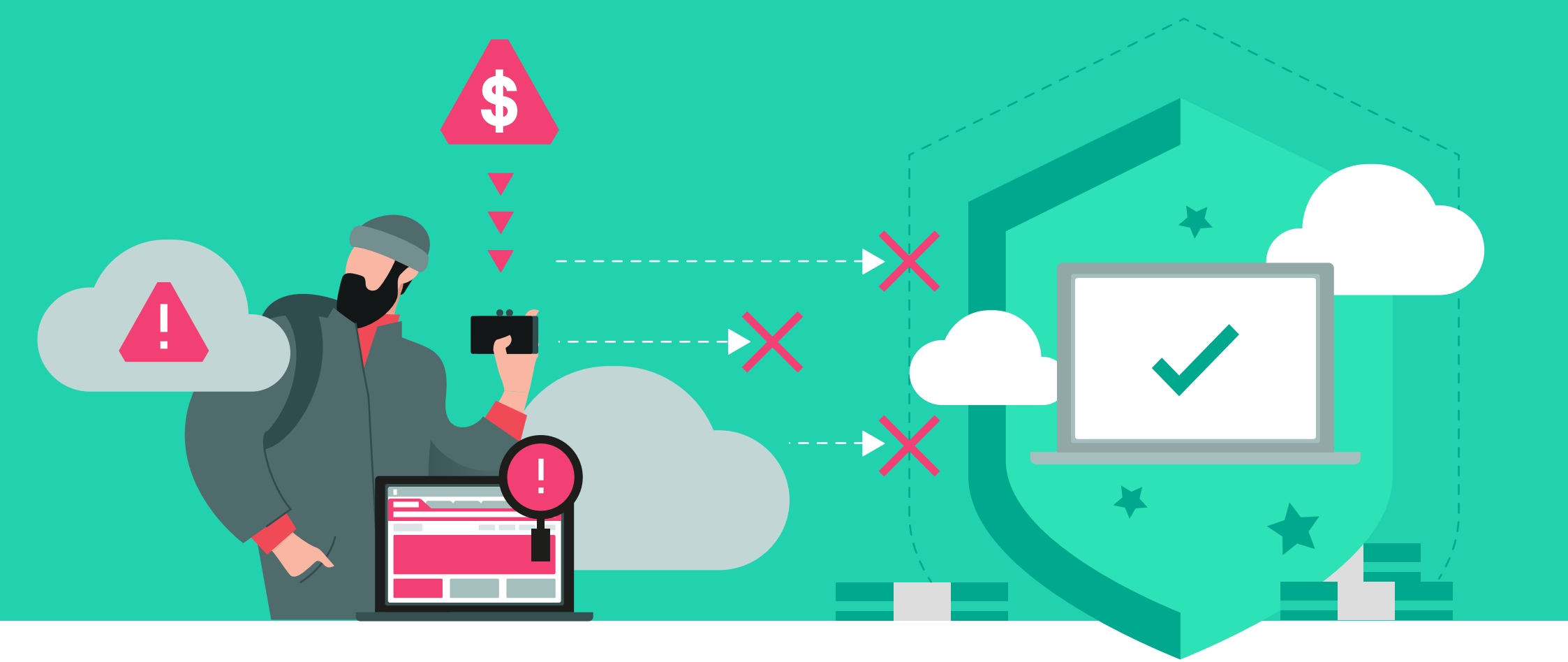


# Преимущество решений «Лаборатории Касперского» для защиты от программ-вымогателей

kaspersky

## Проблема

В 2020 году программы-вымогатели заняли прочное место в ландшафте киберугроз. Они постоянно эволюционируют. Злоумышленники проводят все больше целевых атак на конкретные организации и отрасли, требуя более крупные выкупы, чем прежде. Затраты из-за простоев, связанных с потерей доступа к данным, значительно выросли. Неизвестные киберпреступные группы постоянно создают новые семейства вымогателей. В результате такие программы стали одной из самых серьезных угроз IT-безопасности в SMB-сегменте.

## Решение

Передовая специализированная защита «Лаборатории Касперского» решает эту и многие другие проблемы. Наши продукты включают облачный поведенческий анализ для обнаружения и блокирования программ-вымогателей, в том числе шифровальщиков, защиту облачных рабочих нагрузок, виртуальных и физических рабочих мест и общих сетевых ресурсов, а также откат вредоносных действий.

# 2020 год в цифрах

## В 40 млрд $

**ОЦЕНИВАЕТСЯ МИРОВОЙ УЩЕРБ,**
ожидаемый в 2020 г. в связи с выплатой выкупов вымогателям и простоями [1]

## В 23 РАЗА

**ЗАТРАТЫ, СВЯЗАННЫЕ С ПРОСТОЯМИ, ПРЕВЫШАЮТ**
среднюю сумму требуемого выкупа (по данным исследования[2])

## 141 000 $

**СОСТАВЛЯЛ СРЕДНИЙ УЩЕРБ ИЗ-ЗА ПРОСТОЕВ**
в связи с атаками программ-вымогателей в 2019 г. (на 200% больше, чем в 2018 г.)[3]

[1] Ransomware Demands: $170B Worldwide Forecast in 2020, Report (отчет «Прогноз об общей сумме требуемых выкупов в 2020 г.: 170 млрд долларов США»)
[2] Datto's Global State of the Channel Ransomware Report 2019 (отчет компании Datto о ситуации с программами-вымогателями в сфере поставщиков управляемых услуг, 2019 г.)
[3] Help Net Security: каждая пятая компания из SMB-сегмента подверглась атаке программы-вымогателя

## 62,4%

**КОМПАНИЙ ПОДВЕРГЛИСЬ АТАКАМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ**
(по данным глобального опроса IT-директоров в 2019 г.[4])

## 30%

**АТАК ШИФРОВАЛЬЩИКОВ В 2019 ГОДУ**
были направлены на корпоративных пользователей[5]

## 20%

**МАЛЫХ И СРЕДНИХ КОМПАНИЙ**
в 2019 г. подверглись атакам программ-вымогателей[2]

[4] Statista: процент организаций по всему миру, подвергшихся атакам программ-вымогателей с 2017 по 2019 г.)
[5] Каждая третья атака программ-вымогателей направлена на корпоративных пользователей: в День борьбы с шифровальщиками «Лаборатория Касперского» и Интерпол напоминают о важности резервного копирования и защиты данных

## 21%

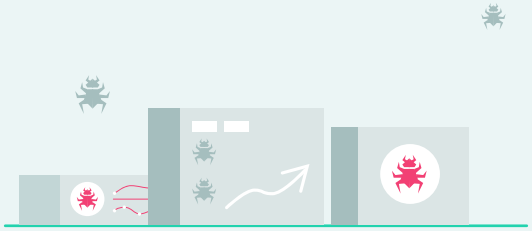
**СОСТАВЛЯЕТ ДОЛЯ АТАК С ИСПОЛЬЗОВАНИЕМ WANNACRY**
среди всех выявленных атак программ-вымогателей в 2019 году[5]

## 22

**НОВЫХ СЕМЕЙСТВА ПРОГРАММ-ВЫМОГАТЕЛЕЙ**
и **46 156** модификаций шифровальщиков было выявлено исследователями[6]

## 49%

**АТАК ВЫМОГАТЕЛЕЙ В I КВАРТАЛЕ 2020 Г.**
проводились с использованием шифровальщиков[7]



[6] Kaspersky Security Bulletin 2019. Статистика
[7] Отчет KSN: программы-вымогатели в 2018–2020 гг.)

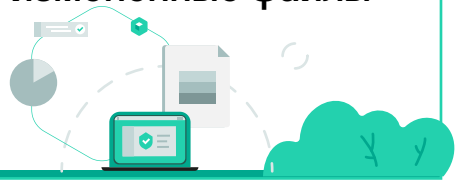
Решения «Лаборатории Касперского» предлагают современную многоуровневую защиту, которая блокирует программы-вымогатели как на этапе доставки, так и на этапе выполнения.

## Защита от эксплойтов

Защита от эксплойтов не дает вредоносным программам (в том числе вымогателям) проникнуть в систему, используя уязвимости ПО. Она срабатывает в ответ на подозрительные действия и анализирует поведение, сравнивая его с вредоносными шаблонами. Специальные сигнатуры применяются для обнаружения вредоносных файлов, использующих эксплойты, до того, как эти файлы будут открыты. Проактивная защита позволяет отслеживать вредоносное ПО и сразу блокировать его при открытии файла.

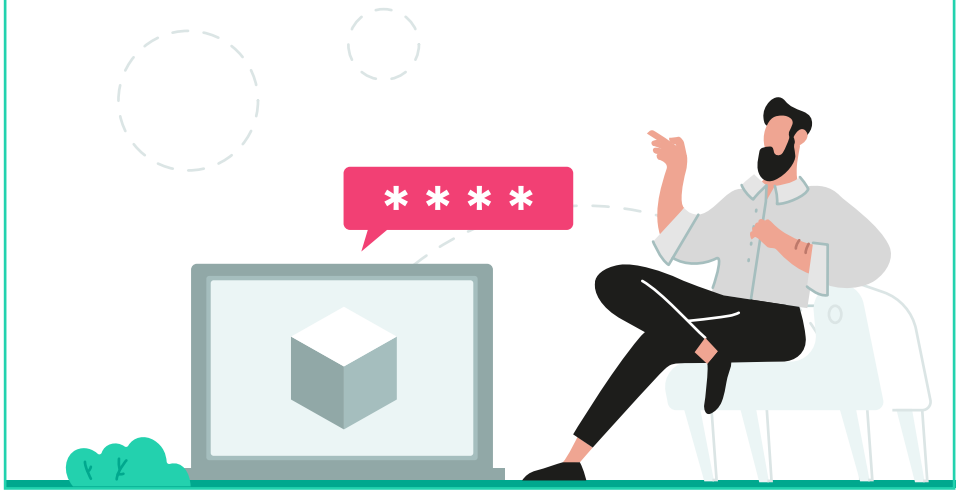
## Анализ поведения на основе машинного обучения (с автоматическим откатом изменений)

Технологии «Лаборатории Касперского» на основе машинного обучения находят ранее неизвестное вредоносное ПО (в том числе программы-вымогатели), используя большие массивы аналитических данных об угрозах и создавая эффективные модели обнаружения. Они работают как в среде компании, так и в лабораторных условиях, опираясь на несколько уровней безопасности.
В решениях «Лаборатории Касперского» также реализована функция отката вредоносных действий, которая позволяет отменить действия вредоносных программ (например, восстановить измененные файлы и системный реестр).



## Управление шифрованием

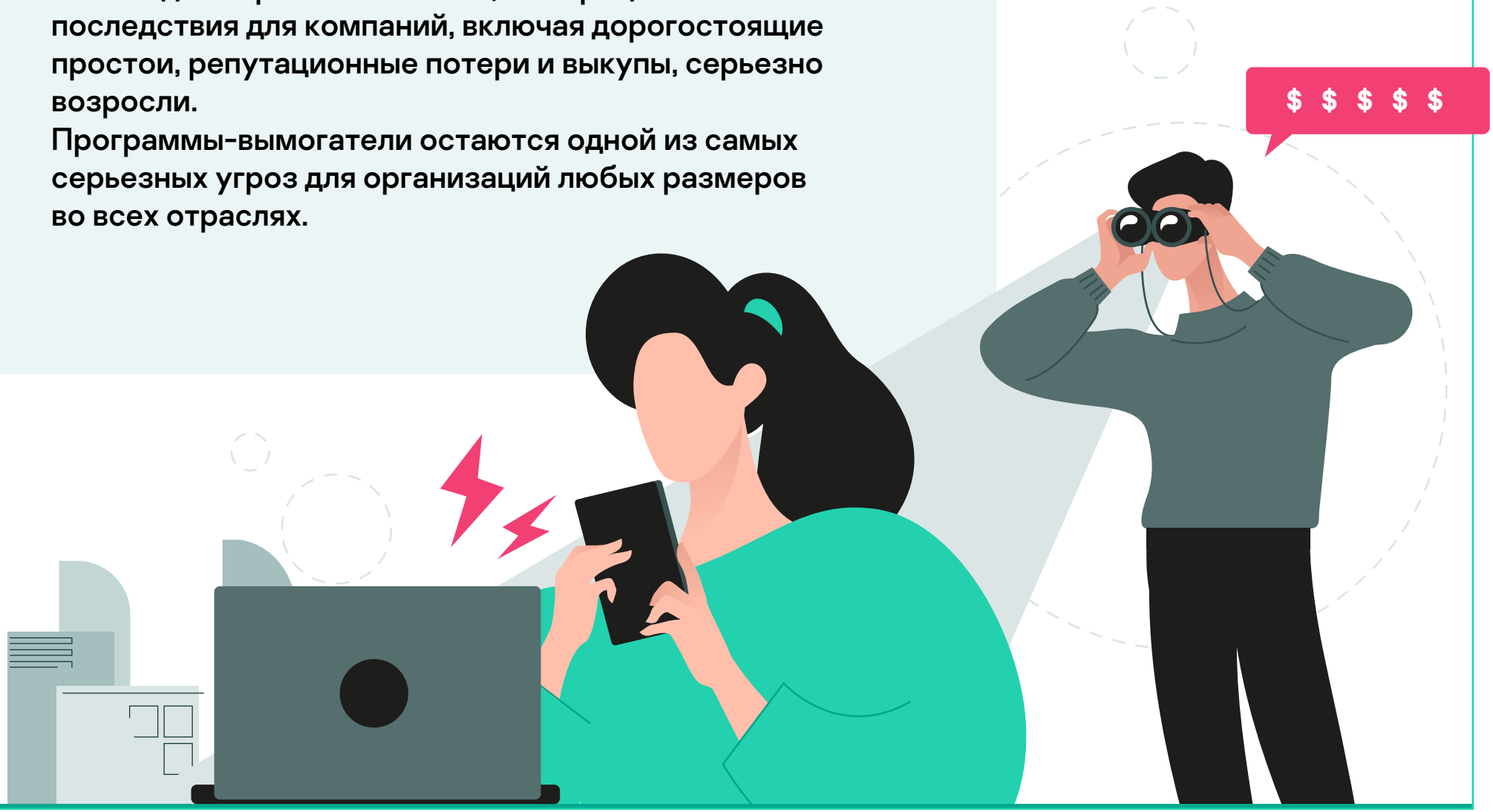
«Лаборатория Касперского» помогает настроить шифрование устройств на базе Windows и macOS, предотвращая несанкционированный доступ к данным. Полное шифрование диска предотвращает утечку информации при потере устройства. Шифрование файлов защищает их при передаче по непроверенным каналам. А подсистема Crypto Disk сохраняет зашифрованные пользовательские данные в отдельном файле.




## Оценка уязвимостей и управление установкой исправлений

Оценка уязвимостей и управление установкой исправлений не позволяют вредоносному ПО, в том числе программам-вымогателям, использовать недавно обнаруженные и незакрытые уязвимости операционных систем и распространенных приложений. Наши технологии автоматизируют проверку ПО на наличие уязвимостей, установку исправлений и обновлений, а также развертывание приложений, и все это – из единой консоли управления.

Хотя общее количество атак программ-вымогателей в последнее время снизилось, их отрицательные последствия для компаний, включая дорогостоящие простои, репутационные потери и выкупы, серьезно возросли.
Программы-вымогатели остаются одной из самых серьезных угроз для организаций любых размеров во всех отраслях.

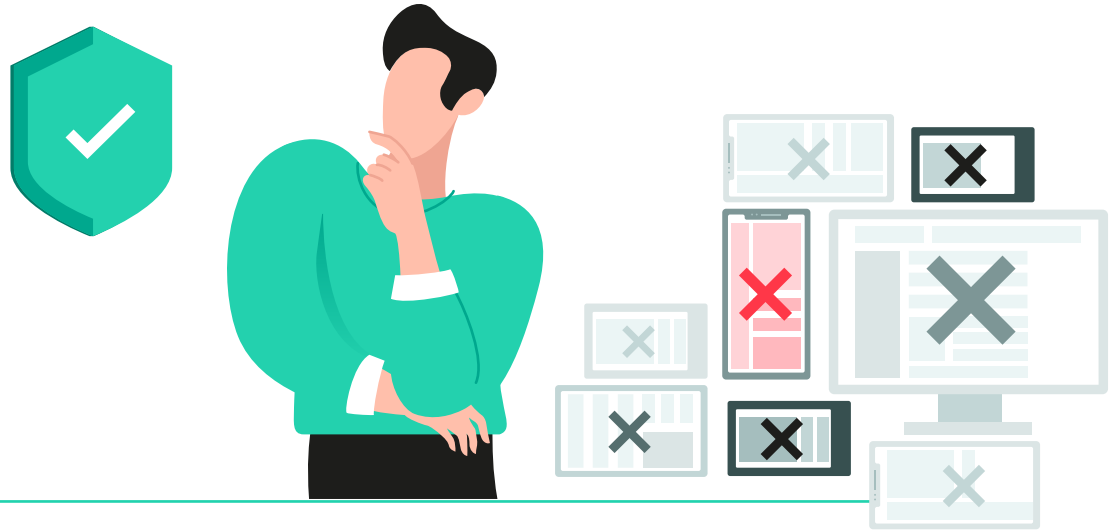


## Как защититься от программ-вымогателей?

- Регулярно делайте резервные копии данных, чтобы их можно было восстановить в случае инцидента.
- Используйте инструменты для автоматического обнаружения уязвимостей и установки исправлений (патч-менеджмент).
- Своевременно обновляйте приложения и операционные системы на всех устройствах.
- Остерегайтесь фишинговых атак, поддельных сообщений и ссылок, потенциально вредоносных файлов.
- Проведите обучение сотрудников. В этом вам помогут тренинги, например платформа Kaspersky Automated Security Awareness Platform.
- Используйте эффективную многоуровневую защиту, например линейку решений Kaspersky Security для бизнеса, а для личных устройств Kaspersky Total Security, чтобы противостоять программам-вымогателям и откатывать изменения, которые они внесли.

# Что делать при заражении программой-вымогателем?

- Отключитесь от интернета.
- Не платите выкуп. Одна треть жертв не может восстановить доступ к данным даже после выплаты выкупа.
- Немедленно обратитесь за технической поддержкой, чтобы восстановить данные.
- Используйте ресурсы для восстановления файлов, например, на платформе No More Ransom, где размещено более 100 бесплатных инструментов для дешифрования.



kaspersky