

Компьютерные преступления

Оксана Докучаева



Проверка связи





Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти



Поставьте в чат:

-  если меня видно и слышно
-  если нет

Оксана Докучаева

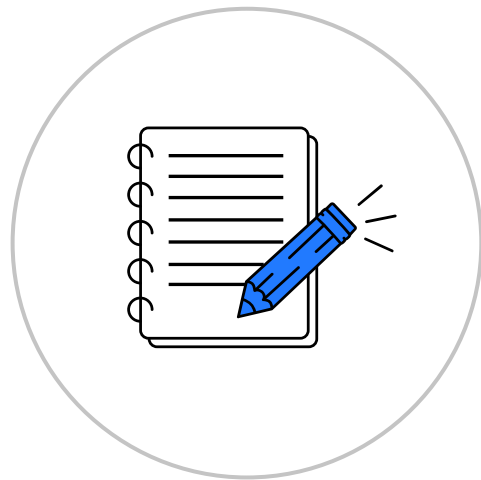
О спикере:

- 13 лет оперативного опыта в Центре информационной безопасности ФСБ России
- Автор публикаций по информационной безопасности и расследованию компьютерных преступлений
- Опыт взаимодействия с Советом Безопасности РФ, правоохранительными органами, спецслужбами, организациями РФ и иностранных государств по вопросам обеспечения информационной безопасности



Правила участия

- 1 Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
- 2 Продолжительность вебинара — 80 минут
- 3 Вы можете писать свои вопросы в чате
- 4 Запись вебинара будет доступна в LMS



Вспомним материалы лекции

- 1 Вы узнали, что такое юридическая ответственность и какая она бывает
- 2 Вы изучили уголовную, административную, гражданскую и дисциплинарную ответственность в сфере информационной безопасности
- 3 Вы узнали, какова степень ответственности в сфере ИБ для разных категорий работников в организациях



Вспомним

Вопрос: что такое информационное правонарушение?



Вспомним

Вопрос: что такое информационное правонарушение?

Ответ: предусмотренное законом общественно опасное деяние, причиняющее вред или создающее опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов и влекущее юридическую ответственность





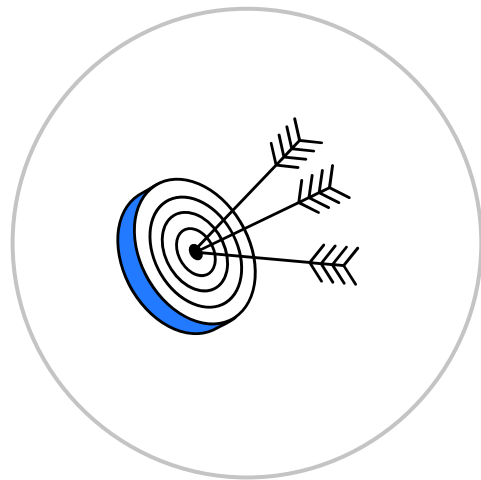
**Как вы думаете,
чем правонарушение
отличается от
преступления?**



Ваши вопросы?

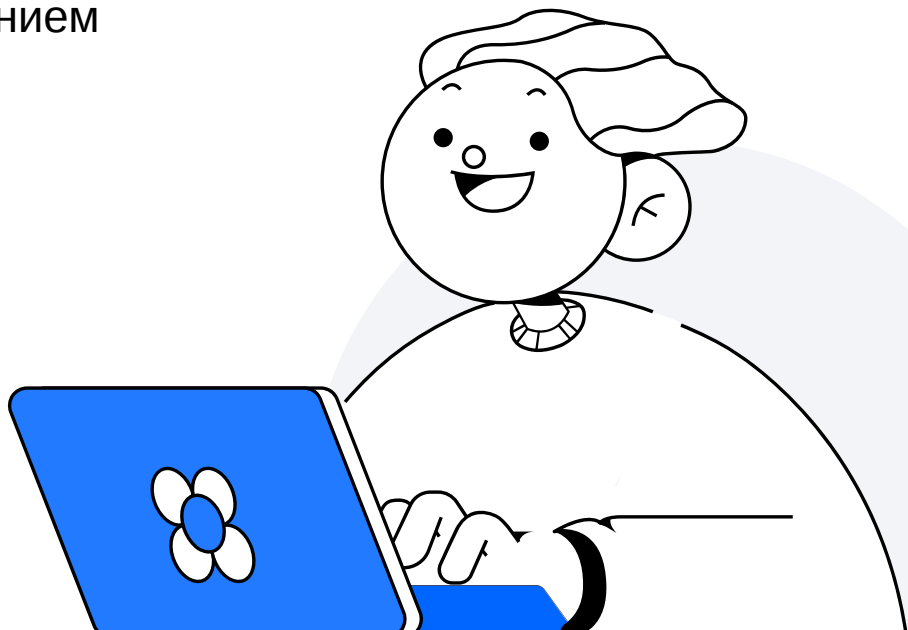
Цели занятия

- Узнать о текущем состоянии компьютерных преступлений
- Рассмотреть примеры преступлений в сфере компьютерной информации и преступлений с использованием информационных технологий



План занятия

- 1 Статистический анализ компьютерных преступлений
- 2 Примеры преступлений в сфере компьютерной информации
- 3 Примеры преступлений с использованием информационных технологий

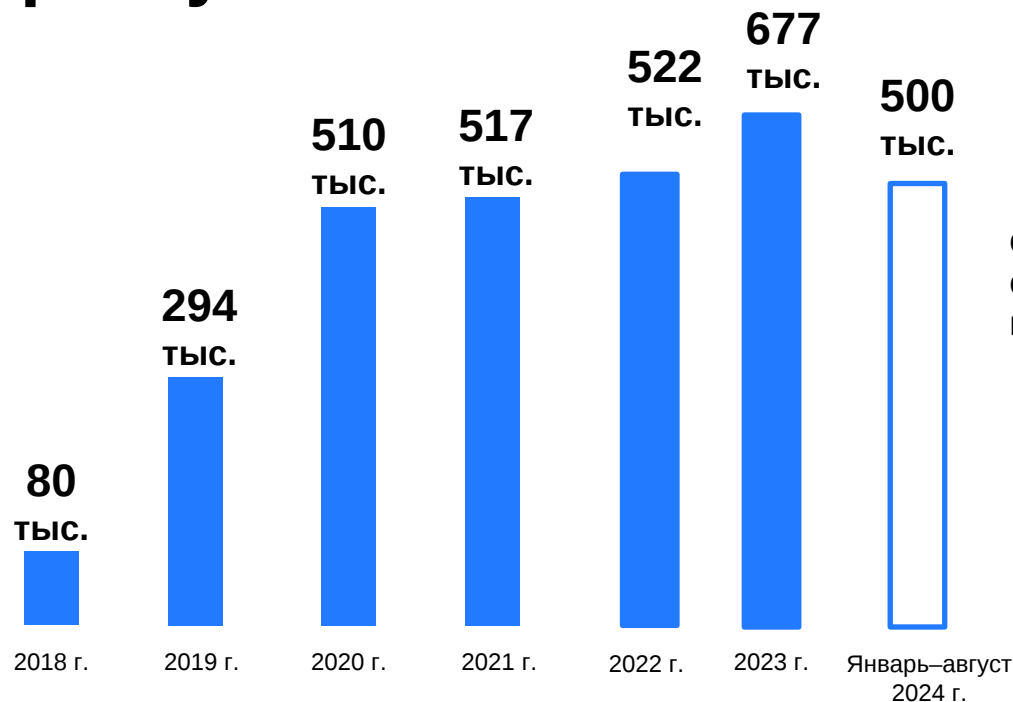


Статистический анализ компьютерных преступлений



1

Статистика компьютерных преступлений в РФ — количество дел



39,2%

от числа всех регистрируемых преступлений
составляют компьютерные преступления —
на 2024 год по данным МВД РФ

Свыше 83,4 % преступлений
совершается
с использованием интернета

Более 46,3 % — с использованием
мобильной связи

[Ссылка на источник данных](#)

Наиболее частые преступления в 2024 году

- Мошенничество
- Кража
- Мошенничество с использованием электронных средств платежа
- Мошенничество в сфере компьютерной информации
- Неправомерный доступ к компьютерной информации
- с целью незаконного производства, сбыта или пересылки наркотических средств
- Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма
- Создание, использование и распространение вредоносных компьютерных программ

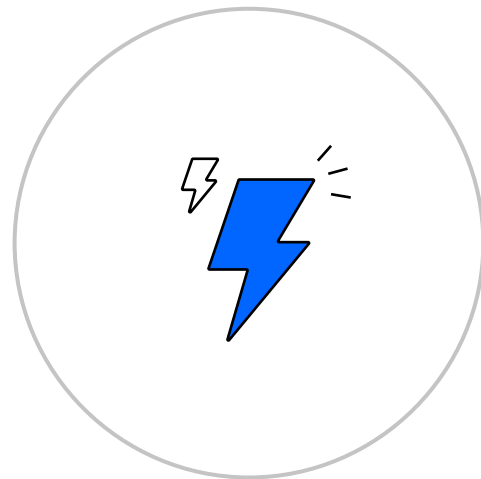




**Как вы думаете,
почему компьютерных
преступлений так много?**

Факторы, влияющие на рост числа преступлений

- Низкая грамотность пользователей
- Широкое распространение устройств с доступом в интернет
- Большое число пользователей банковских приложений и простота использования таких приложений
- Простота совершения преступлений
- Осознание безнаказанности у преступников
- Низкий уровень раскрываемости
- Недостаточно серьёзные санкции за совершение преступления
- Недостаток квалифицированных кадров в правоохранительных органах



Наиболее частые жертвы компьютерных преступлений

- 1 Пенсионеры
- 2 Несовершеннолетние
- 3 Инвалиды

Распространённые сценарии

- Телефонное мошенничество
- Мошенничество в СМС и мессенджерах
- Внедрение вредоносных программ посредством фишинговых атак
- Неправомерный доступ к компьютерной информации посредством фишинговых атак
- Неправомерный доступ к компьютерной информации посредством Ddos-атак
- Атаки на веб-ресурсы в целях нарушения их работоспособности
- Вовлечение в экстремизм/терроризм посредством телефонного мошенничества

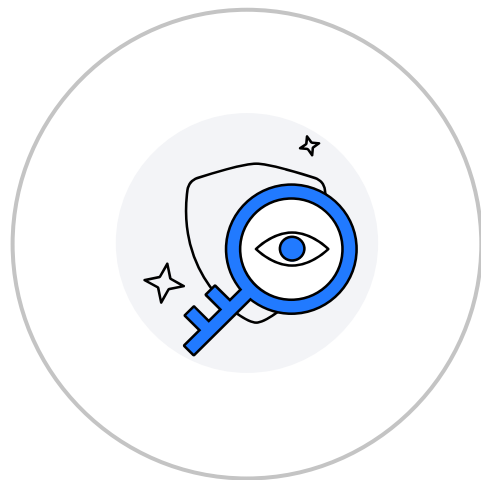




**Как вы думаете,
почему популярны именно
такие способы совершения
преступлений?**

Профилактика преступлений

- Повышение уровня образованности пользователей с точки зрения общей киберграмотности
- Использование программного обеспечения для защиты информации на устройствах, регулярное обновление ПО
- Использование определителей номеров, голосовых помощников, определяющих мошеннические звонки
- Повышение уровня ответственности за совершение такого рода преступлений
- Демонстрация неотвратимости наказания



Выводы

- 1 Отмечается постоянный рост числа компьютерных преступлений
- 2 Ущерб от компьютерных преступлений исчисляется в миллиардах рублей





Ваши вопросы?

Примеры преступлений в сфере компьютерной информации



2



**Что такое преступления
в сфере компьютерной
информации?**

Вспомним

Вопрос: какие статьи УК РФ содержат составы преступлений в сфере компьютерной информации?



Вспомним

Вопрос: какие статьи УК РФ содержат составы преступлений в сфере компьютерной информации?

Ответ:

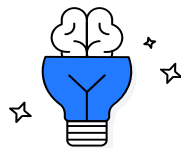
- ст. 272
- ст. 273
- ст. 274
- ст. 274.1
- ст. 274.2



Пример преступления: статья 272 УК РФ*

Некто «А», работник салона оператора связи, с помощью специализированного сайта нашёл номера телефонов, на счетах которых были значительные средства. На рабочем месте он проверил с помощью административно-биллинговой системы наличие денег и выбрал номера для хищения средств.

«А» выпустил новые сим-карты к выбранным номерам, вставил их в своё устройство, вывел средства на собственную платёжную карту, после чего обналичил



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 272. Неправомерный доступ к компьютерной информации



**Как вы думаете,
в чём сложность
квалификации таких
преступлений?**

Пример преступления: статьи 272, 273 УК РФ*

«Б», обладающий специализированными знаниями в области компьютерной техники и ПО, решил использовать специальные программы для «перепрошивки» игровых приставок за вознаграждение.

«Б» по телефону договорился с заказчиком услуги, после чего у себя дома с помощью заранее приобретённого ПО перепрошил приставку и запустил на ней нелицензионные экземпляры игр



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

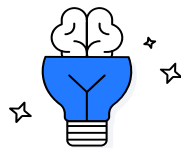
* Ст. 272. Неправомерный доступ к компьютерной информации.

Ст. 273. Создание, использование и распространение вредоносных компьютерных программ

Пример преступления 1: статья 273 УК РФ*

«П», обладающий достаточными знаниями в области информационных технологий, достоверно зная о средствах защиты Интернет-ресурсов, обнаружил на неустановленном интернет-ресурсе объявление о приобретении вредоносных компьютерных программ, позволяющих читать, редактировать, удалять любые файлы на сервере, работать с базами данных, а также работать в консоли сервера.

«П» использовал собственную вредоносную программу путем ее загрузки в файловую структуру заинтересовавшего Интернет-ресурса, изменив его файловую структуру, после чего получил доступ к его административной панели и создал к ней свой пароль, передав доступ к панели и саму вредоносную программу за вознаграждение доступ третьему лицу.



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 273. Создание, использование и распространение вредоносных компьютерных программ

Пример преступления 1: статья 274.1 УК РФ*

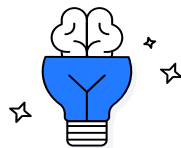
«А», «Б» и «В», сговорившись, атаковали объект оборонной промышленности, чтобы получить финансовую выгоду.

Они нанесли ущерб в размере свыше 650 тыс. руб.

«В» просканировал порты объекта, логины и пароли, передал информацию «А» и «Б».

«А» и «Б», используя эту информацию, заблокировали информацию в ИС и сетях предприятия, что повлекло нарушение рабочего и производственного процесса.

После блокировки «А» и «Б» указали в качестве каналов связи для разблокирования информации адреса электронной почты, а для получения имущественных выгод — биткоин-кошелёк



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

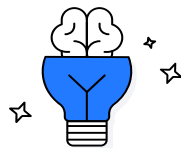
Пример преступления 2: статья 274.1 УК РФ*

«Д», работник оператора связи, имела доступ к:

- персональным данным клиентов
- их платёжным реквизитам
- прочим сведениям из баз данных клиентов

Вступив в сговор с «Н», «Д» со служебного компьютера, используя учётные записи других работников и собственную, получала данные из базы оператора связи о телефонных переговорах и сообщениях клиентов.

Эти данные она передавала «Н» за вознаграждение



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации



**Как вы думаете, почему
преступление квалифицировано
именно по ст. 274.1?**

Выводы

- 1 Способы совершения преступлений в сфере компьютерной информации многообразны
- 2 Чаще всего преступления в сфере компьютерной информации носят корыстный характер
- 3 Наблюдаются проблемы в правильности квалификации преступлений





Ваши вопросы?

Примеры преступлений с использованием информационных технологий



3

Вспомним

Вопрос: чем отличаются преступления в сфере компьютерной информации от преступлений с использованием информационных технологий?



Вспомним

Вопрос: чем отличаются преступления в сфере компьютерной информации от преступлений с использованием информационных технологий?

Ответ:

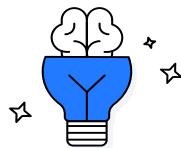
- в первом случае предметом является компьютерная информация
- во втором информация и технологии являются средством совершения преступления



Пример преступления 1: статья 159 УК РФ*

«Р» нашёл объявление на Авито о продаже игровой приставки и аксессуаров на общую сумму 25 тыс. руб.

«Р» связался с продавцом и договорился приобрести товар. В момент получения приставки для подтверждения оплаты он продемонстрировал поддельный снимок экрана банковского приложения



Опишите:

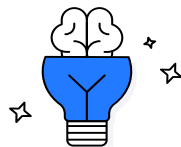
- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159. Мошенничество

Пример преступления 2: статья 159 УК РФ*

“Т”, приискал пустующую квартиру и разместил объявление о сдаче вышеуказанной квартиры на интернет-сайте «Авито.ру», в результате чего встретился в указанной квартире с потерпевшим, представившись собственником указанной квартиры, заключил с потерпевшим договор найма указанной квартиры в устной форме за 16000 рублей в месяц, после чего потерпевший передал ему денежные средства.

Таким образом “Т” похитил денежные средства, после чего с похищенным с места преступления скрылся, распорядился им по своему усмотрению, причинив своими действиями потерпевшему значительный материальный ущерб на указанную сумму.



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

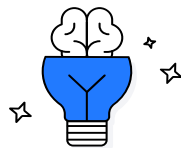
* Ст. 159. Мошенничество



**Как вы думаете,
почему эти преступления
отнесены к совершённым
с применением ИТ?**

Пример преступления 1: статья 159.3 УК*

«Б» нашла чужую платёжную карту Сбербанка.
С помощью бесконтактной оплаты совершила
покупки в 19 магазинах на сумму более 11 тыс. руб.



Опишите:

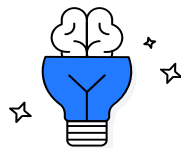
- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.3. Мошенничество с использованием электронных средств платежа

Пример преступления 2: статья 159.3 УК*

«Л» использовал чужую похищенную платёжную карту без ведома потерпевшего. Совершил несколько покупок в различных магазинах и скрылся с товарами.

Своими действиями «Л» ввёл в заблуждение работников магазинов и причинил ущерб владельцу карты



Опишите:

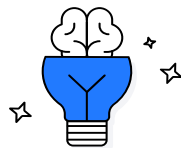
- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.3. Мошенничество с использованием электронных средств платежа

Пример преступления: статьи 158 ч. 3, 159.3 УК РФ

«П» похитила у знакомой платёжную карту,
ПИН-код которой она знала.

«П» сняла через банкоматы 55 тыс. руб.
и совершила покупки в нескольких магазинах
на сумму около 15 тыс. руб.



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 158 ч.3. Кража.

Ст. 159.3. Мошенничество с использованием электронных средств платежа

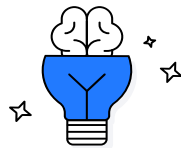


**Как вы думаете,
почему одни действия с картой
квалифицируются по ч. 3 ст. 158,
а другие — по ст. 159.3?**

Пример преступления 1:

статья 159.6 УК РФ*

«Б» отправил с мобильного телефона «Р» СМС на номер сервиса денежных переводов и совершил незаконный перевод 100 тыс. руб. со счёта «Р» на собственный счёт



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

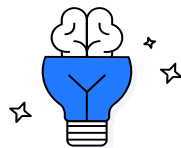
* Ст. 159.6. Мошенничество в сфере компьютерной информации

Пример преступления 2: статья 159.6 УК РФ*

«Д» отправил СМС на номер незнакомого ему «Ш», имитирующее сообщение банка: «Ваша банковская карта заблокирована, информация по номеру...».

«Ш» перезвонил на указанный номер, и «Д» под предлогом проверки клиентов банка, держащих на счетах свыше 5 млн руб., узнал у «Ш» данные его платёжной карты и кодовое слово.

Используя полученную информацию, «Д» с помощью интернет-банка вывел свыше 2 млн руб. со счёта потерпевшего



Опишите:

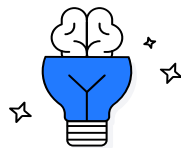
- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.6. Мошенничество в сфере компьютерной информации

Пример преступления 3: статья 159.6 УК РФ*

«З» нашёл чужую платёжную карту и мобильный телефон. Собственника этих вещей он найти не пытался. Прочитав на телефоне СМС о списании денежных средств, «З» понял, что банковская карта привязана к номеру найденного телефона.

С помощью компьютера и услуги «Мобильный банк» он оплатил товары в интернет-магазине более чем на 17 тыс. руб.



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.6. Мошенничество в сфере компьютерной информации



**Как вы думаете,
чем отличаются преступления,
предусмотренные
ст. 159.3 и 159.6?**

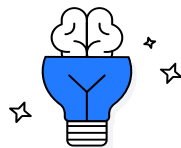
Пример преступления 4: статья 159.6 УК РФ*

«И», зная, что неиспользуемые дольше 180 дней телефонные номера поступают в повторную продажу, приобретал сим-карты с такими номерами.

После приобретения сим-карт «И» проверял, к каким из них подключена услуга управления денежными средствами.

«И» переводил деньги с таких сим-карт с помощью СМС-сервиса на счета других людей, которые потом переводили похищенные средства на его счёт.

Таким образом «И» похитил у нескольких потерпевших свыше 50 тыс. руб.



Опишите:

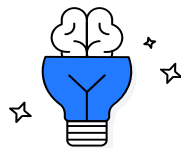
- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.6. Мошенничество в сфере компьютерной информации

Пример преступления 5: статья 159.6 УК РФ*

«Ч», работающий менеджером в отделе по продвижению консалтинговых услуг, получил от работодателя данные для входа в систему заказа железнодорожных билетов.

«Ч» за счёт работодателя заказал через систему 255 билетов на своё имя. Впоследствии он сдал их через кассу вокзала, а полученные наличные средства оставил себе



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.6. Мошенничество в сфере компьютерной информации

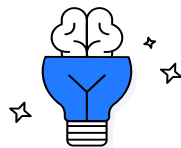
Пример преступления 6: статья 159.6 УК РФ*

«П» получил паспортные данные «К» и придумал, как похитить у него деньги.

Имея паспортные данные, «П» узнал номер банковской карты «К» и номер телефона, к которому она привязана.

В салоне связи «П» перевыпустил сим-карту «К» по его паспортным данным.

После получения сим-карты, «П» получил доступ к мобильному банкингу. Он вывел средства с привязанной карты на QIWI-кошелёк и далее на свой номер с помощью СМС на номер 900



Опишите:

- субъект преступления
- объект преступления
- субъективную сторону
- объективную сторону

* Ст. 159.6. Мошенничество в сфере компьютерной информации

Выводы

- 1 Преступления, совершаемые с использованием информационных технологий, крайне разнообразны
- 2 Именно эти преступления наносят самый значительный материальный ущерб
- 3 Санкции за преступления явно занижены

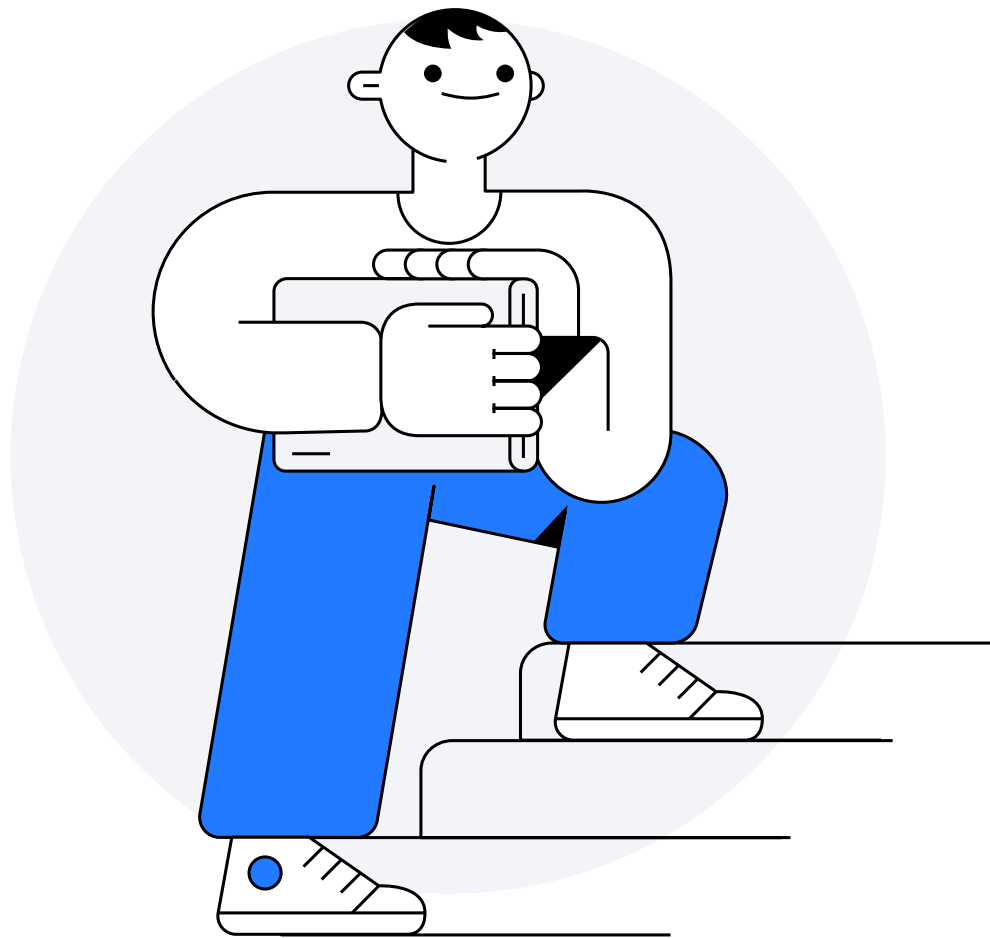


Итоги занятия

- 1 Изучили статистику компьютерных преступлений
- 2 Рассмотрели примеры преступлений в сфере компьютерной информации
- 3 Рассмотрели примеры преступлений с использованием информационных технологий



Домашнее задание



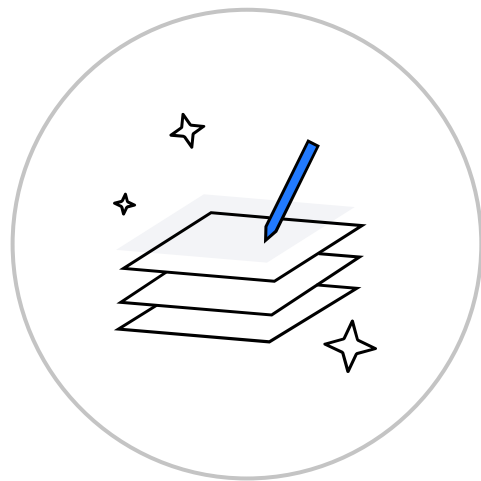
Домашнее задание

Цель: проверка знаний и понимания пройденного материала

Инструменты: Уголовный кодекс РФ

Формат выполнения: Google Документ

Описание: кейсы с задачами в сфере компьютерных преступлений —
подготовка материалов для судебного заседания



Анонс следующего занятия

Деловая игра «Судебное заседание»

По описаниям компьютерных преступлений группам студентов нужно будет определить:

- объект преступления
- предмет преступления
- объективную сторону
- субъект преступления
- субъективную сторону
- признаки состава преступления, под которые попадает деяние
- соответствующее наказание

Во время вебинара мы смоделируем онлайн-заседание суда, выделим роли судей, потерпевших, обвиняемых и т. д.

Анонс следующего занятия

Заполнить минимум за 2 часа до вебинара таблицу «Деловая игра. Таблица распределения ролей»

- Выберите два кейса, в котором вы будете принимать участие. Один кейс — на стороне обвинения, второй кейс — на стороне защиты
- Впишите свою фамилию в соответствующую ячейку
- Содержание кейсов не раскрываем) Распределение нужно для сокращения времени на организационные моменты во время вебинара
- Оставляем за собой право немного корректировать распределение, если оно будет не равномерным

[ссылка на таблицу размещена в личном кабинете](#)

Компьютерные преступления

Оксана Докучаева

