезопасности

"Золотые правила" (чек-лист):

- Бдительность
- Сложные/уникальные пароли + менеджер
- 2FA
- Обновления
- Бэкапы
- Антивирус/файрвол
- Шифрование
- Осторожность с почтой
- Защита мобильных устройств
- Непрерывное обучение

Спасибо за внимание!
Вопросы? Обсудим!