

# Кибербезопасность

---

В условиях информационных спецопераций



18.03.2022

Александр Фадеев

Проректор по цифровизации

# Пароли

В случае подбора вашего пароля, злоумышленник от вашего имени сможет рассылать и выводить на печать экстремистские материалы, подписывать документы, получать доступ к корпоративной информации и внутренним ресурсам сети. При этом вся ответственность останется за вами!

Пароль из цифр, строчных и заглавных букв:



## Почему нельзя использовать простые пароли?

- Простые комбинации типа «qwerty» и «12345678», все слова из английского и русского словаря, все даты за последние 100 лет перебираются роботами-взломщиками за доли секунды



## Самый надежный пароль:

Двухфакторная авторизация через СМС

## Когда категорически необходимо поменять пароль?

- если ваш пароль состоит из даты (рождения), или одного слова, или последовательности на клавиатуре (типа, «qwerty»)
- если вы хоть раз сохраняли пароль на облачном сервисе (диске, заметках)
- если вы хоть раз пересылали пароль по сети (электронная почта, мессенджер, СМС)
- если вы хоть раз передавали пароль хоть кому-либо
- если вы хоть раз оставляли пароль на видном месте (на мониторе, под стеклом стола и т.д.)
- если вы использовали пароль на разных сайтах
- если вы сохраняли пароли в браузерах
- если вы вводили пароль на сенсорной клавиатуре



# Облачные сервисы

Все, что размещено на облаке –  
вам не принадлежит



## Чему угроза:

- Файлы на облачных хранилищах: DropBox, GoogleDrive, AppStore, OneDrive, ...
- Электронная почта на иностранных серверах
- Переписка в мессенджерах
- Веб-приложения (общие документы, доски, сайты, заметки, ...)

## Что делать:

- Сделать копию всех документов на локальный компьютер, на доверенное облако, на съемный носитель.
- Удалить файлы, документы, письма с облаков
- Перейти на российские электронную почту, видеоконференцсвязь, общие документы

## В чем угроза:

- Чтение, анализ, поиск по словам
  - (в файлах, письмах, сообщениях)
- Распространение личной информации
- Рассылка от вашего имени
- Авторизация на третьих сервисах
- Блокировка, недоступность

## Лицензия на программное обеспечение может стать недействительной



### В чем угроза:

Отзыв лицензий для проприетарного (коммерческого) программного обеспечения, ПО перестает работать, возможна блокировка компьютера/смартфона

### Что делать:

1. Сделать копии всех важных данных на съемные носители
2. Сделать копии инсталляций программ, операционных систем, ключей
3. Временно отключить все обновления, заблокировать сайты производителей ПО
4. Перейти на отечественное ПО
5. Перейти на свободно распространяемое ПО с открытым (!) кодом
6. Сделать копию адресной книги смартфона

<https://habr.com/ru/news/t/655381>



<https://freeanalogs.ru>



<https://alternativeto.net>







## «iFRAME-закладки» и скрипты чужих сайтов HTTPS:// - защита соединения с сайтом

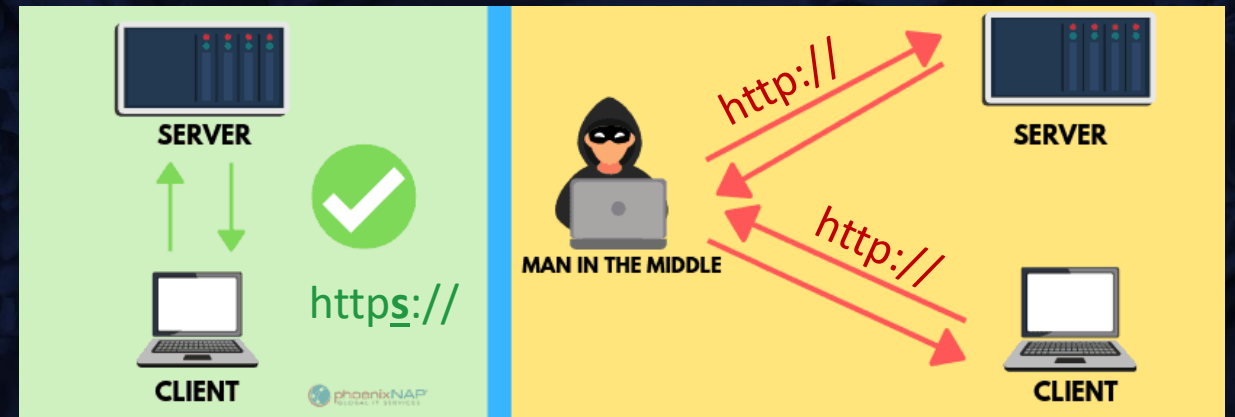
Вместо видеоплеера с сервера может быть загружена экстремистская информация, видео или фишинговая программа злоумышленника

**Удалить:** метрики, статистику, блоки рекламы, iFrame, Carpa, все java-скрипты сторонних систем

Без SSL злоумышленник может осуществить:

- Подмену информации
- Перехват и просмотр информации

```
4 <meta charset="UTF-8">
5 <meta name="viewport"
  content="width=device-width, initial-scale=1.0">
6 <link rel="stylesheet"
  href="css/style.css">
7 <title>Form</title>
8 </head>
9
10 <body>
11 <div class="wrap">
12 <h1>Embeds</h1>
13
14 <h2>iFrame</h2>
15 <iframe src="https://...com"
  frameborder="2" width="100%"
  height="300px"></iframe>
16
17 <h2>Audio</h2>
18
19 <h2>Video</h2>
20
21 </div>
22 </body>
23 </html>
24
```



## Любой посредник – шпион



VPN и Прокси позволяют отправлять ваши запросы от имени компьютера в другой стране

### В чем угроза:

- Все передаваемые данные через посредника – могут просматриваться, подменяться, удаляться:
  - **Пароли, переписка, данные банковских карт, просмотренная информация и т.д.**



# Базовые принципы личной кибербезопасности

Будьте бдительны!



## Электронная почта

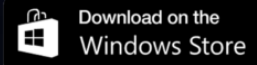
- Не открывайте электронные письма от неизвестных отправителей.
- Не нажимайте на ссылки, картинки и кнопки в электронных письмах
- Никогда не запускайте программы, присланные по электронной почте

## Оплата картой

<https://vash.bank.ru/...>

- Платите только на сайтах проверенных банков, с реальным адресом
- Платите только картой с ограниченным балансом
- Используйте одноразовые коды для подтверждения каждого платежа
- Не сохраняйте данные банковской карты

## В Интернете



- Устанавливайте программы только с официальных маркетов и сайтов производителей
- Не скачивайте файлы, расширения и программы, на неизвестных сайтах
- Не запускайте неизвестные программы
- Установите разработанный в России антивирус
  - Браузер, поисковик, офис...

## Сеть учреждения

1. DDoS атаки: Огромное количество безобидных запросов. Парализуют ваши серверы.
  1. Отключать зоны-источники атак на время (договор с провайдером, два провайдера)
2. Поиск уязвимостей на компьютерах сети: Подключение к компьютеру, внедрение вредоносного кода, **включение компьютера в хакерские сети**
  1. Жесткая блокировка портов – точек подключения к компьютеру
  2. Удаление всех программ, позволяющих подключиться (Radmin, Torrent, p2p...)
  3. Удаление любых серверов с персональных компьютеров (сайты, ftp...)
  4. Удаление нелегальных и взломанных программ
  5. Перенос компьютеров в сети с «серыми IP-адресами» 10.x.x.x, 172.16-31.x.x, 192.168.x.x
  6. **Отключить неиспользуемые службы, сервисы, устройства, пользователей. Инвентаризация. Ведение журнала инцидентов.**
3. Поиск уязвимостей на сетевом и офисном оборудовании (принтеры, роутеры)
4. Установка вредоносного ПО под предлогом «супер-антивируса»: Обычный компьютер превращается в агента сети компьютерных атак. Использовать легальный антивирус.
5. Полное отключение интернета страны
  1. Переход на отечественные DNS-системы




# Спасибо за внимание


---

**Фадеев А.С.**

Проректор по цифровизации

 Томск, проспект Ленина, 30

 +7-923-457-9515

 [fas@tpu.ru](mailto:fas@tpu.ru)