РОСКОМНАДЗОР

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

Основы кибербезопасности и защита личных данных

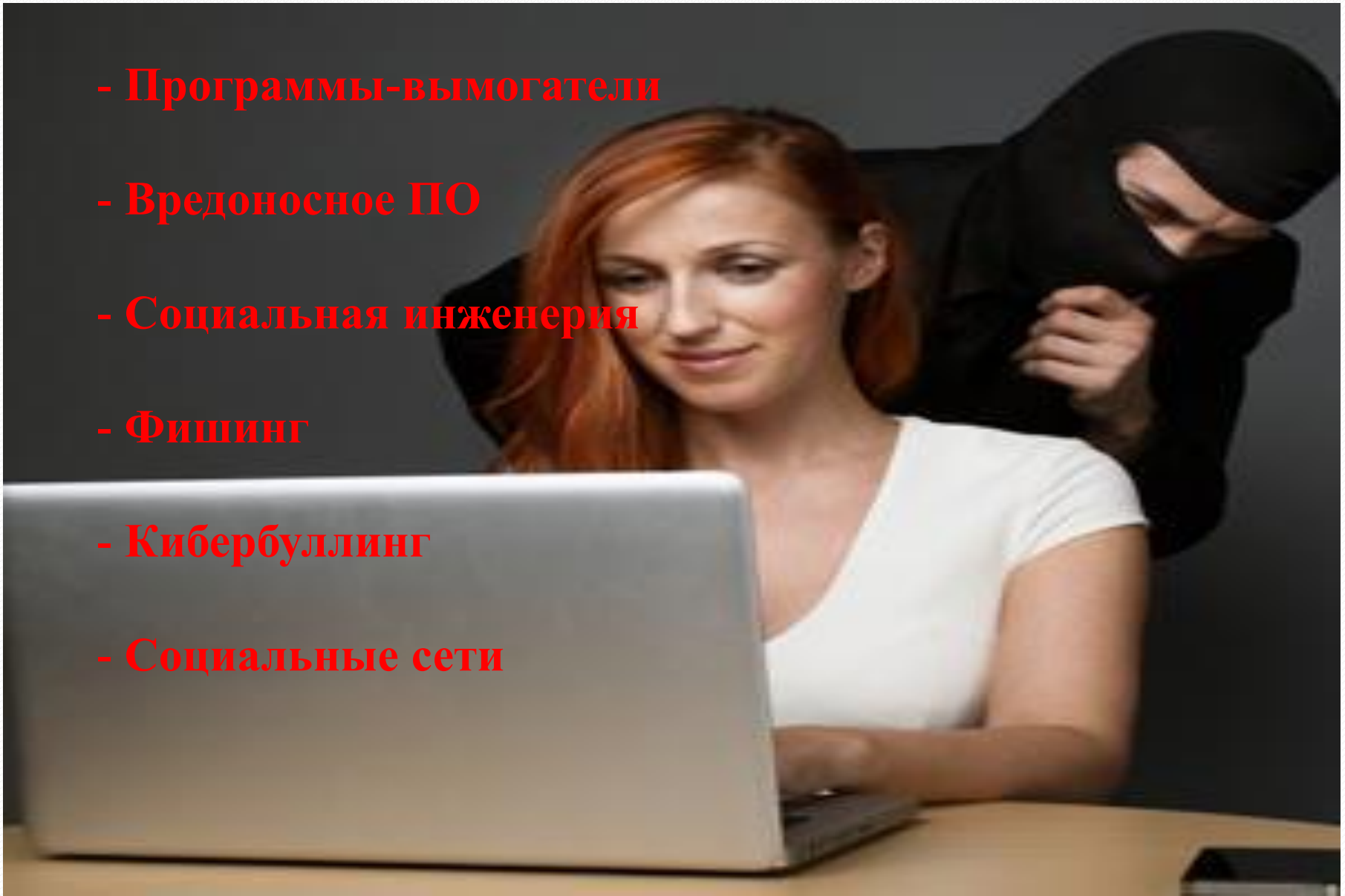
Казакова Ирина Андреевна,

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



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
Граждане	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.
Бизнес	Воздействие на системы интернет-банкинга, блокирование систем покупки билетов, онлайн-торговли, геоинформационных систем и хакерские атаки на частные сайты.
Государство	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.

бнаружена 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 полуения этого ключа.

Язык ввода: English

ВВОД

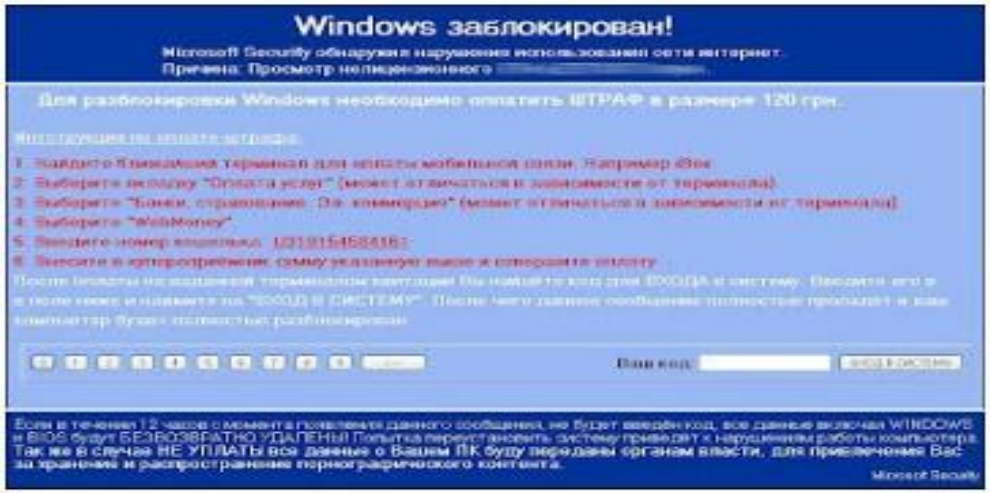
A problem has been detected and Windows has been shut down to prevent damage to your Computer.

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 поковырятся в реестре Windows

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

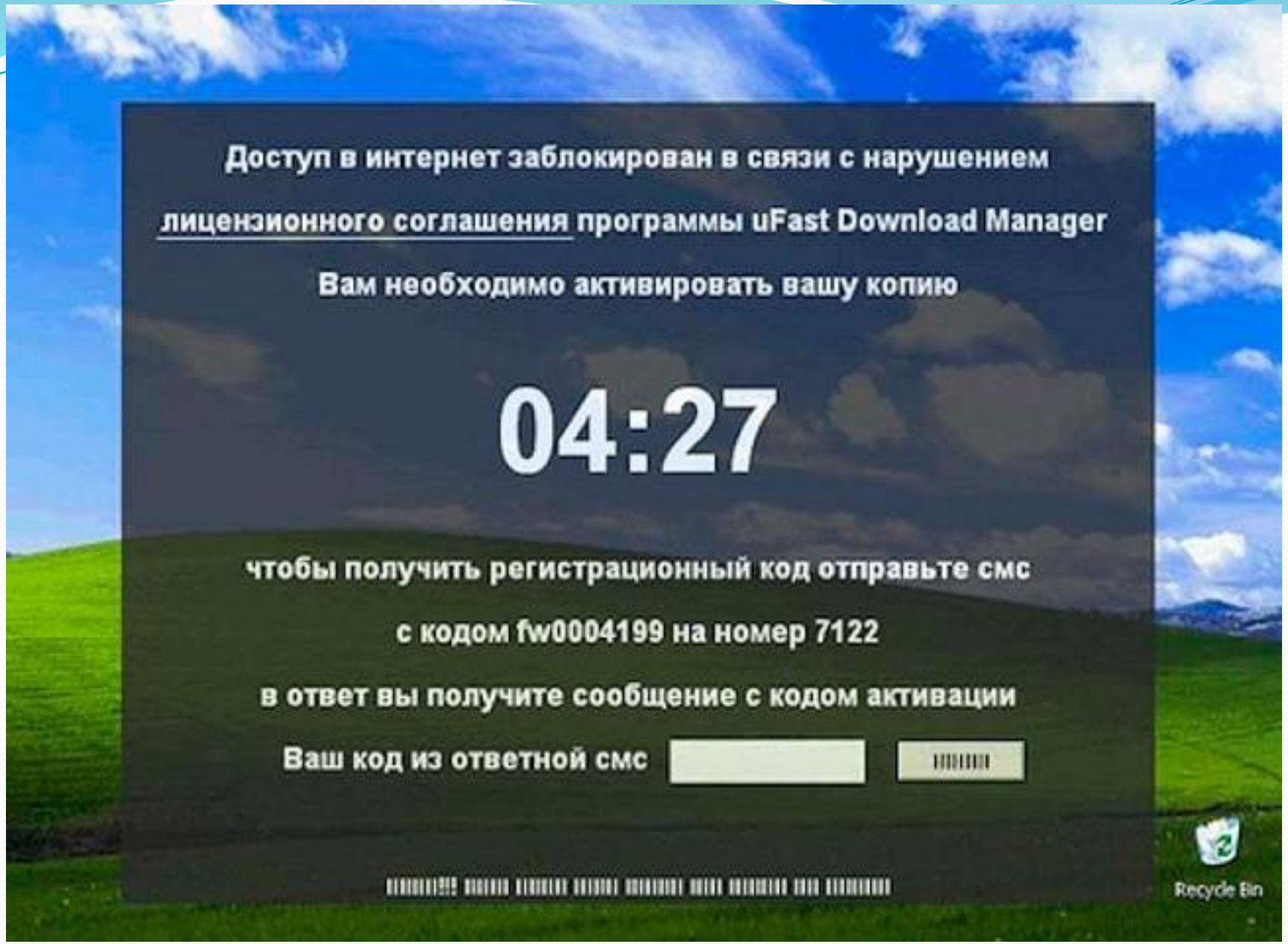
значение параметра Shell исправить на значение explorer.exe

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

Все подобные банеры-вымогатели лечаться теми же методами.

ВАШ КОМПЬЮТЕР ЗАБЛОКИРОВАН

Для разблокировки необходимо отправить смс


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

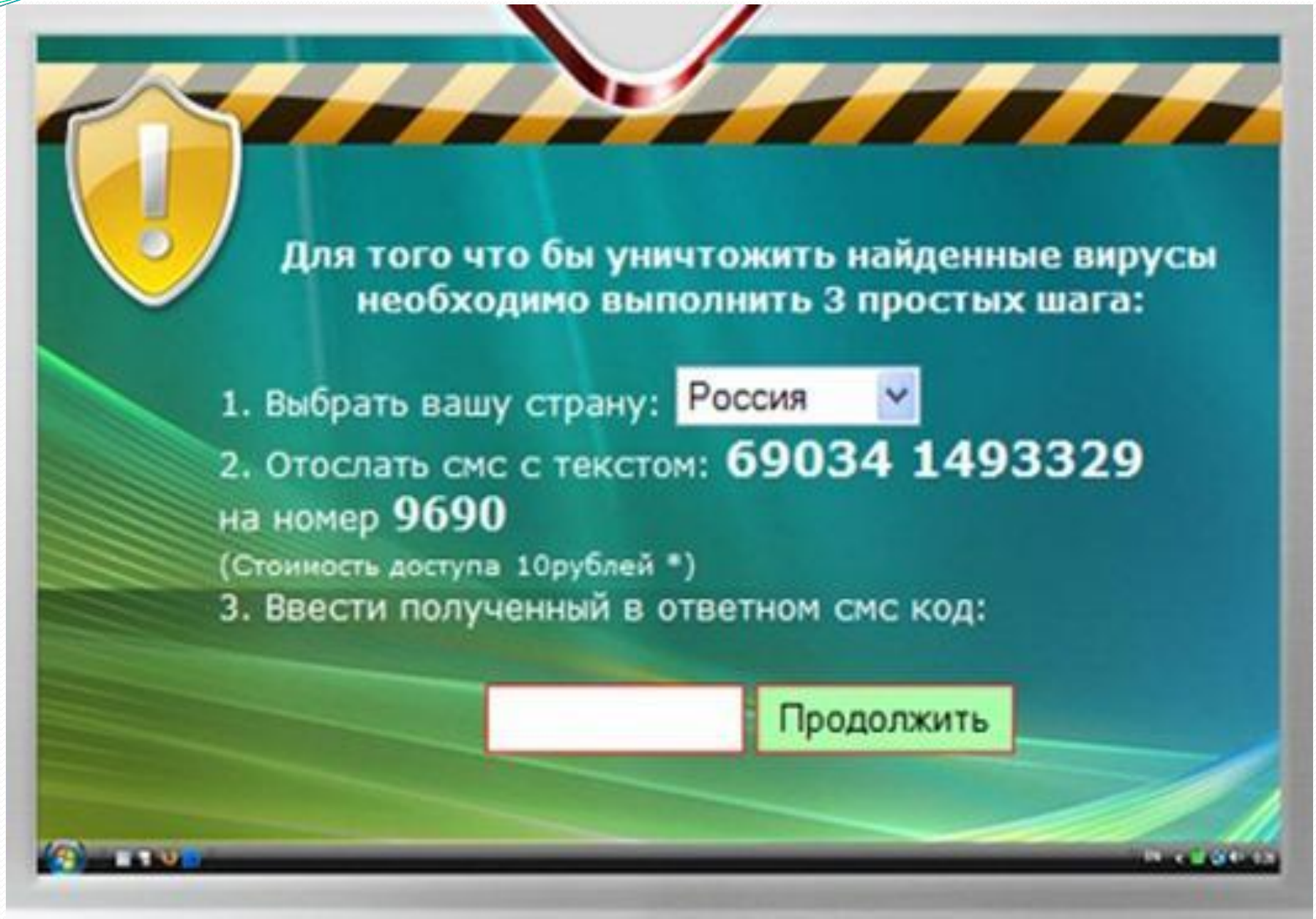
Вредоносный спам

Вредоносная реклама

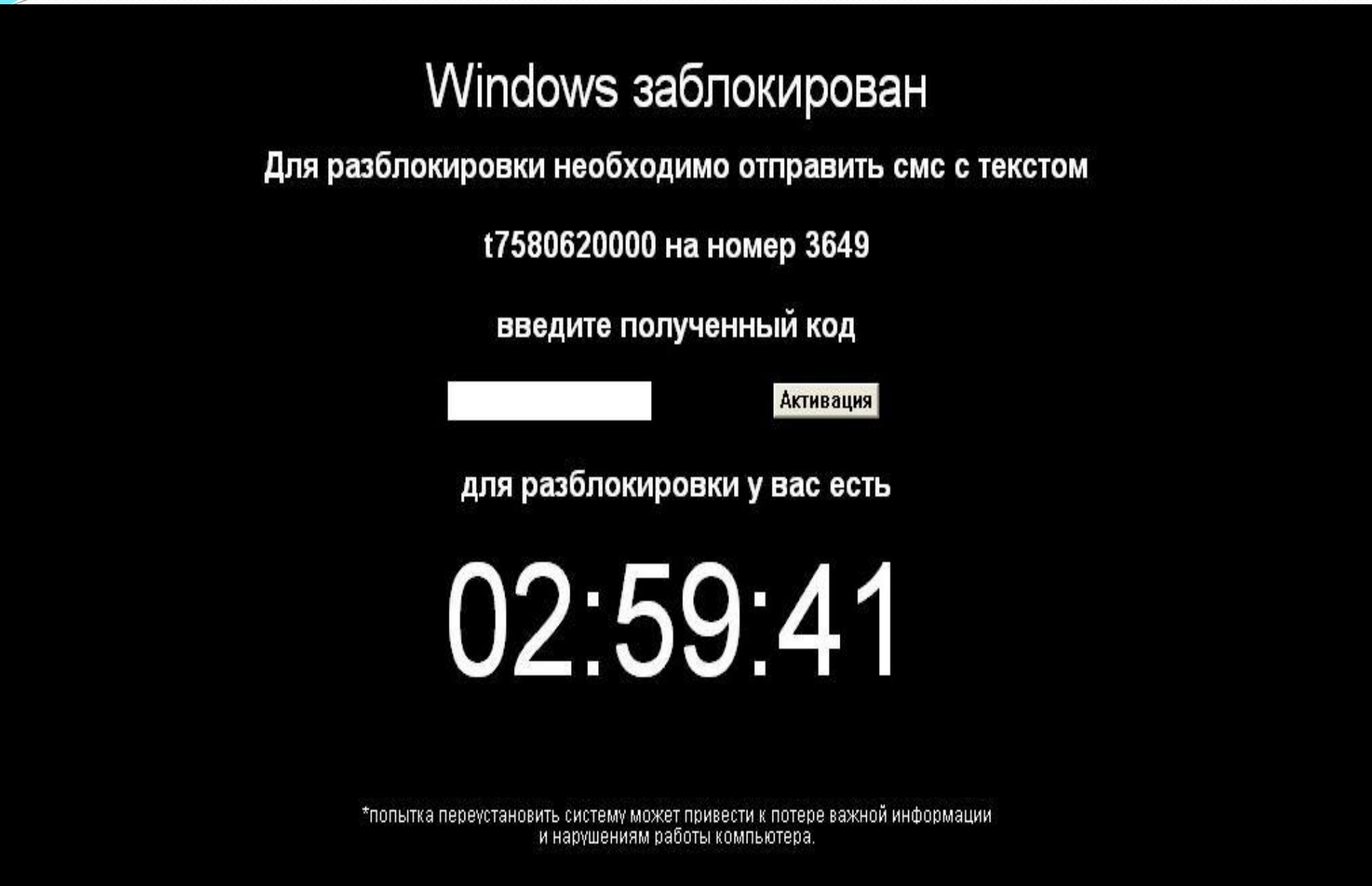
Типы программ-вымогателей

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

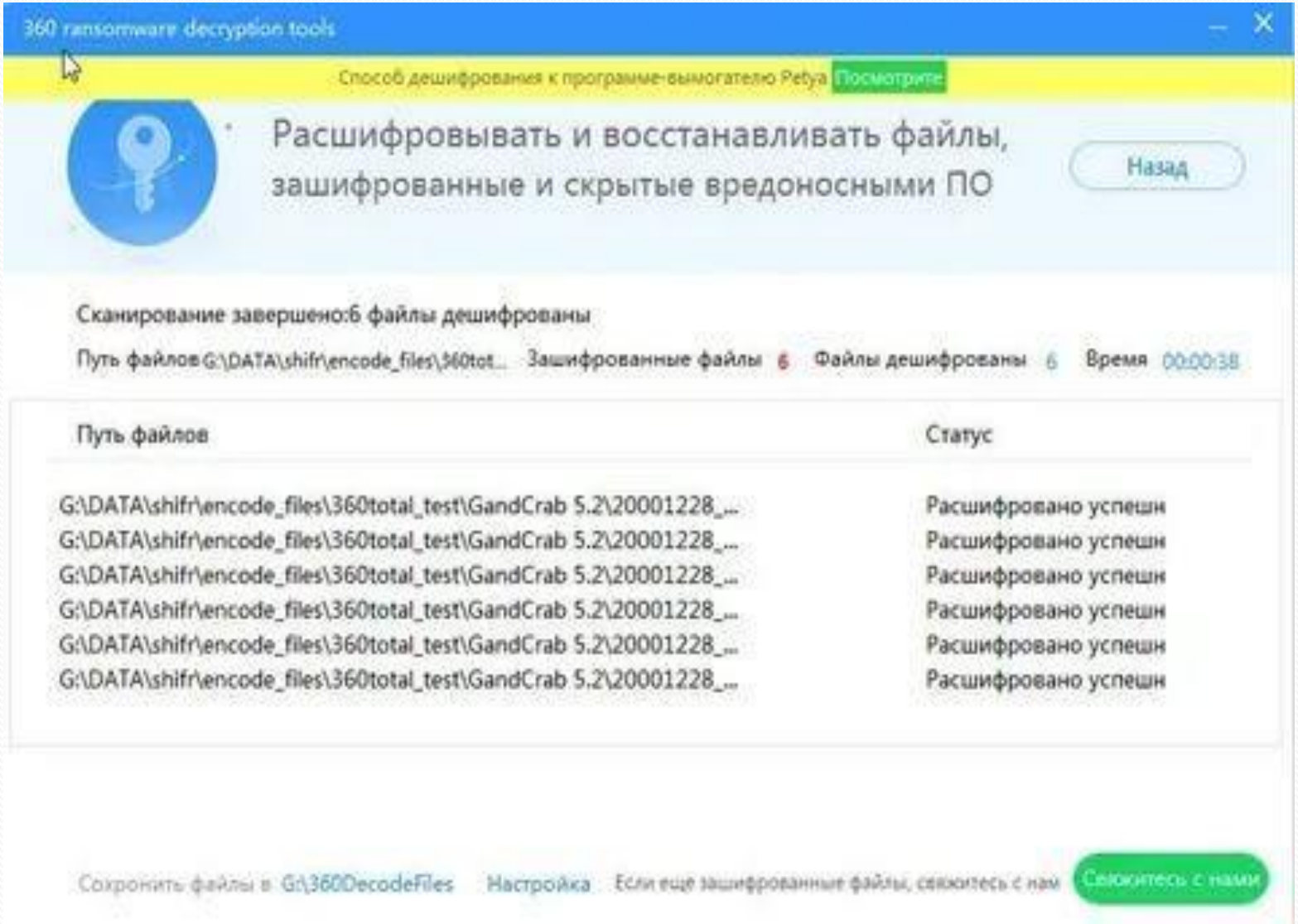
Псевдоантивирусы



Вирусы, блокирующие экран



Программы-вымогатели, шифрующие файлы

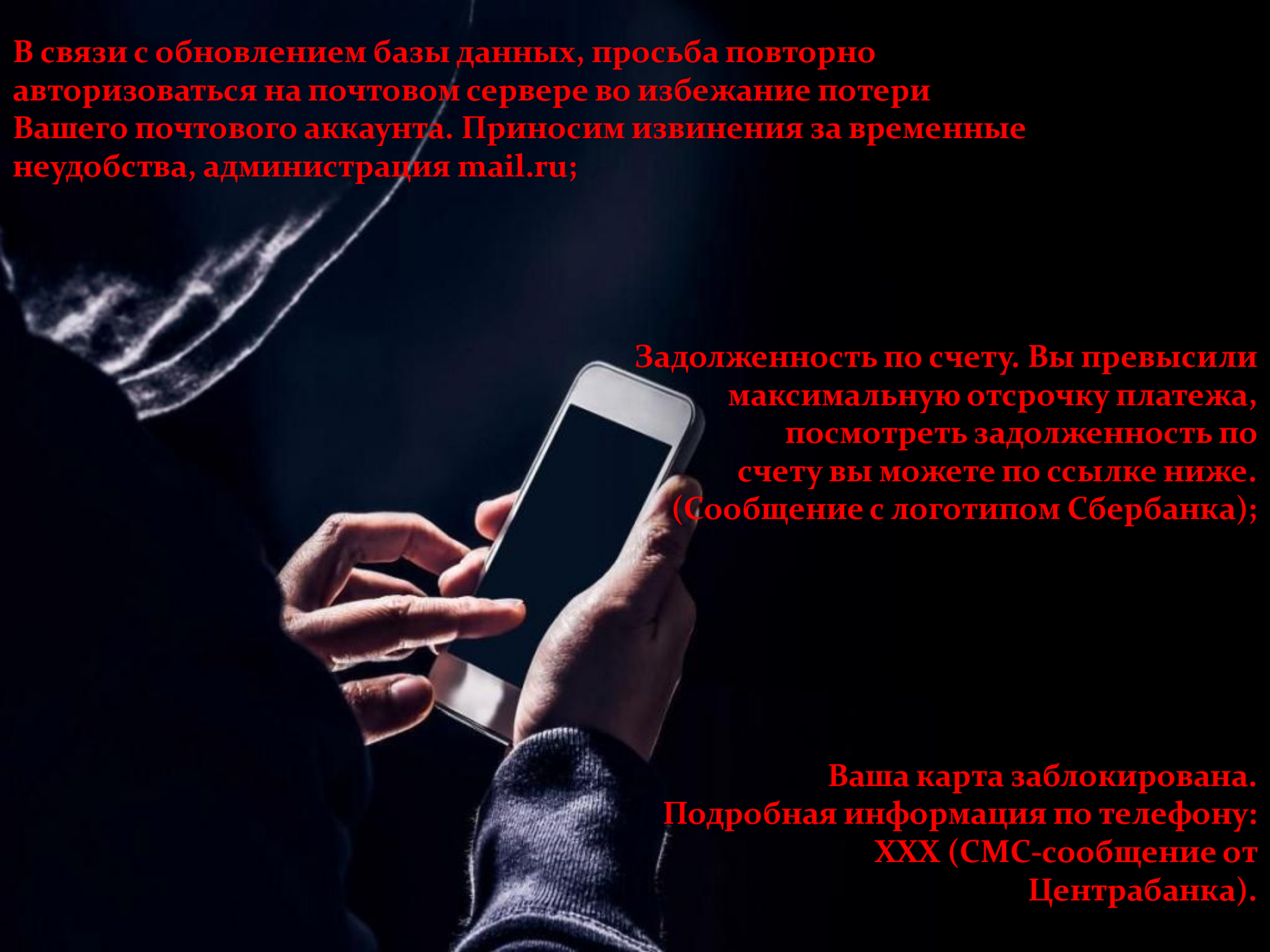


Вредоносное программное обеспечение

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.



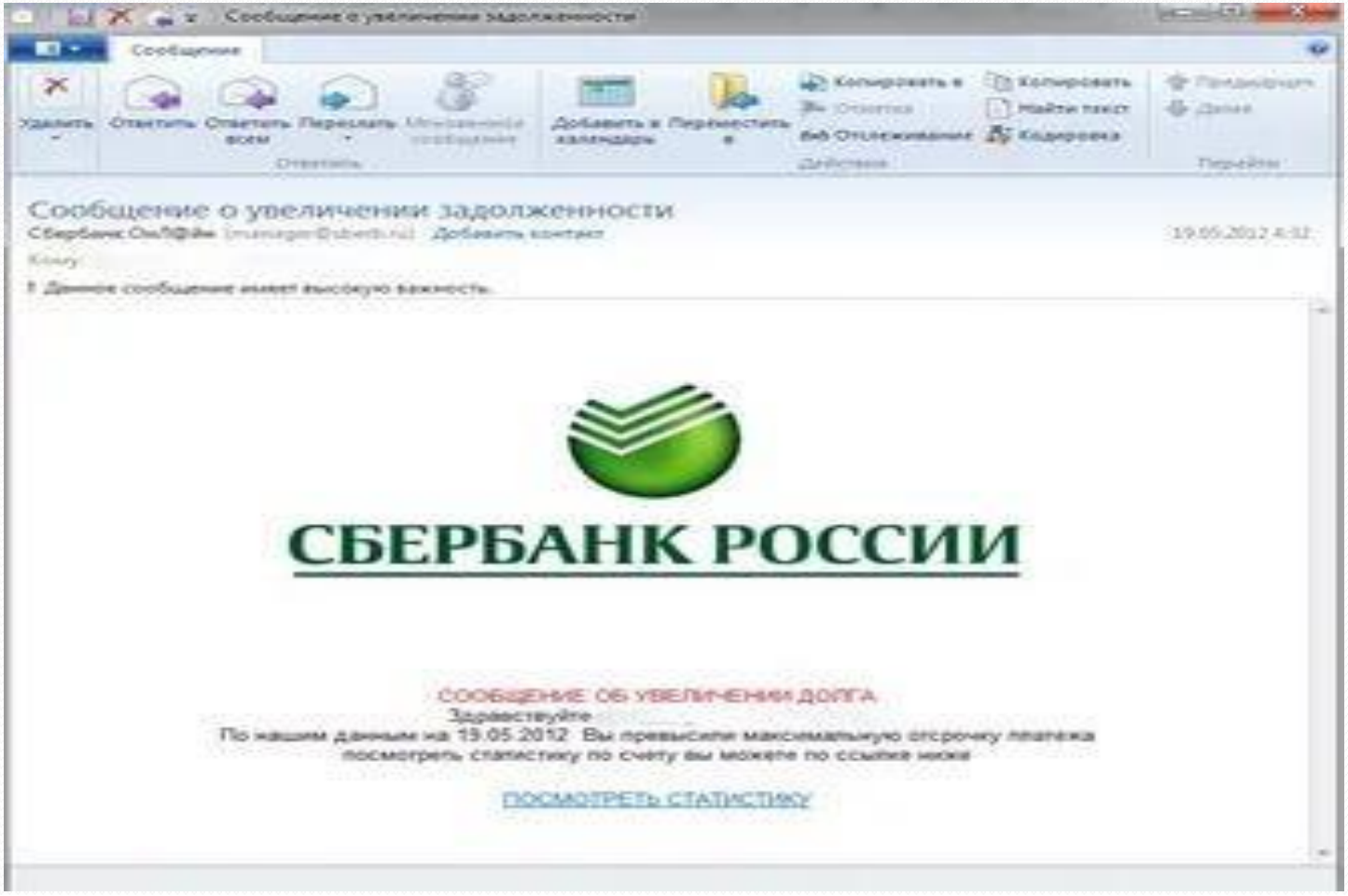
В связи с обновлением базы данных, просьба повторно авторизоваться на почтовом сервере во избежание потери Вашего почтового аккаунта. Приносим извинения за временные неудобства, администрация mail.ru;

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

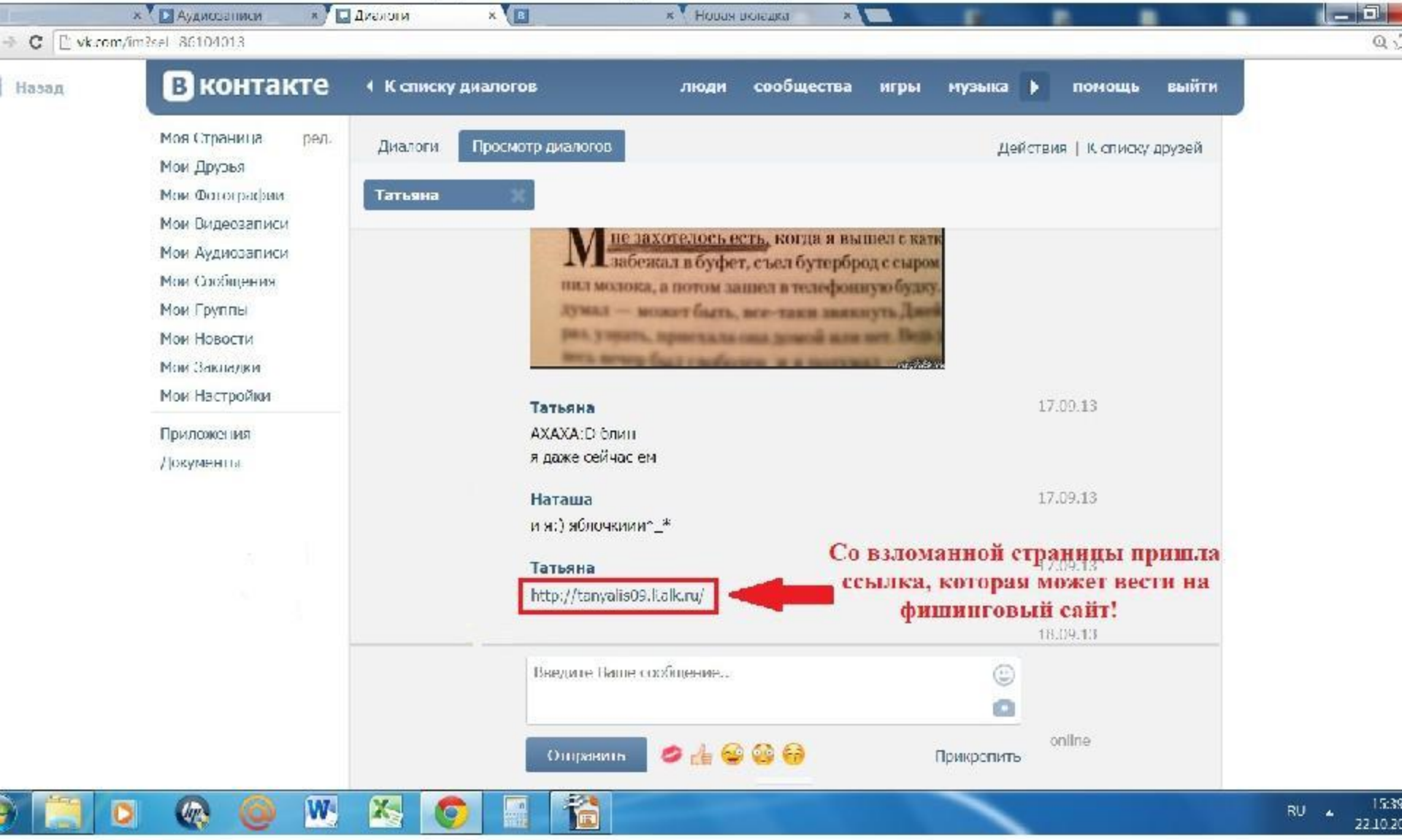
Ваша карта заблокирована. Подробная информация по телефону: XXX (СМС-сообщение от Центрабанка).

Фишинг

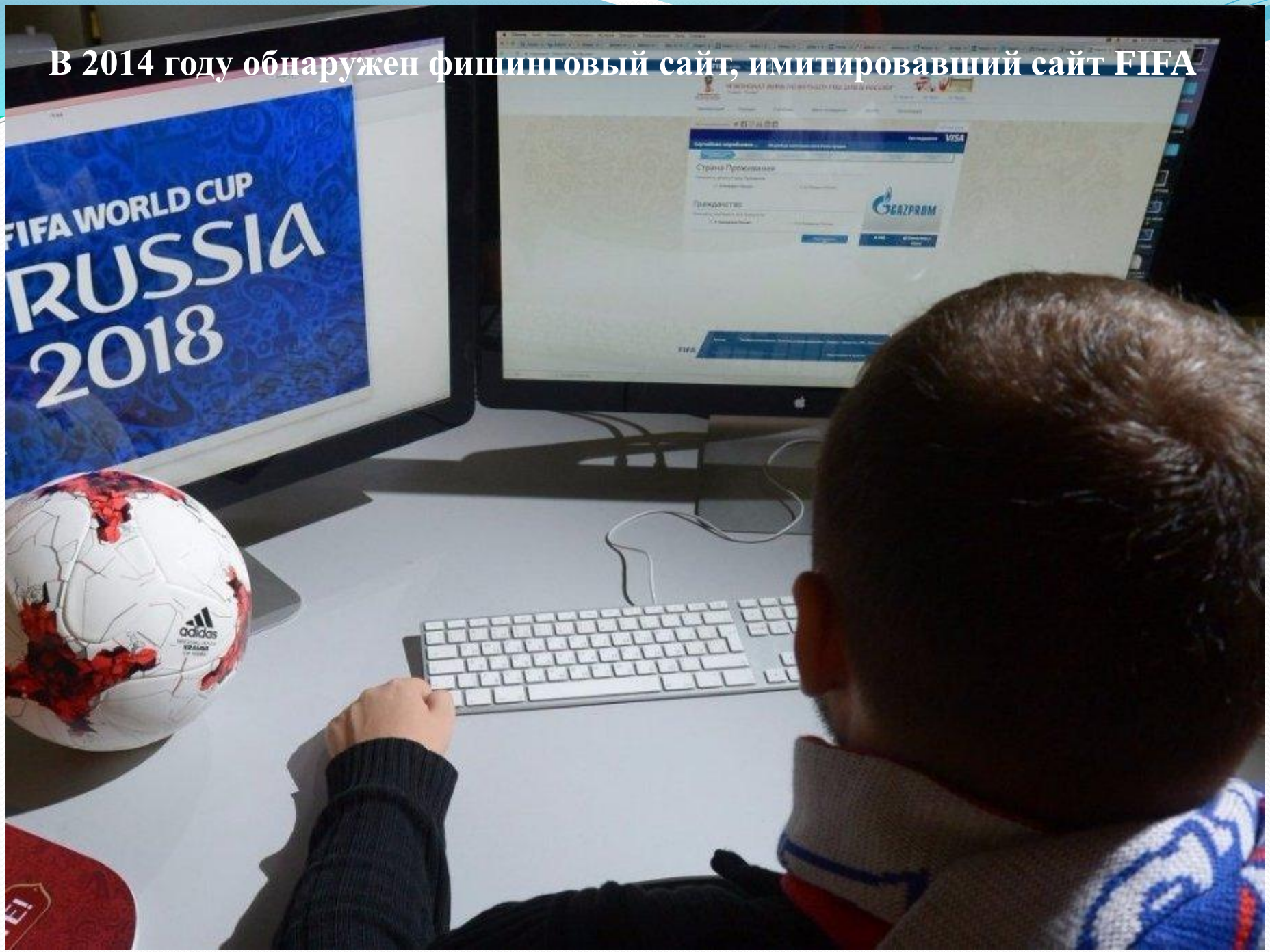
- это рассылка поддельной электронной корреспонденции, которая выглядит как сообщения от надежных источников.



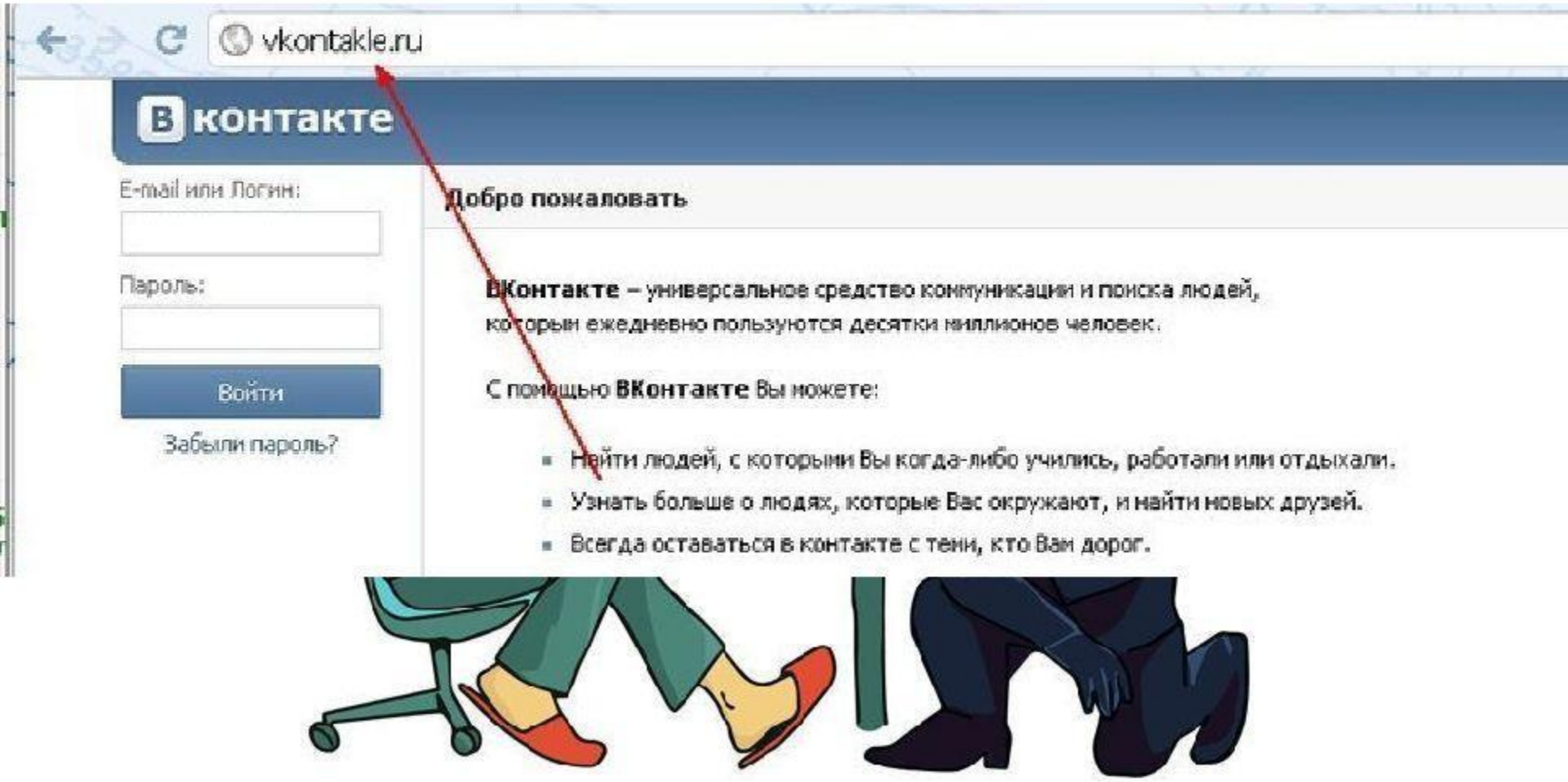
Примеры фишинга



К содержанию


В 2014 году обнаружен фишинговый сайт, имитировавший сайт FIFA
FIFA WORLD CUP
RUSSIA
2018
adidas
VISA
Страна Проживания
Гражданство
GAZPROM
FIFA

Фишинг


vkontakle.ru
ВКонтакте
E-mail или Логин:
Пароль:
Войти
Забыли пароль?
Добро пожаловать
ВКонтакте – универсальное средство коммуникации и поиска людей, которым ежедневно пользуются десятки миллионов человек.
С помощью ВКонтакте Вы можете:
Найти людей, с которыми Вы когда-либо учились, работали или отдыхали.
Узнать больше о людях, которые Вас окружают, и найти новых друзей.
Всегда оставаться в контакте с теми, кто Вам дорог.

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*

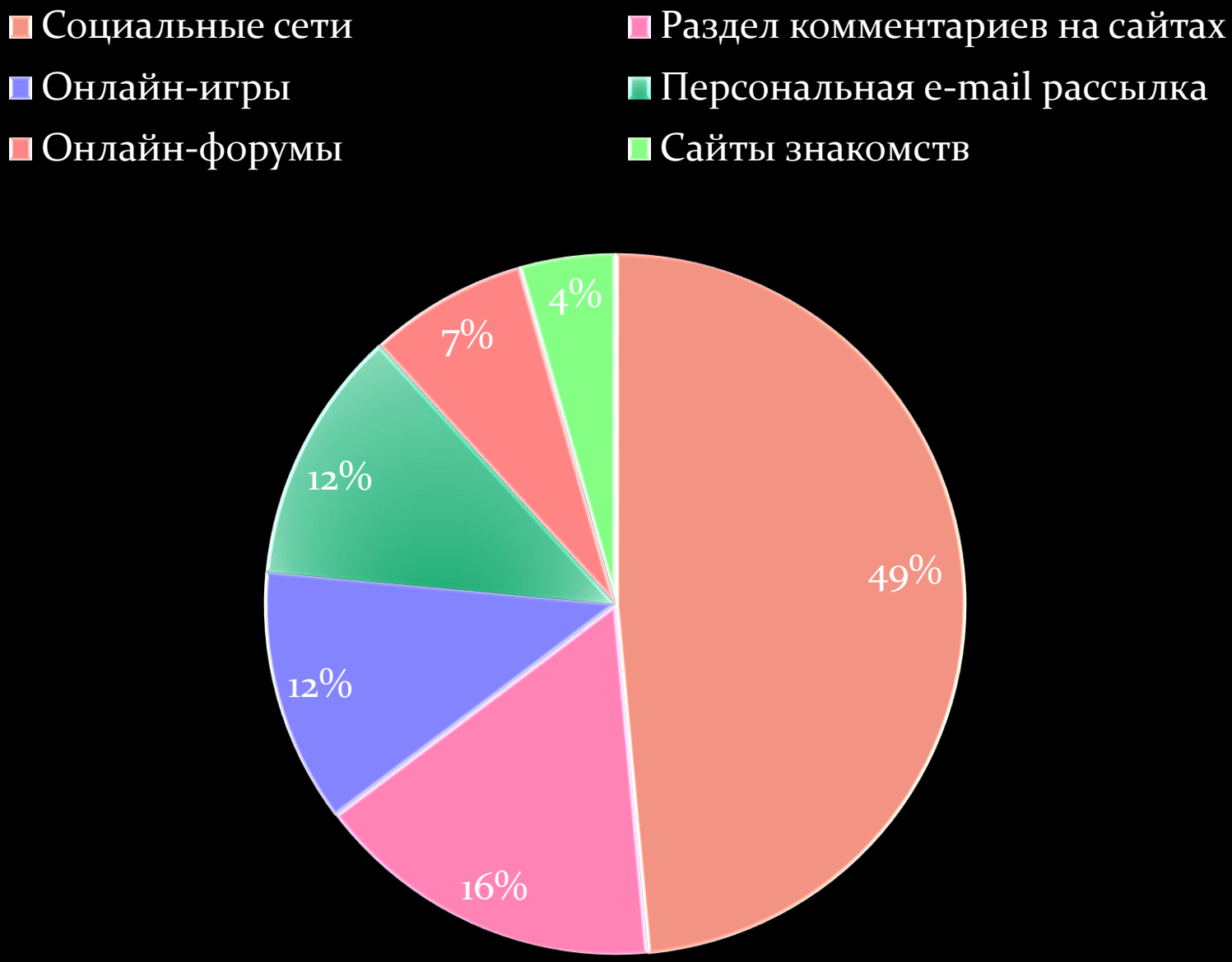
KASPERSKY

- Совместный опрос «Лаборатории Касперского» и портала Сетевичок.рф (онлайн-поддержка и обучение подростков основам кибербезопасности).
- Опрос проводился в Интернете в 2016-16гг., участие приняли более 1100 подростков.

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



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

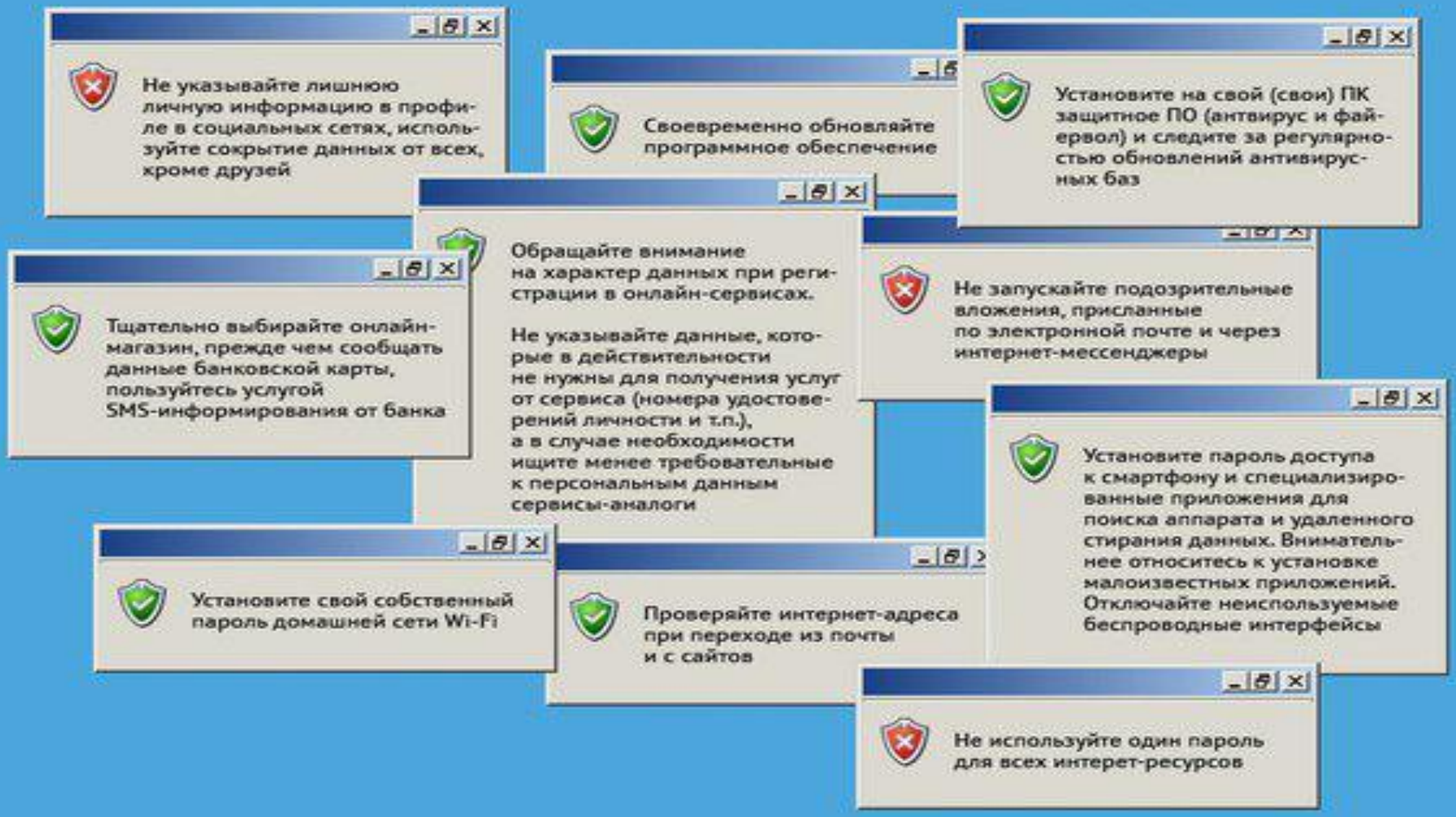
Принуждение к выполнению воли третьих лиц

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

Манипулирование субъектом персональных данных

10 способов защиты личных данных

Как не стать жертвой интернет-мошенников



РОСКОМНАДЗОР

Береги свои ПЕРСОНАЛЬНЫЕ ДАННЫЕ!

RSpectr