

# РОСКОМНАДЗОР



Управление Федеральной службы по надзору  
в сфере связи, информационных технологий  
и массовых коммуникаций по Вологодской области

# **Основы кибербезопасности и защита личных данных**

Казакова Ирина Андреевна,  
специалист – эксперт отдела по защите  
прав субъектов персональных данных и  
правовой работы

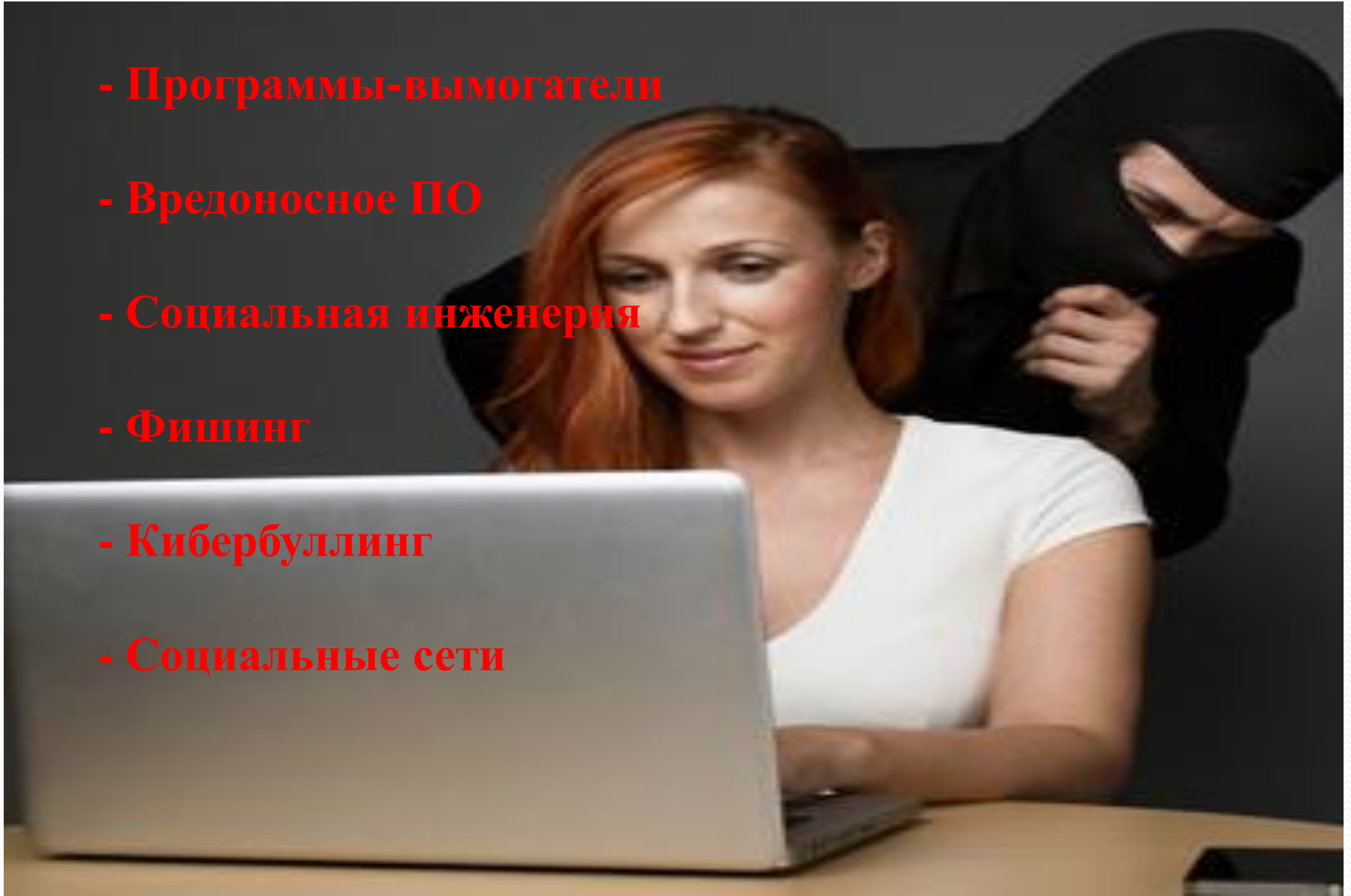
# Кибербезопасность -

**это реализация мер по защите систем, сетей и программных приложений от цифровых атак**



# КИБЕРУГРОЗЫ В СЕТИ ИНТЕРНЕТ

- Программы-вымогатели
- Вредоносное ПО
- Социальная инженерия
- Фишинг
- Кибербуллинг
- Социальные сети



# ИСТОЧНИКИ КИБЕРУГРОЗ

**ПРАКТИКА ПРИНЯТИЯ** условий пользовательского соглашения по умолчанию

**ХИЩЕНИЕ ПД**

**ИСПОЛЬЗОВАНИЕ** «серых» мобильных приложений

**ФИШИНГ**

**ПОВСЕМЕСТНОЕ ИСПОЛЬЗОВАНИЕ** видеонаблюдения

**ПЕРЕДАЧА ПД** по незащищенным каналам связи

**ИСПОЛЬЗОВАНИЕ** геолокационных сервисов

**РАСПРОСТРАНЕНИЕ ПД** в открытых источниках

**ОБЩЕНИЕ** с виртуальными друзьями



# Объекты и виды киберугроз

Объекты угроз	Виды угроз
<b>Граждане</b>	Утечка и обнародование частной информации, мошенничество, распространение опасного контента, воздействие на личность путем сбора персональных данных и атаки на инфраструктуру, используемую гражданами в обычной жизни.
<b>Бизнес</b>	Воздействие на системы интернет-банкинга, блокирование систем покупки билетов, онлайн-торговли, геоинформационных систем и хакерские атаки на частные сайты.
<b>Государство</b>	Атаки на ключевые государственные системы управления (электронное правительство, сайты госорганов), экономическая блокада (масштабное отключение платежных систем, систем бронирования), аппаратная атака на персональные компьютеры, смартфоны граждан и организаций, атаки на бытовые объекты, которые управляются с помощью информационно-коммуникационных технологий, и критически важную инфраструктуру.

# Типы угроз кибербезопасности



# Программы-вымогатели

Программа-вымогатель – это вредоносное ПО, которое блокирует компьютеры или личные файлы пользователей, требуя выкуп за восстановление доступа.





Обнаружена проблема, которая может повредить вашему компьютеру.

Драйвер устройства, вызвавший повреждения был обезврежен системой.  
Нарушенный драйвер на стеке ядра должны быть заменены рабочей версией.

Technical information:

\*\*\* STOP: 0x000000C4 (0x0000003C, 0x00000000, 0x00000000)

Microsoft Windows

**Ваша система заблокирована! Драйвер признан не лицензионным. Пожалуйста активируйте драйвер лицензионным ключём с диска Windows или отправьте смс на номер 6008 с текстом adn9 2 (учитывайте, что между adn9 и 2 стоит пробел) для получения этого ключа.**



Язык ввода: English



ВВОД

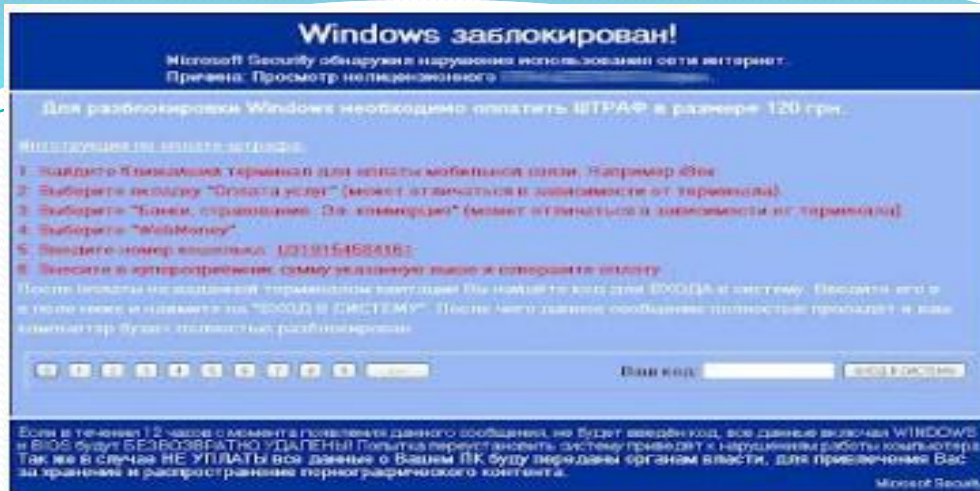
A problem has been detected and Windows has been shut down to prevent damage to your Computer.

A device driver attempting to corrupt the system has been caught.  
The faulty driver currently on the kernel stack must be replaced with a working version.

Technical information:

\*\*\* STOP: 0x000000C4 (0x0000003C, 0x00000000, 0x00000000)

\*\*\* STOP: c000007b Unknown Hard Error Unknown Hard Error Beginning dump of physical memory



## Второй способ:

**Самый простой вариант разблокировать систему (не требуется дополнительный софт, загрузочные диски), требуется немного поковыряются в реестре Windows**

зайти в раздел реестра (команда regedit) `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

значение параметра **Shell** исправить на значение `explorer.exe`

значение параметра **Userinit** исправить на значение `C:\WINDOWS\system32\userinit.exe`, (не забудьте про запятую в конце строки)

Все подобные банеры-вымогатели лечатся теми же методами:

ВАШ КОМПЬЮТЕР ЗАБЛОКИРОВАН

Для разблокировки необходимо отправить смс

**Windows заблокирован**

Для разблокировки необходимо отправить смс с текстом

**Доступ в интернет заблокирован в связи с нарушением  
лицензионного соглашения программы uFast Download Manager**

**Вам необходимо активировать вашу копию**

**04:27**

**чтобы получить регистрационный код отправьте смс  
с кодом fw0004199 на номер 7122**

**в ответ вы получите сообщение с кодом активации**

**Ваш код из ответной смс**

\*\*\*\*\*



Recycle Bin

# Заражение программой-вымогателем *Вредоносный спам*

КОМПЬЮТЕР ЗАБЛОКИРОВАН!

Удаление вирусов,  
троянов-вымогателей,  
разблокировка рабочего стола.

Звоните (963)136-57-40

Выезд на дом.

Разблокировать

[www.compserviceufa.ru](http://www.compserviceufa.ru)

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера лицом, достигшим восемнадцатилетнего возраста, - наказываются лишением свободы на срок от двух до восьми лет с ограничением свободы на срок до одного года либо без такового.

# Вредоносная реклама



Добро пожаловать  
в наше онлайн-казино!

**ДЖЕКПОТ**

**\$32784**

**Сорвать**



Играть



Играть



Играть



Играть



Играть

# Типы программ-вымогателей

- Псевдоантивирусы
- Вирусы, блокирующие экран
- Программы-вымогатели, шифрующие файлы



# Псевдоантивирусы



Для того что бы уничтожить найденные вирусы необходимо выполнить 3 простых шага:

1. Выбрать вашу страну:
2. Отослать смс с текстом: **69034 1493329**  
на номер **9690**  
(Стоимость доступа 10рублей \*)
3. Ввести полученный в ответном смс код:

Продолжить



# Вирусы, блокирующие экран

Windows заблокирован

Для разблокировки необходимо отправить смс с текстом

t7580620000 на номер 3649

введите полученный код

Активация

для разблокировки у вас есть

02:59:41


\*попытка переустановить систему может привести к потере важной информации и нарушениям работы компьютера.



# Программы-вымогатели, шифрующие файлы

360 ransomware decryption tools

Способ дешифрования к программе-вымогателю Refua [Посмотрите](#)

 Расшифровывать и восстанавливать файлы, зашифрованные и скрытые вредоносными ПО [Назад](#)

Сканирование завершено: 6 файлы дешифрованы

Путь файлов G:\DATA\shifr\encode\_files\360tot... Зашифрованные файлы 6 Файлы дешифрованы 6 Время 00:00:38

Путь файлов	Статус
G:\DATA\shifr\encode_files\360total_test\GandCrab 5.2\20001228_...	Расшифровано успешно
G:\DATA\shifr\encode_files\360total_test\GandCrab 5.2\20001228_...	Расшифровано успешно
G:\DATA\shifr\encode_files\360total_test\GandCrab 5.2\20001228_...	Расшифровано успешно
G:\DATA\shifr\encode_files\360total_test\GandCrab 5.2\20001228_...	Расшифровано успешно
G:\DATA\shifr\encode_files\360total_test\GandCrab 5.2\20001228_...	Расшифровано успешно
G:\DATA\shifr\encode_files\360total_test\GandCrab 5.2\20001228_...	Расшифровано успешно

Сохранить файлы в G:\360DecodeFiles [Настройка](#) Если еще зашифрованные файлы, свяжитесь с нами [Свяжитесь с нами](#)

# Вредоносное программное обеспечение

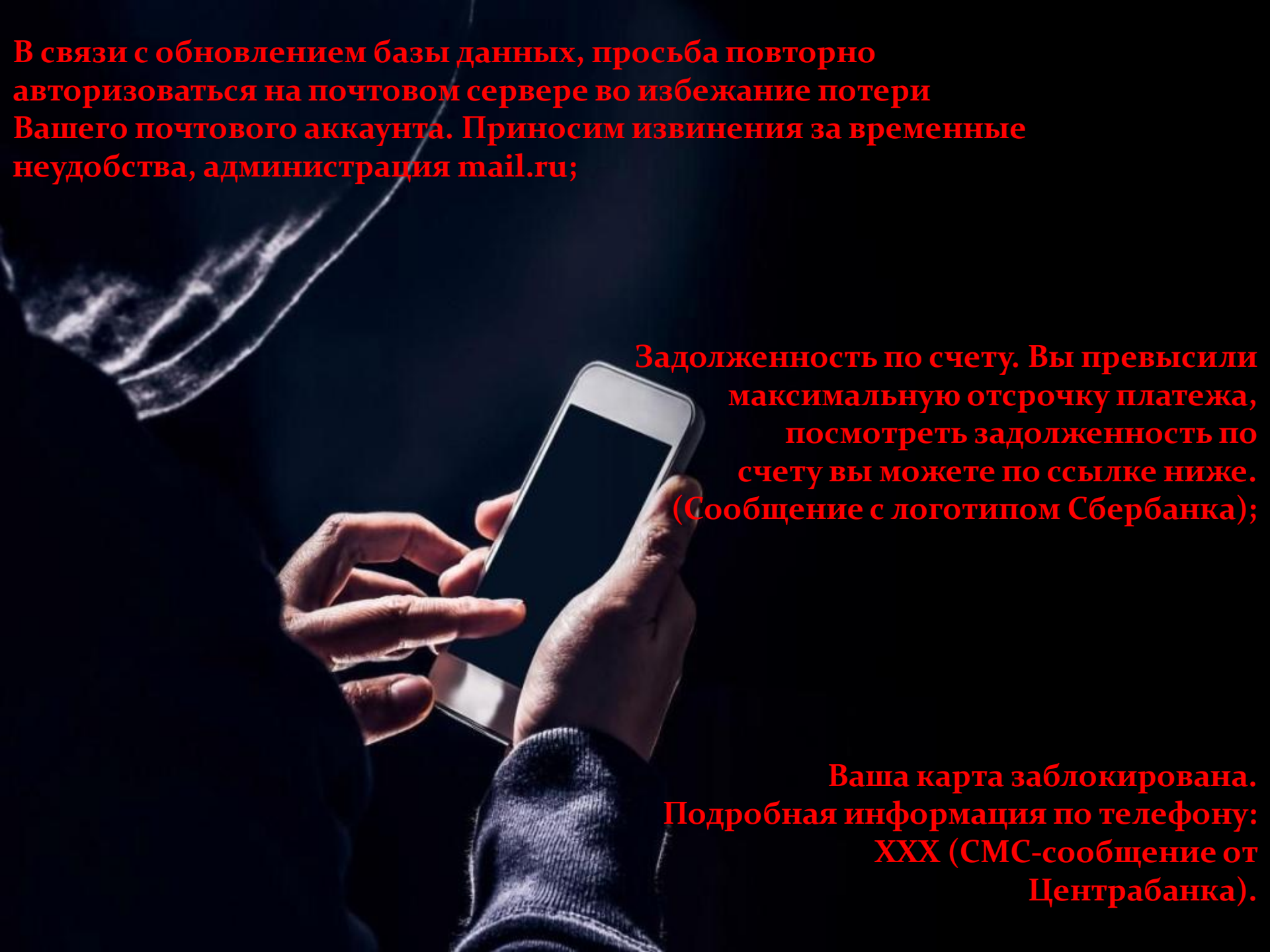
Вредоносное программное обеспечение предназначено для получения несанкционированного доступа или повреждения компьютерной системы.



# Социальная инженерия

– это тактика, которую используют злоумышленники, чтобы склонить пользователя к раскрытию конфиденциальной информации.



A close-up photograph of a person's hands holding a white smartphone. The person is wearing a dark, textured sweater. The background is dark and out of focus. The text is overlaid on the image in a bright red color.

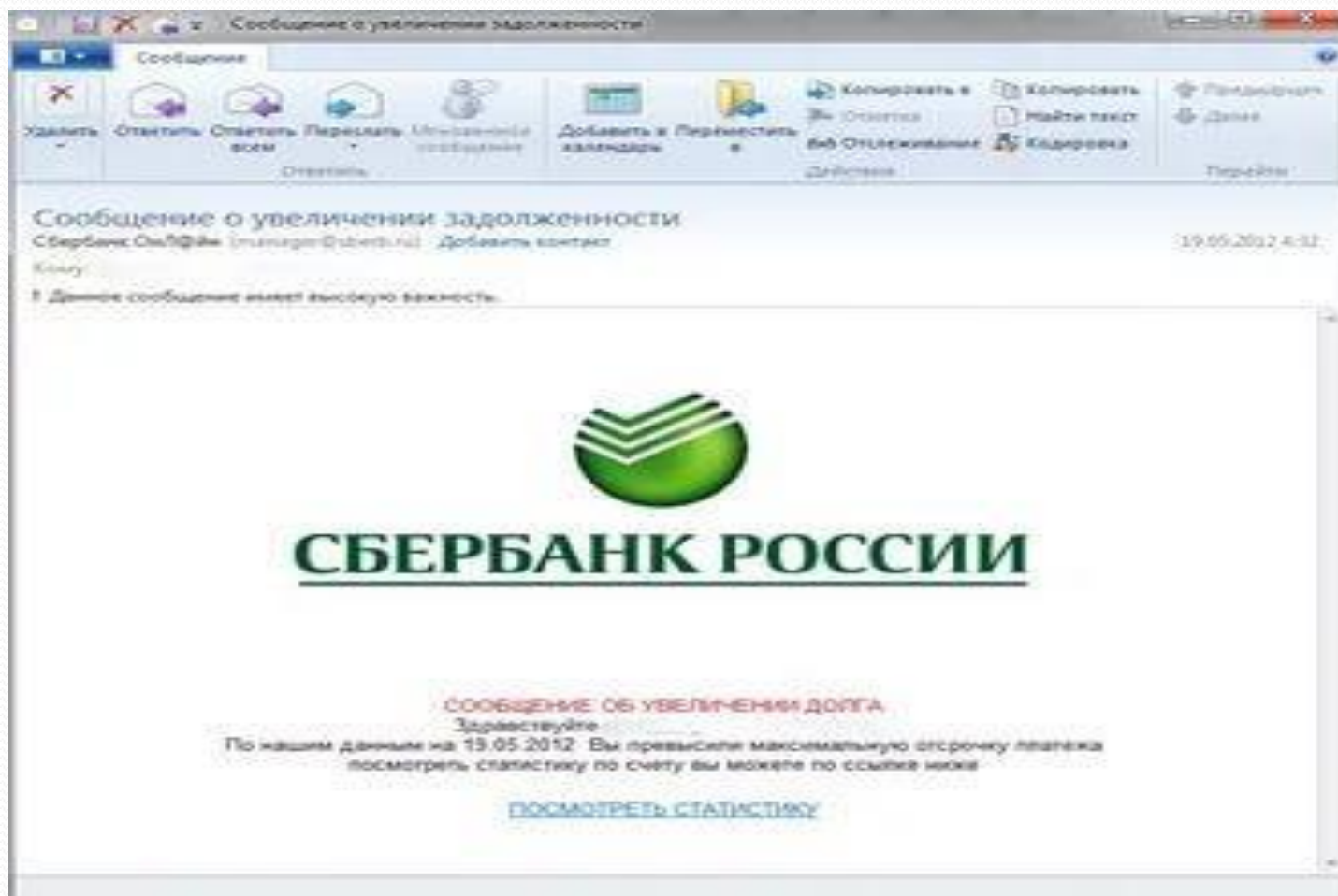
**В связи с обновлением базы данных, просьба повторно авторизоваться на почтовом сервере во избежание потери Вашего почтового аккаунта. Приносим извинения за временные неудобства, администрация mail.ru;**

**Задолженность по счету. Вы превысили максимальную отсрочку платежа, посмотреть задолженность по счету вы можете по ссылке ниже. (Сообщение с логотипом Сбербанка);**

**Ваша карта заблокирована. Подробная информация по телефону: XXX (СМС-сообщение от Центробанка).**

# Фишинг

- это рассылка поддельной электронной корреспонденции, которая выглядит как сообщения от надежных источников.



# Примеры фишинга

vk.com/im?real=86104013

Назад **В контакте** К списку диалогов люди сообщества игры музыка помощь выйти

Моя Страница рел.  
Мои Друзья  
Мои Фотографии  
Мои Видеозаписи  
Мои Аудиозаписи  
Мои Ссылки  
Мои Группы  
Мои Новости  
Мои Закладки  
Мои Настройки

Приложения  
Документы

Диалоги **Просмотр диалогов** Действия | К списку друзей

**Татьяна** ✕

**М**не захотелось есть, когда я вышел с кат...  
забежал в буфет, съел бутерброд с сыром  
и молока, а потом зашел в телефонную будку.  
думал — может быть, все-таки заказать Дюф...  
два урны, прислали она домой как ит. Велу...  
моя жена была счастлива, а я получил...

**Татьяна** 17.09.13  
АХАХА:D блин  
я даже сейчас ем

**Наташа** 17.09.13  
и я:) яблочкин^\_\*

**Татьяна** 17.09.13  
<http://tanyalis09.tolk.ru/>

Со взломанной страницы пришла ссылка, которая может вести на фишинговый сайт!

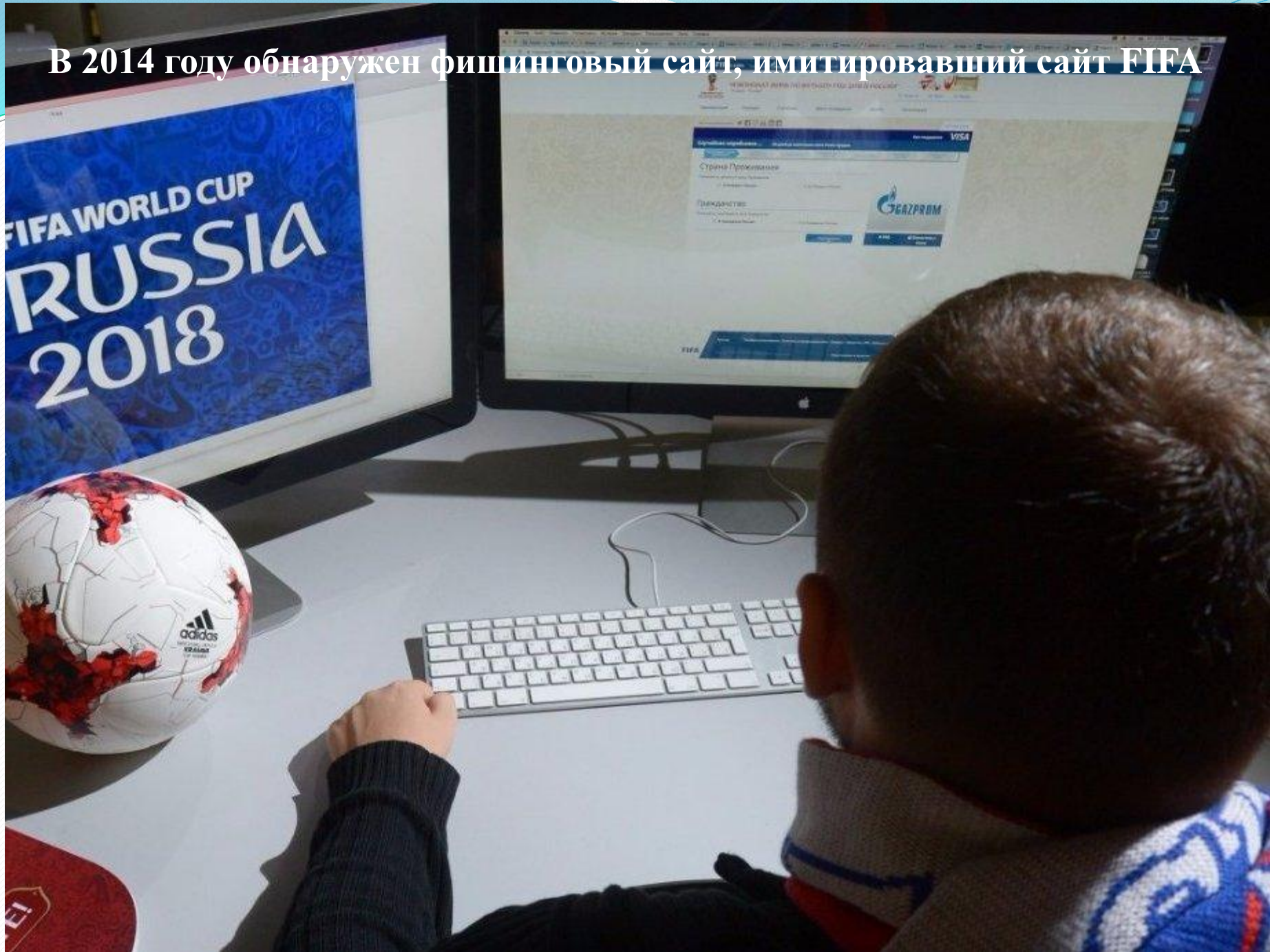
Введите Ваше сообщение...

Отправить Прикрепить online

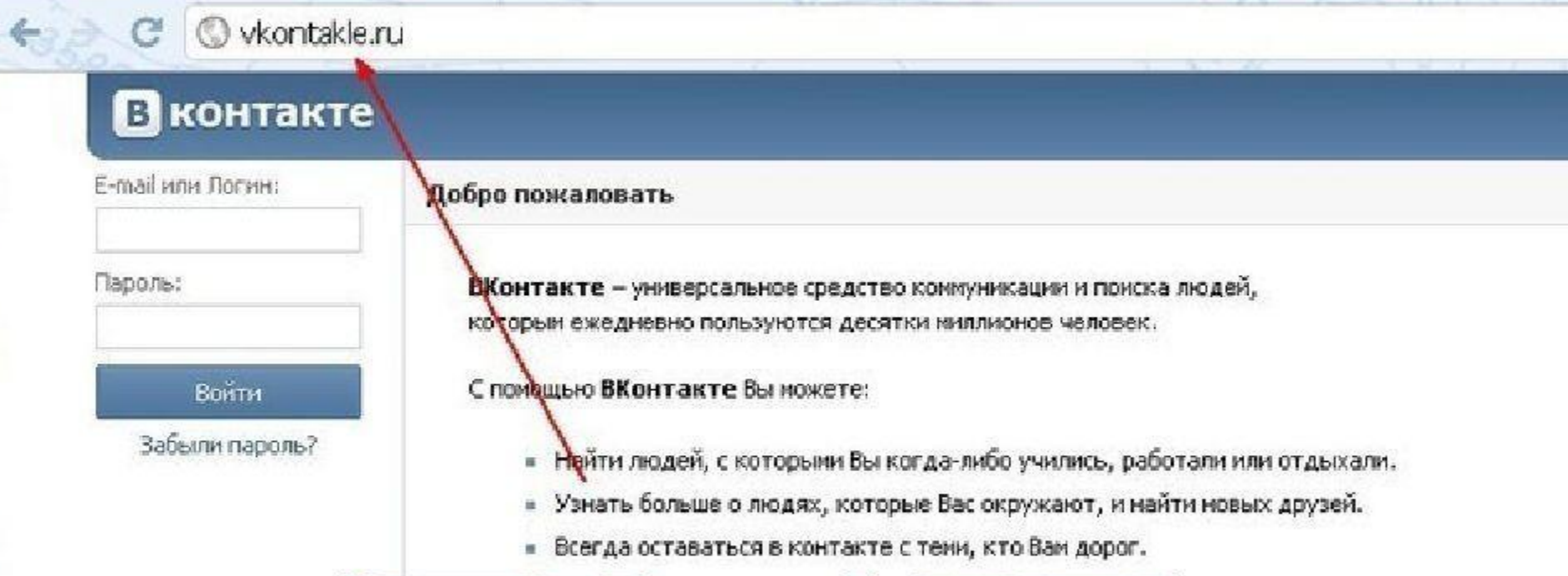
15:39 22.10.2013 RU

К содержанию

В 2014 году обнаружен фишинговый сайт, имитировавший сайт FIFA



# Фишинг





# Основные советы по борьбе с фишингом:

- Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
- Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
- Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установи надежный пароль (PIN) на мобильный телефон;
- Отключи сохранение пароля в браузере;
- Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

# Кибербулинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.



# КИБЕРБУЛЛИНГ



## ПОСЛЕДСТВИЯ:

58%	детей сталкивались с кибербуллингом
17%	детей готовы обратиться к РОДИТЕЛЯМ в случае травли
3%	детей готовы обратиться к УЧИТЕЛЯМ в случае травли*



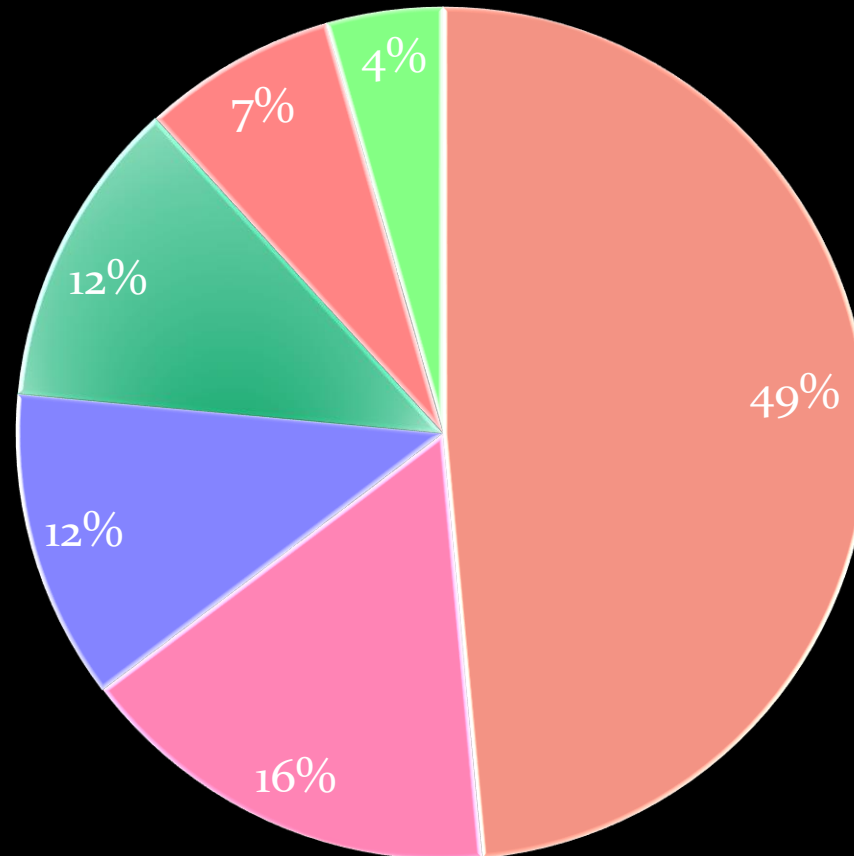
# Кибербуллинг: где встречается?

- мобильная связь (смс-сообщения);
- мобильные приложения и мессенджеры (What's App, Viber, Instagram, Badoo и т.д.);
- чаты и форумы в сети «Интернет»;
- электронная почта (рассылка сообщений);
- социальные сети (ВКонтакте, Facebook и т.д.);
- сервисы видеохостинга;
- игровые сайты и виртуальные игровые миры.



# Наиболее часто кибербуллинг встречается на площадках

- Социальные сети
- Онлайн-игры
- Онлайн-форумы
- Раздел комментариев на сайтах
- Персональная e-mail рассылка
- Сайты знакомств



# Основные советы по борьбе с кибербуллингом:

- Не бросайся в бой.
- Управляй своей киберрепутацией.
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
- Не стоит вести хулиганский образ виртуальной жизни.
- Веди себя вежливо.
- Игнорируй единичный негатив.
- Бан агрессора.



# Последствия киберугроз

Присвоение личного имущества граждан обманным путем

Вред психическому, нравственному и духовному здоровью граждан

Нарушение права на личную жизнь



Принуждение к выполнению воли третьих лиц

Монетизация пользователя сети Интернет, т.е. пользователь становится товаром

Манипулирование субъектом персональных данных

# 10 способов защиты личных данных

Как не стать жертвой интернет-мошенников



Не указывайте лишнюю личную информацию в профиле в социальных сетях, используйте сокрытие данных от всех, кроме друзей



Своевременно обновляйте программное обеспечение



Установите на свой (свои) ПК защитное ПО (антивирус и фаервол) и следите за регулярностью обновлений антивирусных баз



Тщательно выбирайте онлайн-магазин, прежде чем сообщать данные банковской карты, пользуйтесь услугой SMS-информирования от банка



Обращайте внимание на характер данных при регистрации в онлайн-сервисах.

Не указывайте данные, которые в действительности не нужны для получения услуг от сервиса (номера удостоверений личности и т.п.), а в случае необходимости ищите менее требовательные к персональным данным сервисы-аналоги



Не запускайте подозрительные вложения, присланные по электронной почте и через интернет-мессенджеры



Установите пароль доступа к смартфону и специализированные приложения для поиска аппарата и удаленного стирания данных. Внимательнее относитесь к установке малоизвестных приложений. Отключайте неиспользуемые беспроводные интерфейсы



Установите свой собственный пароль домашней сети Wi-Fi



Проверяйте интернет-адреса при переходе из почты и с сайтов



Не используйте один пароль для всех интернет-ресурсов

## КОМПАС

Дисконт цифровой техники





**РОСКОМНАДЗОР**

# Береги свои ПЕРСОНАЛЬНЫЕ ДАнные!

