

Сезон 2021/2022

Исследование кибератак



УРОК
ЦИФРЫ

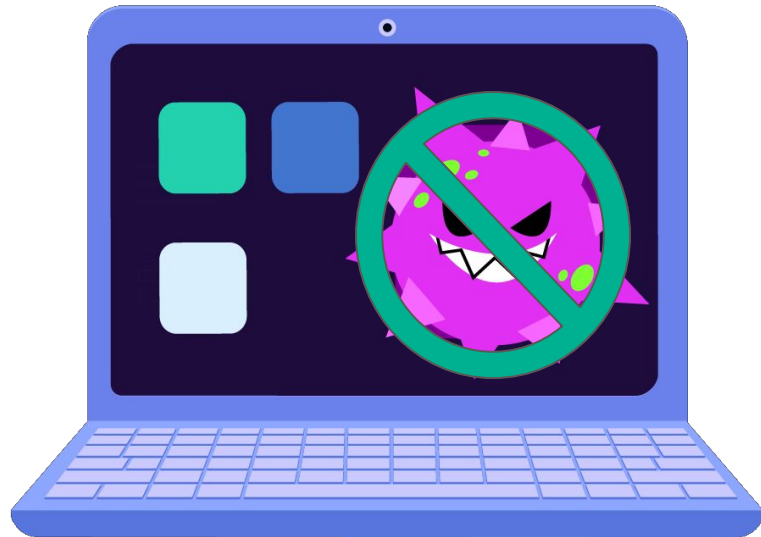
kaspersky

Как найти вирус на компьютере?

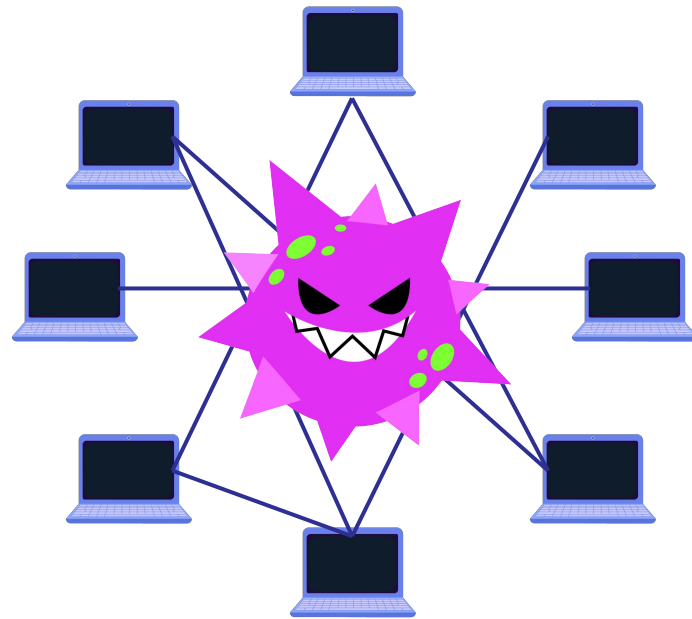


Как найти вирус на компьютере?

Можно воспользоваться антивирусной программой!

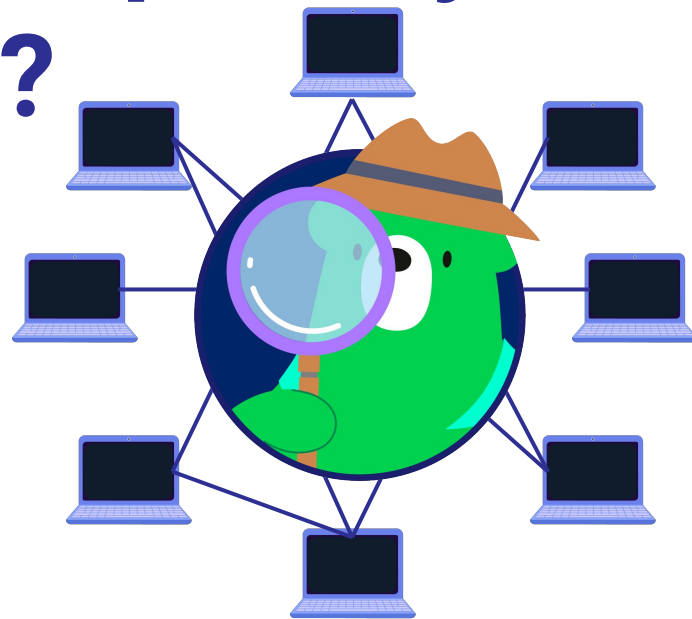


Как исследовать кибератаку в банковской сфере?



Как исследовать кибератаку в банковской сфере?

Это сложная задача, которая требует участия кибердетектива!



Сегодня на уроке

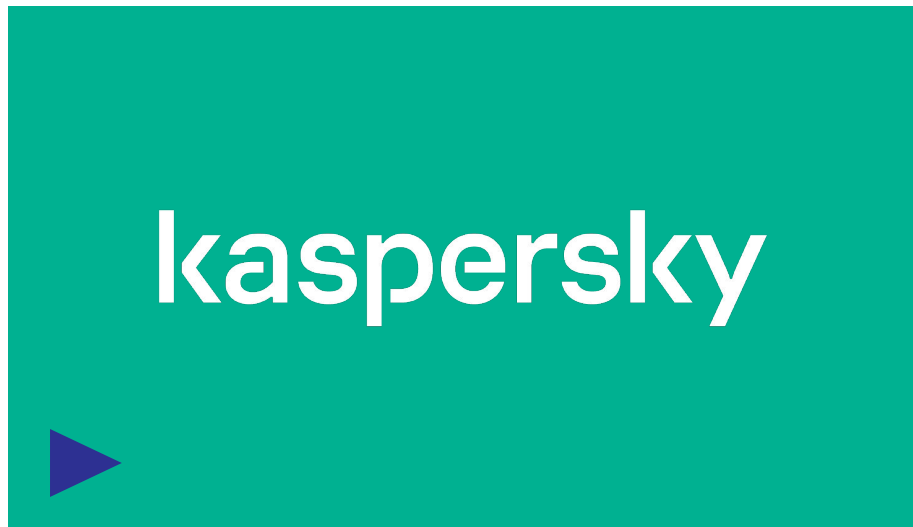
- Познакомимся с понятиями «кибератака» и «киберугроза», узнаем про их разновидности
- Узнаем, как специалистам по кибербезопасности/информационной безопасности (ИБ) удается обнаруживать кибератаки и исследовать их
- Узнаем, как защититься от киберугроз и противостоять злоумышленникам



Посмотрим видео

Посмотрим вводное видео
про исследование кибератак

[Ссылка на видео](#)



Ответим на вопросы




- Что означает понятие «кибератака»?
- Какие разновидности атак можно выделить?
- В чем разница между этими атаками?

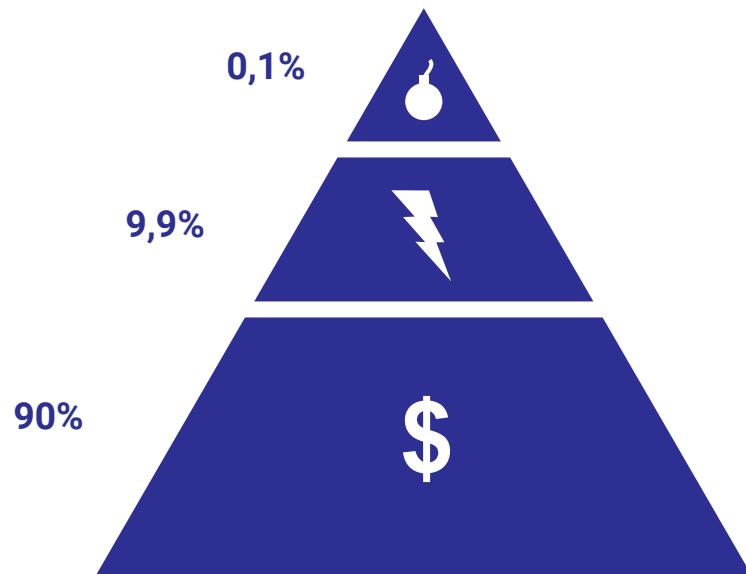
Что означает понятие «кибератака»?

Кибератака (хакерская атака) — это покушение на информационную безопасность цифровой системы.




Это может быть система любой компании (банк, магазин) или устройство отдельного пользователя.

Можно выделить три разновидности кибератак

-  Массовые угрозы
-  Более сложные атаки
-  Самые сложные в техническом плане атаки



В чем различия между этими видами атак?

-  Массовые атаки (ни на кого конкретно не нацелены).
-  Сложные атаки (как правило, нацелены на компании, а не на рядовых пользователей).
-  Самые сложные в техническом плане атаки (направлены на конкретный объект (компания, государственная организация или высокопоставленный человек)).

Что делает специалист по ИБ?



Что делает специалист по ИБ?

Занимается изучением кибератак и пытается определить, кто к ним причастен:

- изучает кибератаки;
- анализирует полученные данные, выстраивает логику кибератаки;
- рекомендует меры защиты от атак;
- ГОТОВИТ отчеты по итогам исследования.



Исследование кибератак

В исследовании кибератак можно выделить несколько этапов:



**Реагирование
на атаку**



**Анализ
атаки**



**Устранение
последствий**

Исследование кибератак



**Реагирование
на атаку**

Специалист по ИБ получает запрос на исследование кибератаки от потерпевшей стороны (или сам замечает подозрительную активность).

На этом этапе ему важно собрать улики для дальнейшего исследования атаки.

Исследование кибератак



**Анализ
атаки**

На этом шаге специалист по ИБ отвечает на вопросы: каким образом произошла кибератака? Какими лазейками воспользовались хакеры?

Для этого специалист по ИБ изучает найденные улики, анализирует уязвимости системы.

Исследование кибератак



**Устранение
последствий**

Когда становится ясно, как произошла кибератака, специалист по ИБ предлагает рекомендации по улучшению системы безопасности для предотвращения повторения инцидента.

Какими навыками нужно обладать специалисту по ИБ, чтобы успешно справляться с такими задачами?



Навыки специалиста по ИБ

- ★ Знать правила информационной безопасности
- ★ Разбираться в том, как работают программы
- ★ Знать языки программирования
- ★ Уметь аналитически мыслить
- ★ Быть любознательным



**Давайте вместе проверим,
насколько хорошо вы знаете
правила информационной
безопасности и готовы быть
специалистом по ИБ.**



**Приготовьте лист бумаги и ручку.
Напишите числа от 1 до 10.**

Вопрос 1: Установлен ли антивирус на вашем компьютере, смартфоне?

1. На всех устройствах
2. Только на компьютере
3. Только на смартфоне
4. Нет, а зачем...

Вопрос 2: Какой сайт для покупки билетов можно считать безопасным?

1. <http://tickets.xyz.ru>
2. <http://tickets.com>
3. <https://tickets.ru>

Вопрос 3: Одинаковый ли у вас пароль от почты и социальных сетей?

1. Да, одинаковый
2. Нет, разный

Вопрос 4: Какой из этих паролей безопасный?

1. 12345678qwerty
2. kot_vasiliy
3. roman9876543210
4. Dog_2010Shzrzk!
5. 876543210

Вопрос 5: Из каких источников вы обычно скачиваете файлы (программы, фильмы, игры, книги)?

- 1. Регулярно что-то качаю (фильмы, программы, книги) из самых разных источников**
- 2. Качаю много, в основном с одних и тех же проверенных мной сайтов**
- 3. Скачиваю только лицензионную продукцию из интернет-магазинов и магазинов приложений**

Вопрос 6: Вам пришло обновление операционной системы, что сделаете?

1. Не буду устанавливать. Не хочу, чтобы скорость Интернета падала
2. Соглашусь на установку. Вдруг что-то важное
3. Потом установлю, может быть
4. А мне операционная система не предлагает ничего...

Вопрос 7: Вы получили следующее сообщение, ваше действие?

«Извините, случайно по ошибке положил на ваш номер 300 рублей, верните мне их на этот номер: +7(XXX)0123456»

1. Верну деньги на указанный номер
2. Перезвоню по этому номеру, чтобы выяснить детали
3. Проигнорирую сообщение

Вопрос 8: Что вы делаете, если в социальной сети вам приходит сообщение от незнакомого человека с просьбой добавить в друзья?

- 1. Обычно я добавляю в друзья всех желающих, чем больше людей в друзьях — тем круче**
- 2. Я добавляю в друзья только тех людей, которых знаю лично**
- 3. Добавляю, если человек — друг моего друга**

Вопрос 9: Какая информация о вас в социальных сетях находится в открытом доступе, то есть видна не только друзьям?

- 1. Имя и картинка на заставке**
- 2. Ф.И.О., фотографии, посты**
- 3. Много всего, я не ограничиваю настройки видимости**
- 4. Никогда не задумывался об этом**

Вопрос 10: Вы хотите скачать песню Beatles Yesterday и нашли несколько вариантов в Интернете. Какие из них скачаете?

1. Yesterday-Beatles-Song.scr
2. Beatles_All_songs.zip
3. Beatles_Yesterday.exe
4. Beatles_Yesterday.mp3

Проверим ответы

№ Ответ:

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

**Ответили верно, ставьте «+»,
если нет, то «-».**

Подсчитайте количество «+».

Результаты викторины

9–10 баллов. Поздравляем, вы надежно защищены!

7–8 баллов. Хороший результат, но есть над чем поработать.

0–6 баллов. Нужно изучить правила информационной безопасности.



Подведем итоги

Посмотрим видео ролик.

[Ссылка на видео](#)



Подведем итоги

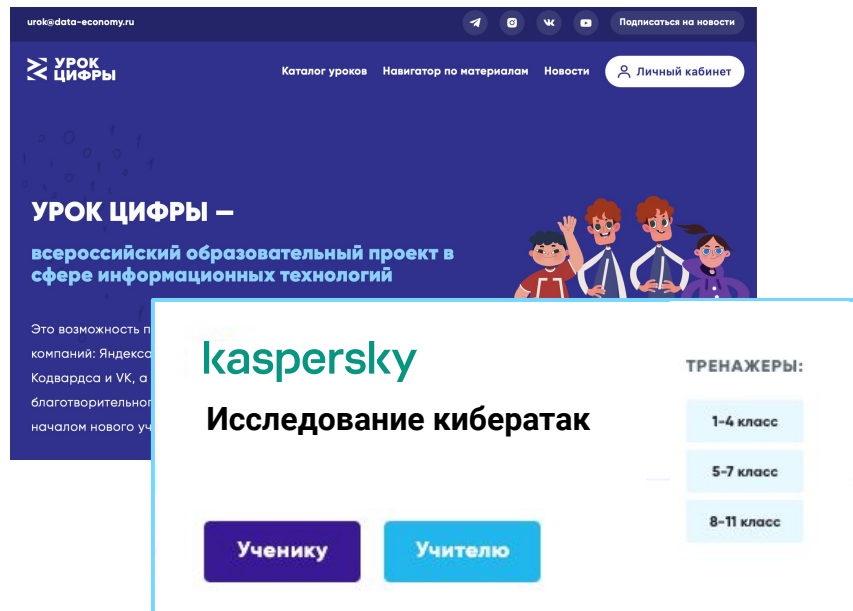
- **Что больше всего запомнилось из урока?**
- **Что нового и полезного узнали?**
- **Что будете использовать в повседневной жизни?**



Домашняя работа

Зайдите на сайт [урокцифры.рф](https://urokцифры.рф), найдите урок «Исследование кибератак», ознакомьтесь с материалами на сайте.

Пройдите тренажер и получите сертификат о прохождении урока.



The screenshot shows the website interface for 'urokцифры'. At the top, there is a navigation bar with the site logo, 'Каталог уроков', 'Навигатор по материалам', 'Новости', and a search bar for 'Личный кабинет'. Below the navigation, the main heading reads 'УРОК ЦИФРЫ – всероссийский образовательный проект в сфере информационных технологий'. An illustration of four diverse children is positioned to the right. A text block on the left describes the project's goal: 'Это возможность... компаний: Яндекс... Кодвардса и VK, а... благотворительно... началом нового уч...'. Overlaid on the bottom right is a white box containing the 'kaspersky' logo, the lesson title 'Исследование кибератак', and a 'ТРЕНАЖЕРЫ:' section with three buttons for '1-4 класс', '5-7 класс', and '8-11 класс'. At the bottom of this box are two buttons: 'Ученику' (purple) and 'Учителю' (light blue).


Полезные ресурсы

kaspersky daily

Продукты ▾ Как купить Продлить Скачать Поддержка Об угрозах Акции Блог ▾

Свежее


фишинг



Распространенные уловки таргетированного фишинга

Чтобы быть готовым к целевым атакам, сотрудникам ИБ необходимо как можно скорее узнавать о таргетированном фишинге в почтовых ящиках коллег.


обман



5 признаков онлайн-мошенничества

Главные признаки, которые подскажут, что вам пишет мошенник.

права




Матрица: Воскрешение. Работа над ошибками

Смотрим, что изменилось в Матрице за 18 лет, прошедших с прошлого обновления.

www.kaspersky.ru/blog/

KIDS SAFE MEDIA



Мидори Кума и необычная гонка

Приключения с Мидори Кума Начинаются!

Вы когда-нибудь видели зелёного медведя?
Если нет, то вот он, смотрите скорее!

Мидори Кума – совершенно особенный медведь из книги «Мидори Кума и необычная гонка».

Скачать книгу

kids.kaspersky.ru/midori