Банк России

# КИБЕРБЕЗОПАСНОСТЬ – НАШИ ДНИ

2021 г.

# СЕГОДНЯ ВЫ УЗНАЕТЕ:

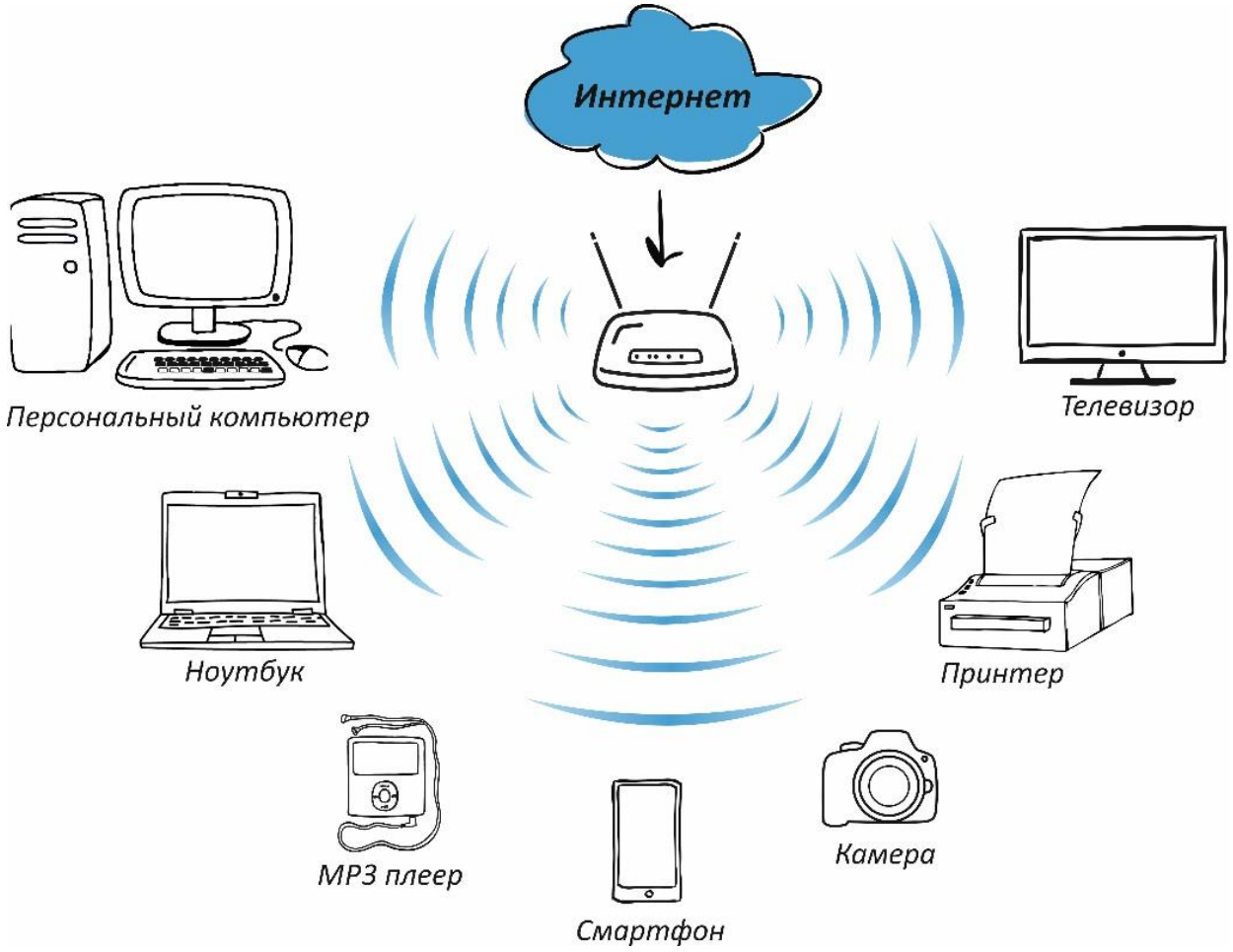
- Какие виды мошенничества существуют в сети Интернет
- Как мошенники могут получить данные о вас и ваших банковских картах
- Какие приемы обмана используют кибермошенники
- Как защититься от киберпреступников

# Что такое КИБЕРПРОСТРАНСТВО ?

**КИБЕРПРОСТРАНСТВО** - это среда информационного взаимодействия и обмена данными в компьютерных сетях и сетях связи.

**Элементами** киберпространства являются серверы, компьютеры, мобильные гаджеты, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети.

**Кибербезопасность** – комплекс мероприятий, направленных на сохранение основных свойств информации в киберпространстве: конфиденциальности, целостности и доступности.



# Основные виды киберугроз

- Социальная инженерия (в т.ч. фишинг, мошенничество с банковскими картами)
- Вредоносное ПО (шифровальщики/вымогатели, трояны, ботнеты, шпионское ПО)
- Эксплуатация веб-уязвимостей
- Хакинг (целенаправленный взлом)
- Сетевые (распределенный отказ в обслуживании (DDoS), изменение маршрутизации и др.)
- «Человек посередине»

# Статистика роста инцидентов по видам кибератак

| | 2020 | 2021 |
|---|---|---|
| | II квартал | II квартал |
| Атаки, направленные на клиентов финансовых организаций. Фишинговые атаки | 583 | 1 160 ▲ +99% |
| Атаки, направленные на клиентов финансовых организаций. Атаки с использованием методов социальной инженерии | 4 589 | 11 173 ▲ +143% |
| Атаки, направленные на финансовые организации. Атаки с использованием ВПО* | 103 | 112 ▲ +9% |
| Атаки, направленные на клиентов финансовых организаций. Эксплуатация уязвимостей программного обеспечения | 186 | 56 ▼ -70% |
| Остальные инциденты | 113 | 251 ▲ +122% |

** Вредоносное программное обеспечение.*

*Из отчета обзоров об инцидентах информационной безопасности при переводе денежных средств за II квартал 2021 года Банка России

# Социальная инженерия

Это метод манипуляции действиями человека, заключающийся в использовании слабостей человеческого фактора в целях незаконного получения личной информации (учетных или банковских данных) или несанкционированного доступа к компьютеру жертвы с целью установки на него вредоносного ПО.

# Социальная инженерия

## Звонок «специалиста» - один из самых популярных способов мошенничества

### Основные признаки :

1) Звонок или СМС с незнакомого номера;
2) Разговор о сохранении или увеличении ваших денег;
3) Вас просят сообщить персональные данные;
4) Вас выводят из равновесия;
5) На вас давят, торопят, не дают обдумать решение.

### Мошенники могут представляться:

1) специалистами банка
2) врачами
3) соцработниками
4) менеджерами турагентства
5) сотрудниками МВД, суда, Банка России.
6) технической поддержкой портала «Госуслуг» и т.д.

### Могут предлагать:

1) уникальное лекарство
2) секретную вакцину
3) несуществующие льготы, пособия и компенсации
4) ссылаясь на несуществующие законы, угрожать штрафом, судом и т.д.

# Фишинг («рыбная ловля»)

Это тип мошенничества, при котором преступники выдают себя за надежный источник в Интернете, чтобы вынудить жертву передать им личную информацию (логин, пароль, персональные данные, данные банковских карт т.д.)

- Поддельные сайты и сервисы

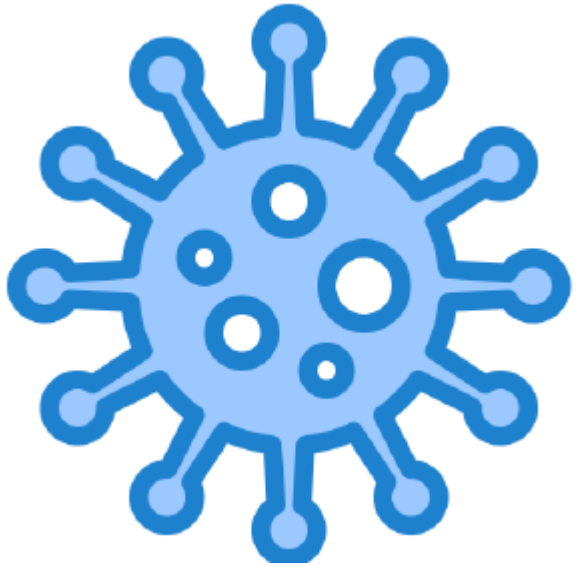
- Мошенничество на сайтах объявлений

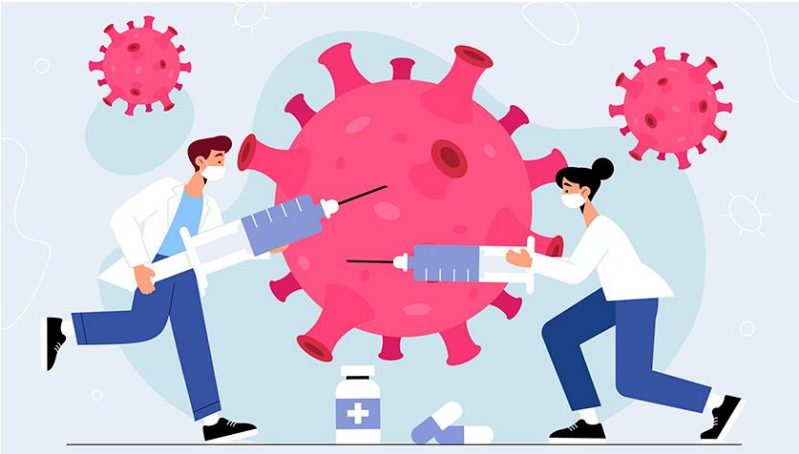
- Подозрительные сообщения
  - СМС
  - Мессенджеры
  - Социальные сети

- Фишинговые письма
- Письма от имени государственных органов

# Актуальные темы мошенничества

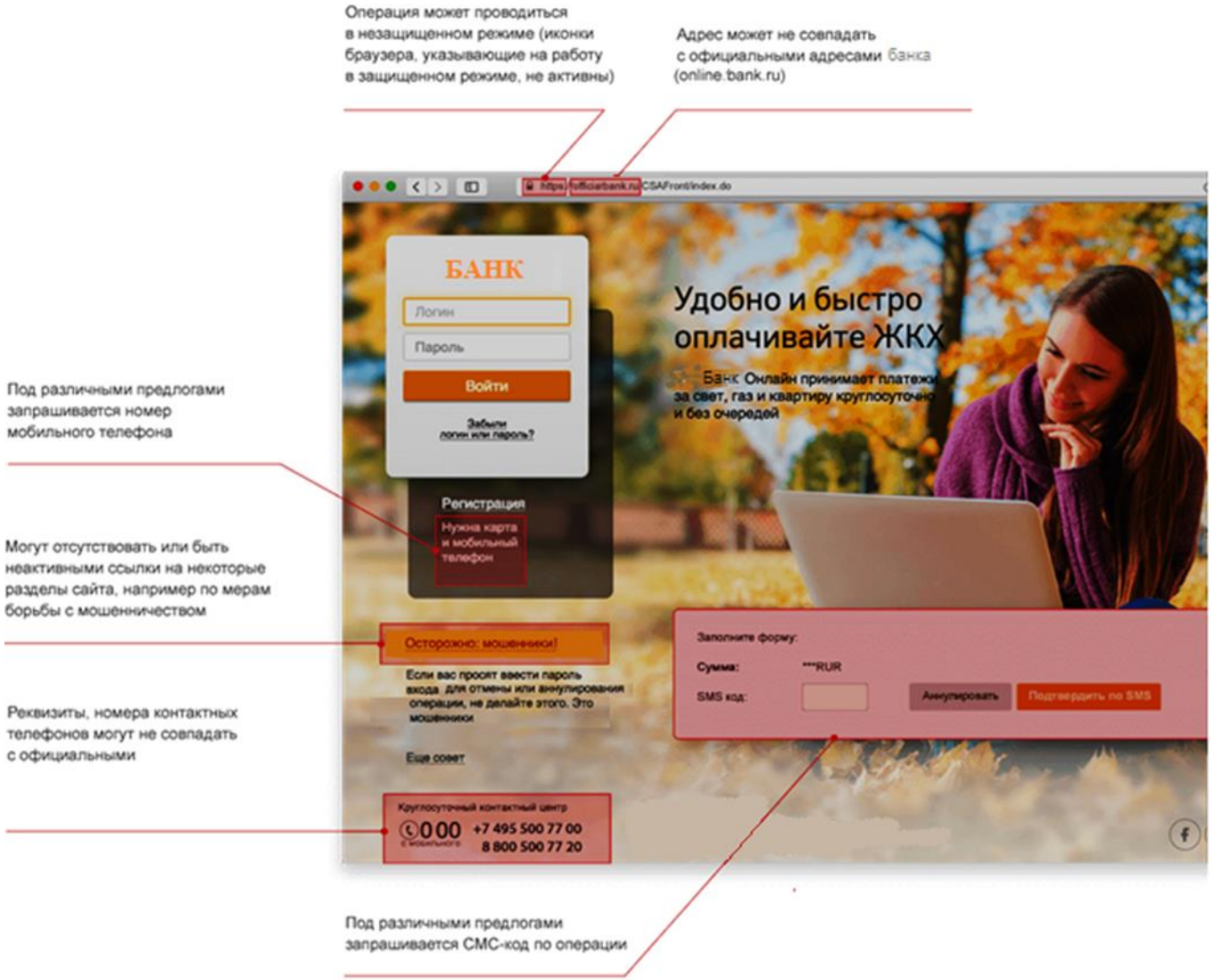
- ✓ Оформление кредитов при помощи взлома аккаунта госуслуг;
- ✓ Фишинговые сайты по теме выплат на детей в 2020 и 2021 году
- ✓ Фейковые СМС-сообщения о том, что выписан штраф за нарушение карантина или режима самоизоляции, с требованием оплатить его по номеру телефона или карты;
- ✓ Фейковые объявления о денежных бонусах для вакцинированных от COVID-19;
- ✓ Схемы с «удаленной работой» и установкой вредоносного ПО для удаленного управления компьютером.





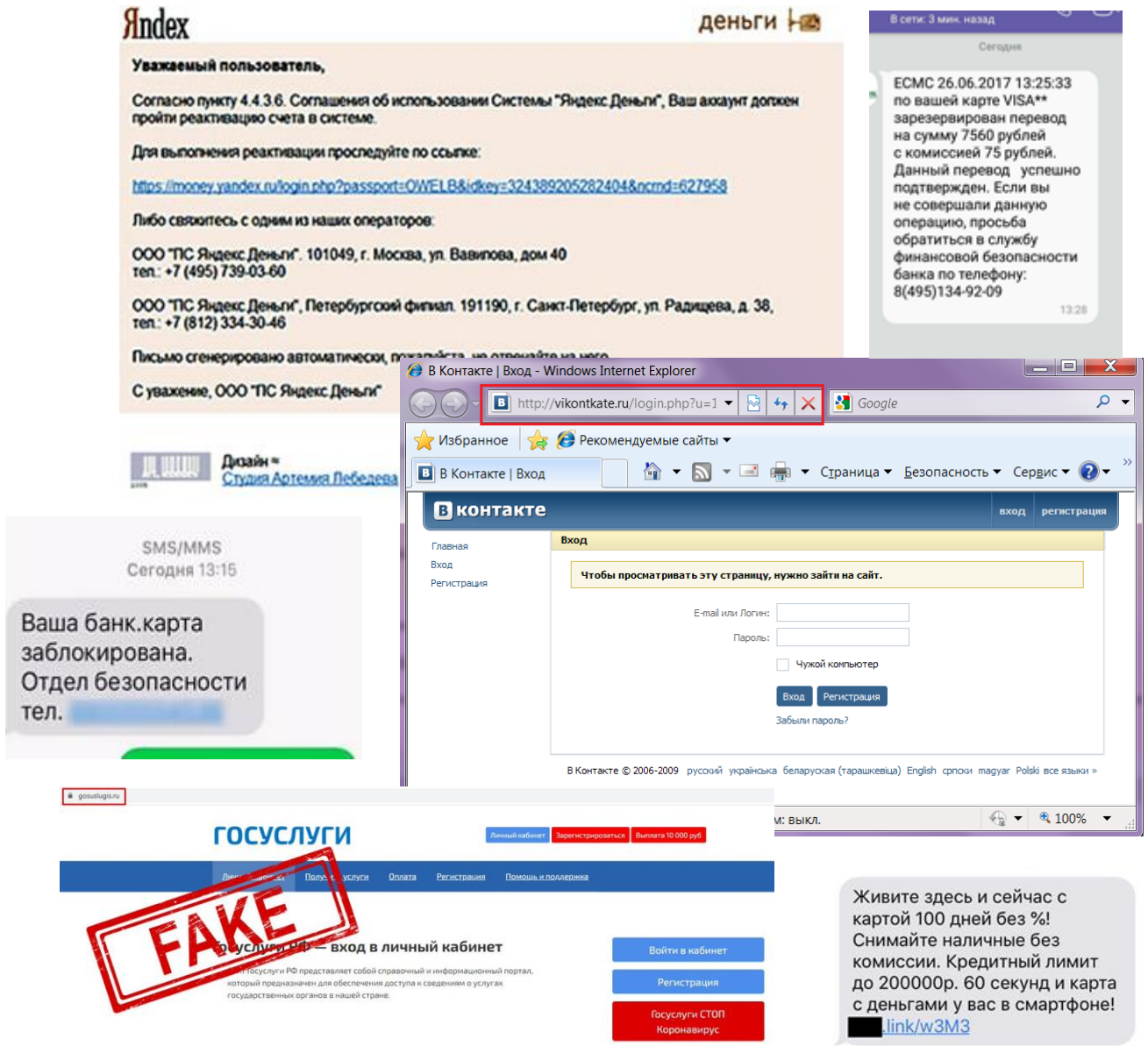
# ПРИЗНАКИ ФИШИНГОВОГО САЙТА:

- Имя сайта  отличается одним или несколькими символами от официального;
- На сайте есть опечатки, несоответствия или указаны подозрительно низкие цены;
- Ссылку на сайт прислал незнакомый адресат;
- Не используется защищенное соединение ( https//: );
- Не используется система безопасных платежей;
- Вы попали на сайт при использовании открытой сети Wi-Fi без пароля.



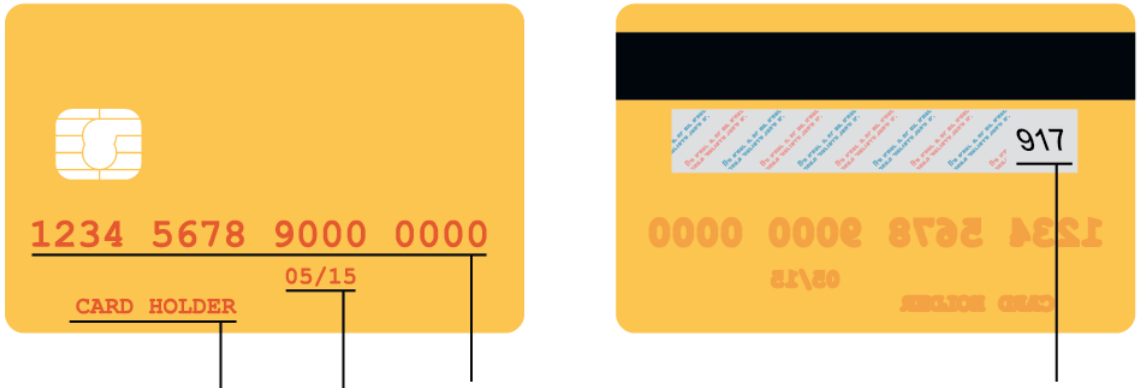
# Как защититься от фишинга?

- ✓ Использовать только личные устройства;
- ✓ Использовать антивирус с актуальными базами;
- ✓ Использовать безопасные сайты и официальные интернет магазины. Всегда проверять адрес сайта, на котором вы вводите личные данные;
- ✓ Использовать систему безопасных платежей;
- ✓ Оформить отдельную карту для совершения покупок в интернете;
- ✓ Никому не сообщать персональную информацию;
- ✓ Подключить SMS – оповещения об операциях по карте;
- ✓ Стараться сообщать о фишинговом сайте (браузеру, регистратору домена, сайту, под который маскируется фишинговая страница)
- ✓ Не доверять определителю номера. Подмена номера телефона звонящего или отправителя SMS – элементарная техническая задача!



# МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам **нужны:**




Номер карты

Срок действия

Имя владельца

Номер CVC или CVV

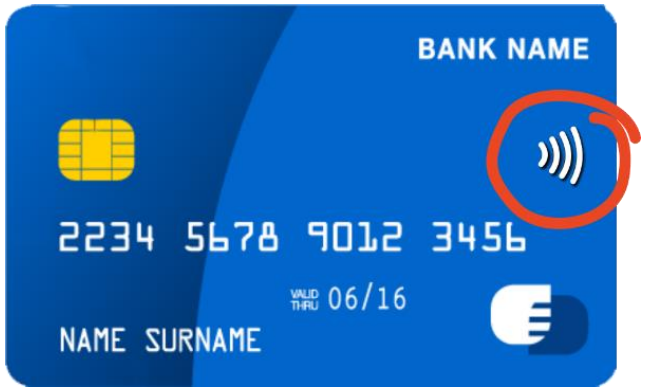
Код из СМС

ПИН-код

# БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ

## ВОЗМОЖНОСТИ

- высокая скорость выполнения платежей
- удобство для операций - до 1000 рублей без ПИН-кода




## РИСКИ

- карту могут украсть и оплачивать недорогие покупки/услуги без ПИН-кода
- возможны мошенничества с платежными терминалами *(считывающие устройства на расстоянии)*

**РЕКОМЕНДАЦИИ:**

- установить суточный лимит и смс-уведомления
- завести отдельную карту для оплаты покупок, на которой будет небольшая сумма

# КАК ИЗБЕЖАТЬ ПРОБЛЕМУ?

- Используйте банковскую карту только в тех местах, которые заслуживают доверия и охраняются
- Осмотрите банкомат. На нем не должно быть  посторонних предметов
- Набирая ПИН-код, прикрывайте клавиатуру рукой
- Подключите мобильный банк и СМС-уведомления
- Никому не сообщайте секретный код из СМС
- Не теряйте карту из виду

# Вредоносное программное обеспечение (ВПО)

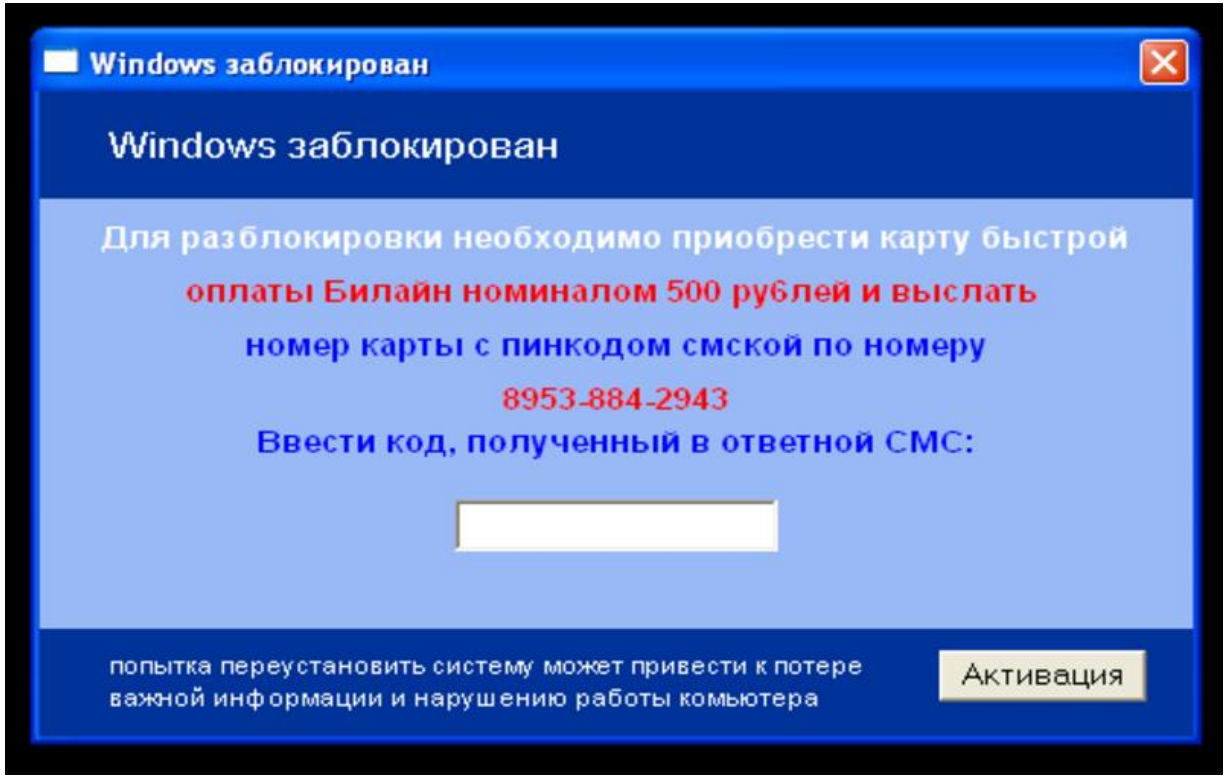
Это любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого компьютера или информации, хранимой на нем, с целью несанкционированного использования его ресурсов или причинение вреда владельцу информации, и/или владельцу компьютера.

## Наиболее распространённые типы вирусного ПО

| | |
|---|---|
| • Вирусы | • Программы-вымогатели/ шифровальщики |
| • Черви | • Боты |
| • Рекламное ПО | • Руткиты |
| • Шпионское ПО | • Троянские программы |

# Признаки заражения ВПО

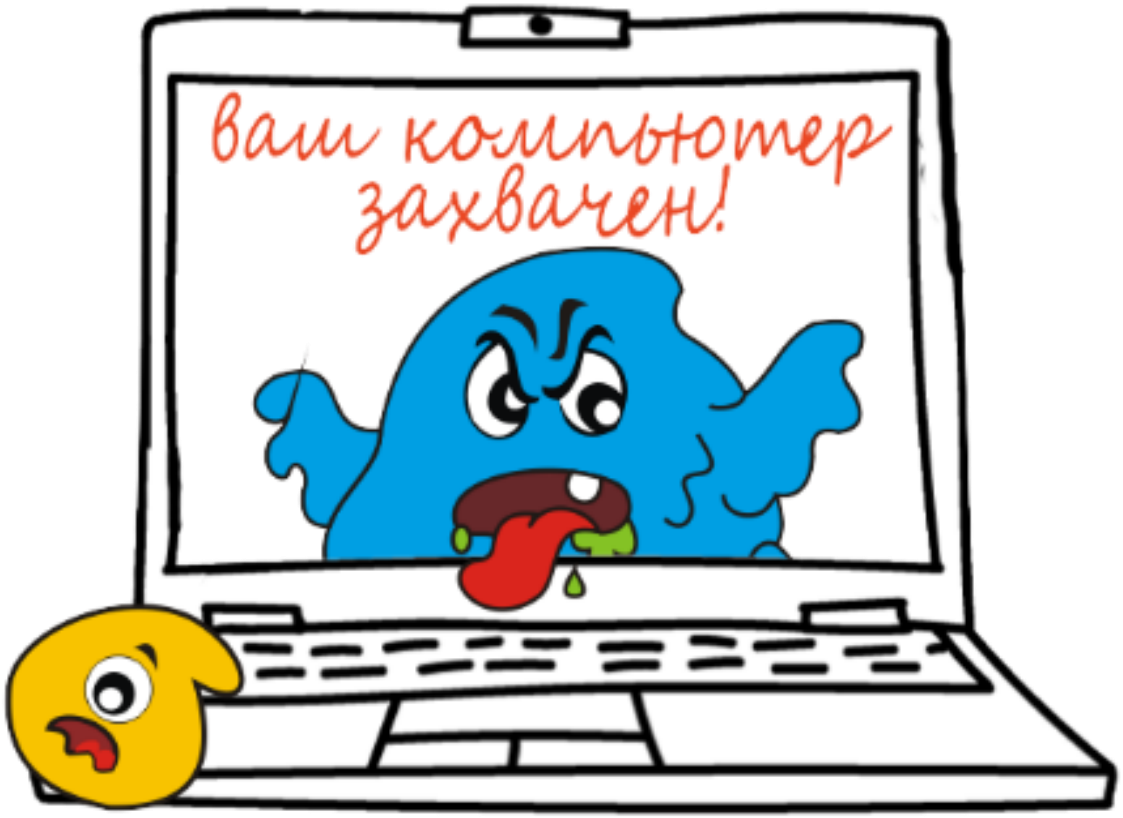
1. На экране появляются неожиданные сообщения или изображения.
2. Происходит самостоятельный запуск программ.
3. Вы видите, что некое приложение пытается соединиться с интернетом, хотя вы эту программу не запускали.
4. Ваши друзья получают от вас по электронной почте сообщения, которых вы не отправляли.
5. Ваш компьютер часто зависает или программы стали выполняться медленно.
6. Вы получаете множество системных сообщений об ошибке.
7. При включении компьютера операционная система не загружается.
8. Вы обнаружили пропажу или изменение файлов или папок.
9. Ваш браузер ведет себя неадекватно — например, вы не можете закрыть вкладку.
10. Вы слышите неожиданные звуки, воспроизводимые в случайном порядке.



# Способы защиты от заражения ВПО

Чтобы защитить свой компьютер от ВПО, необходимо **обязательно использовать антивирусную защиту**, и помнить что нельзя:

1. **Переходить** по подозрительным ссылкам в электронной почте или в браузере.
2. **Открывать** подозрительные вложения электронных писем.
3. **Скачивать** и **устанавливать «пиратское» программное обеспечение** или бесплатное программное обеспечение, полученное из непроверенных источников.
4. **Использовать** флеш накопитель, внешние жесткие диски SD/MMC-карты, телефоны и другие устройства, на которых могут быть вирусные программы, предварительно не проверив их антивирусными программами.



# Полезные материалы

Аналитические материалы по информационной безопасности Банка России

**cbr.ru/analytics/ib/fincert/**

Реальные примеры мошеннических схем

**fincult.info**

Банк России

# СПАСИБО ЗА ВНИМАНИЕ !

2021 г.