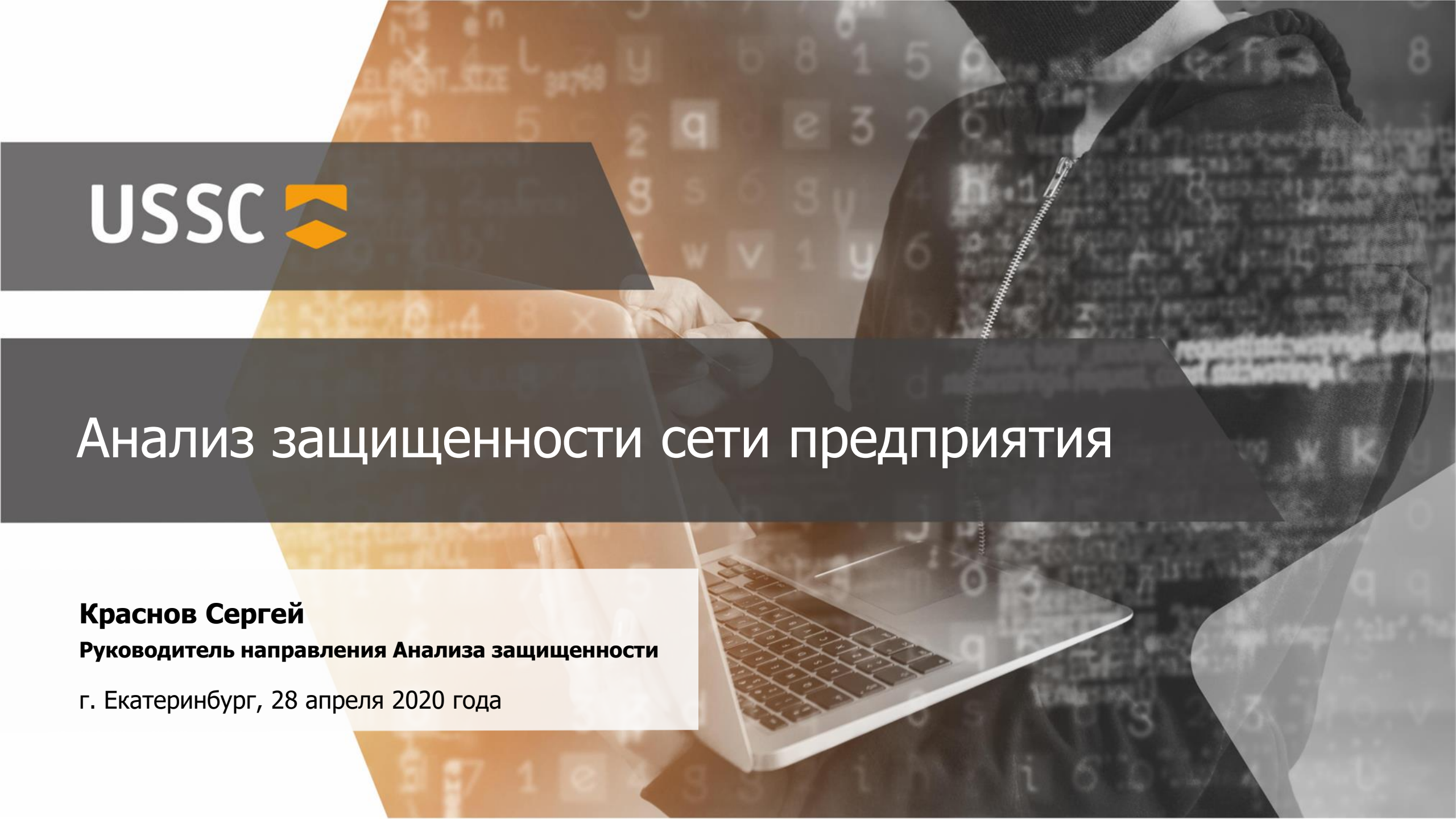


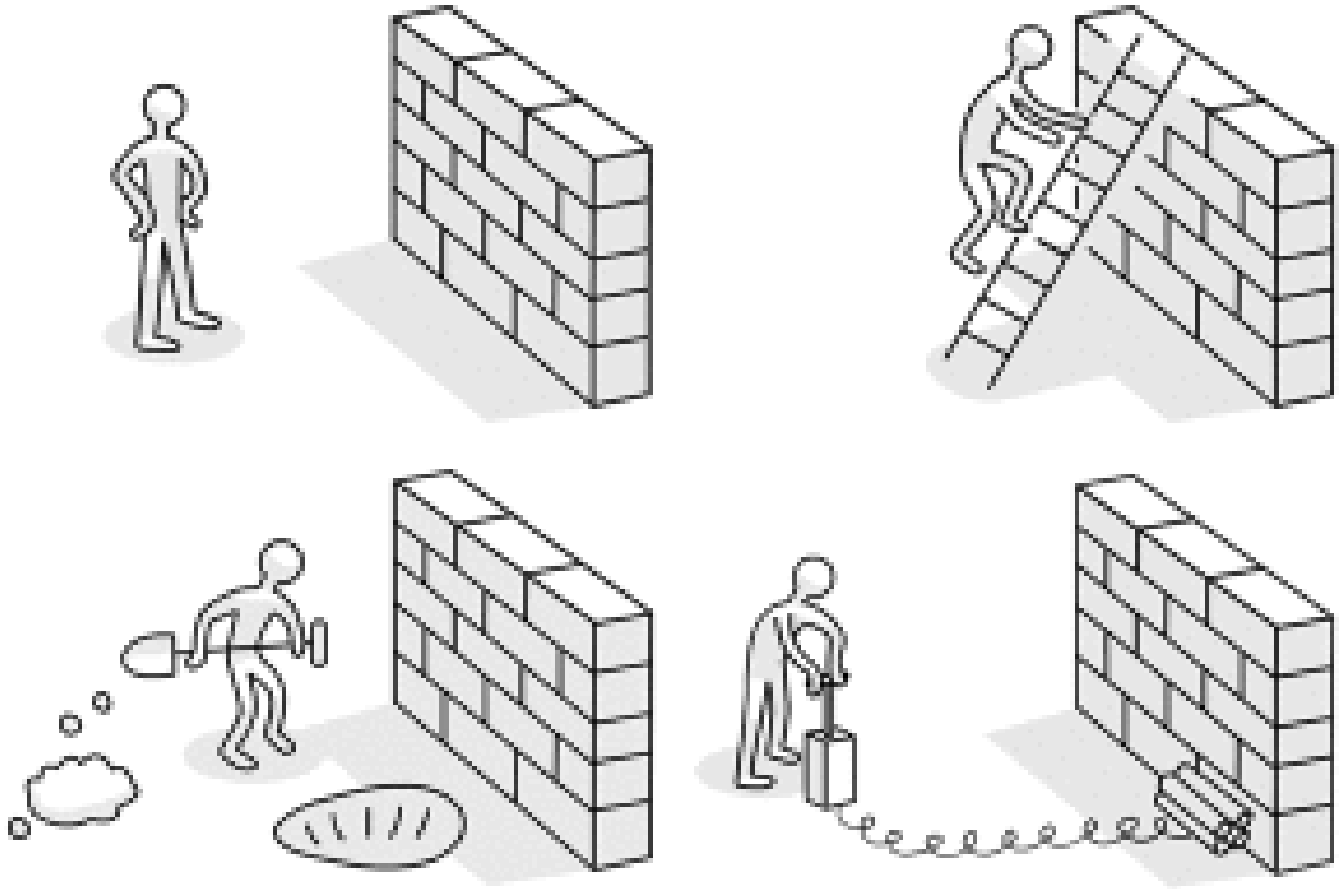
Анализ защищенности сети предприятия

Краснов Сергей

Руководитель направления Анализа защищенности

г. Екатеринбург, 28 апреля 2020 года

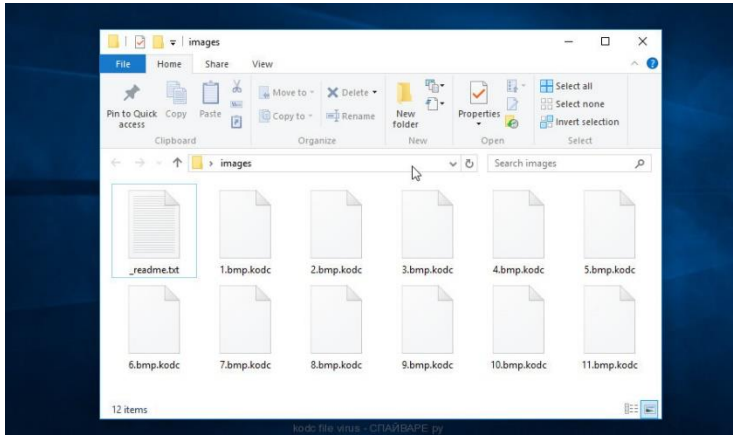
Анализ защищенности/тестирование на проникновение



Методы атак


Использование вредоносного ПО
56%
Социальная инженерия
31%
Взлом инфраструктуры
21%
Эксплуатация веб-уязвимостей
17%
Подбор учетных данных
14%

Взлом сервера базы данных

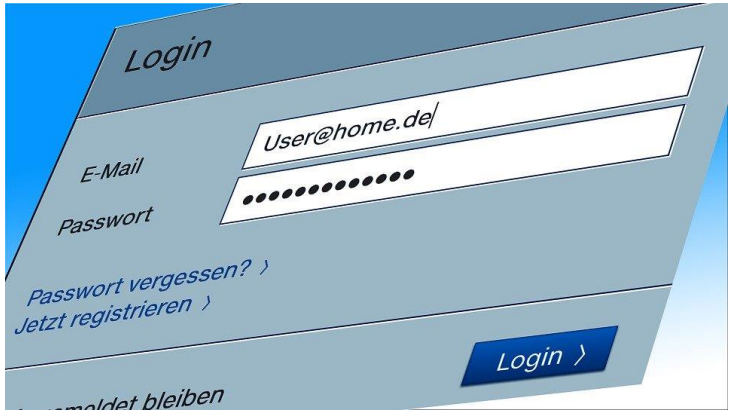


- Современные методы шифрования нельзя расшифровать!
- Доступ к инструментам администрирования должен быть ограничен!

Взлом внутренней сети

- «физический» доступ к беспроводной сети нельзя ограничить!
- Если сеть взломана, то Хакеры получают доступ ко всем данным!

Взлом приложения ДБО



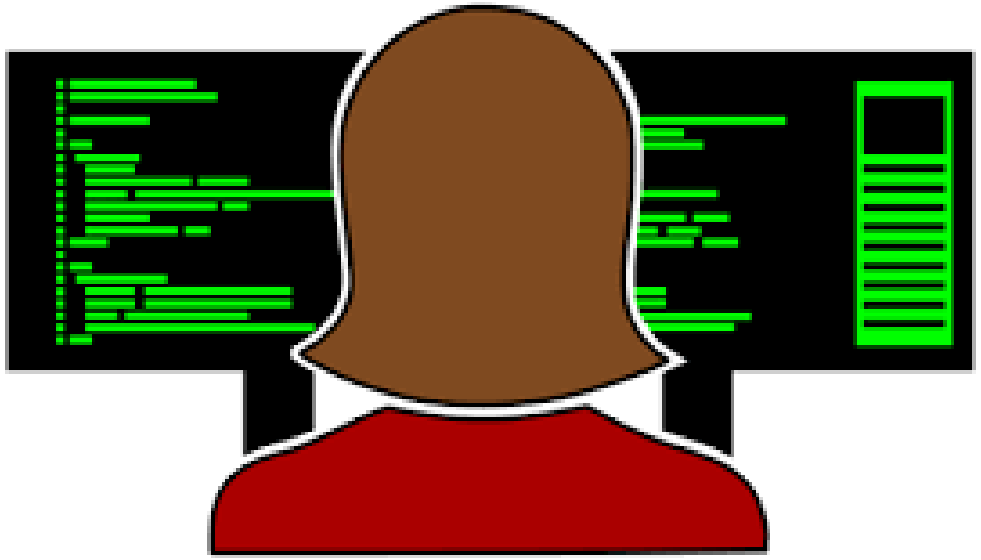
- Механизмы аутентификации можно обойти!
- Необходимо защищать своих клиентов!

Адресный фишинг

- Обмануть человека проще, чем взломать сервер!
- Необходимо обучать сотрудников, рассказывать про угрозы, спам, фишинг!

Взломы, взломы, взломы….

- Атакуют авиакомпании: похищают накопленные мили
- Атакуют управляющие компании: похищают базы клиентов и конфиденциальную информацию
- Атакуют инфраструктуру: майнят биткоины на серверах разработчиков
- Атакуют финансовые организации: проводят фрод, рассылки на клиентов
- …



Криминальный бизнес

Fancy Bears
с англ. — «Прикольные мишки»
2004 г. – наст. время

Жертвы атак: государственные, информационные, военные и другие структуры зарубежных стран, российские оппозиционеры и журналисты

Цель: официальная: борьба за чистый спорт без применения любого вида допинга; по мнению некоторых западных контрразведывательных организаций – государственный шпионаж для российских спецслужб

Методы: фишинговые атаки, письма с вирусами, вредоносные сайты, регистрация доменов-двойников

Известные кибератаки:
2015 г. – информационная система Бундестага (Германия)
2015 г. – телеканал TV5 Monde (Франция)
2015 г. – информационные системы Белого Дома США и NATO
2016 г. – внутренняя сеть Демократической партии и Национальный комитет Демократической партии США
2016 г. – сайт Всемирного антидопингового агентства WADA (Канада)
2016 г. – взлом новейшей версии ОС Windows

Анонимный интернационал
также известен как
«Шалтай-Болтай»
2013 г. – наст. время (?)

Жертвы атак: члены правительства РФ, депутаты, крупные фирмы, СМИ

Цель: продажа через интернет полученных данных

Методы: перехват переписок и взлом аккаунтов

Известные кибератаки:
2013 г. – трансляция новогоднего обращения президента РФ Владимира Путина
2014 г. – электронные письма из ящика, якобы принадлежащего вице-премьеру РФ Аркадию Дворковичу
2014 г. – Twitter-аккаунт премьер-министра РФ Дмитрия Медведева
2015 г. – переписка Натальи Тимаковой, пресс-секретаря премьер-министра Дмитрия Медведева
2015 г. – СМС-переписка Тимура Прокопенко, заместителя главы Управления Президента Российской Федерации по внутренней политике
2016 г. – два почтовых ящика и переписки в WhatsApp телеведущего Дмитрия Киселёва

Anonymous
с англ. — «анонимный», «безымянный»
2003 г. – наст. время

Жертвы атак: правительственные, религиозные и корпоративные веб-сайты

Цель: протест против социальных и политических явлений, цензуры в интернете, преследования и надзора

Методы: хактивизм (соединение слов хакер и активизм) — использование компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации

Известные кибератаки:
2010 г. – платежные системы PayPal, Mastercard, Visa
2010 г. – сайт WikiLeaks
2011 г. – более 40 ресурсов, распространяющих детскую порнографию («Операция Darknet»)
2012 г. – сайт Интерпола
2013 г. – официальный сайт Комиссии по исполнению наказаний (США)
2015 г. – 5000 аккаунтов членов террористической группировки «Исламское государство» (ИГИЛ, запрещена в России) («Операция Париж»)

LulzSec аббревиатура Lulz Security, с англ. — «смех над безопасностью»
Май 2011 – июнь 2011 гг.

Жертвы атак: серверы компаний, считающиеся наиболее надежно защищенными

Цель: первоначально «ради смеха», но позднее группа переориентировалась на «политически мотивированные [...] хакерские атаки»

Методы: после успешных атак традиционно оставляют на ресурсах колкие послания

Известные кибератаки:
2011 г. – сайты сената США, ЦРУ США
2011 г. – сайт британского Агентства по раскрытию тяжких преступлений и борьбе с организованной преступностью (SOCA)
2011 г. – сервер полиции американского штата Аризона
2011 г. – японский сайт Sony BMG
2011 г. – кража паролей Fox.com, LinkedIn и 73 тысяч участников конкурса X Factor
2011 г. – аккаунты пользователей ресурса Sony Pictures

Lizard Squad
с англ. — «Отряд ящериц»
2014 г. – наст. время

Жертвы атак: серверы игр, сайты игровых услуг

Цель: объяснения причин атак и мотивов ни за одним из взломов не последовало

Методы: DDoS-атака (Distributed Denial of Service, с англ. – распределённый отказ в обслуживании): атака выполняется одновременно с большого числа компьютеров для отказа в обслуживании хорошо защищённой крупной компании или правительственной организации

Известные кибератаки:
2014 – серверы игр League of Legends и Call of Duty
2014 г. – серверы Sony Playstation Network и Microsoft Xbox Live
2014 г. – Интернет в Северной Корее
2015 г. – сайт Malaysia Airlines

Syrian Electronic Army
«Сирийская электронная армия»
2011 г. – наст. время

Жертвы атак: ресурсы политических оппозиционных групп, правозащитных организаций и западные новостные сайты, дающие, по мнению САА, ложную информацию о конфликте в Сирии

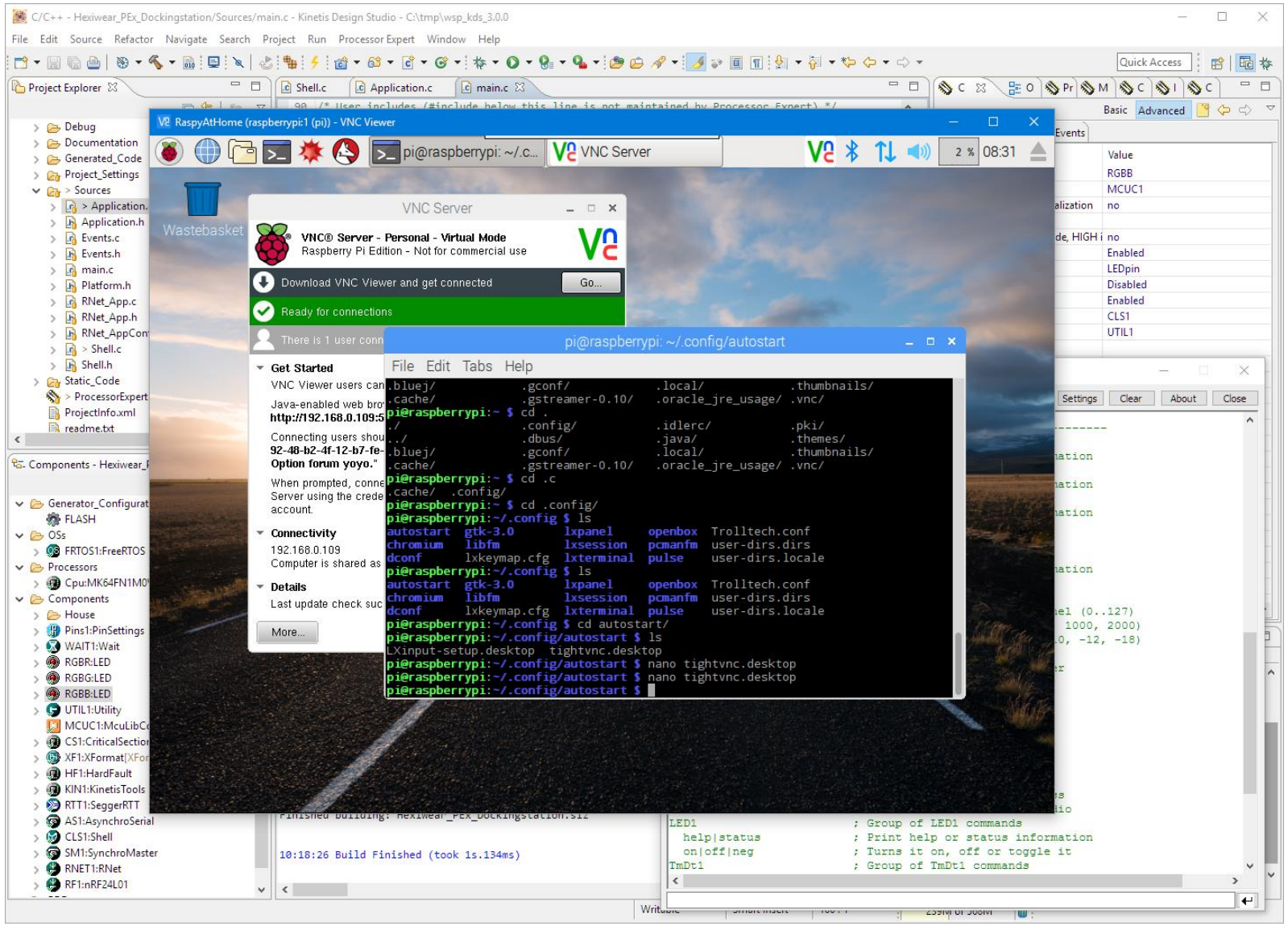
Цель: поддержка президента Сирии Башара Асада

Методы: DDoS-атаки, рассылка спама, распространение вирусов, фишинг (рассылка электронных писем от имени популярных брендов с просьбами сообщить свои учётные данные и пароли)

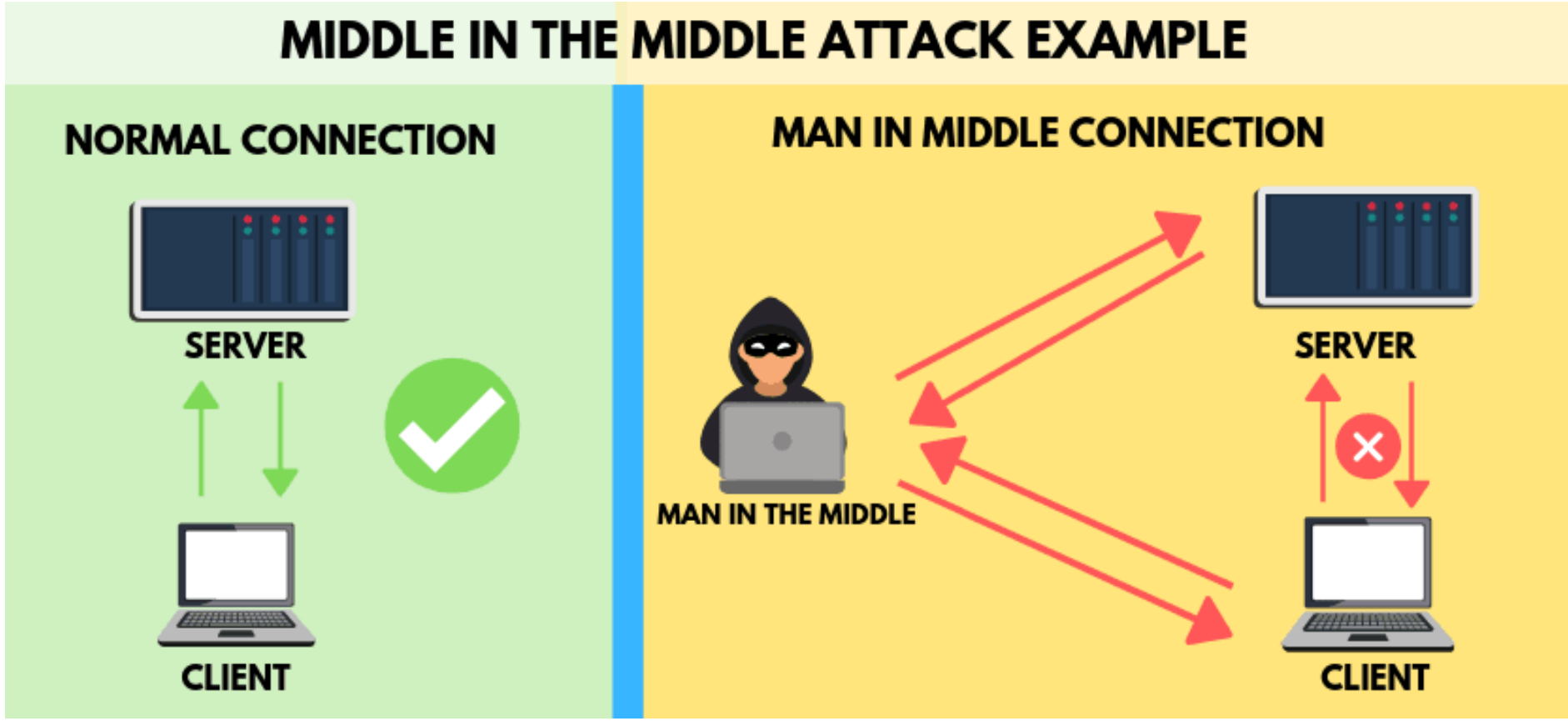
Известные кибератаки:
2012 г. – Twitter-аккаунт новостного агентства Reuters (Великобритания)
2013 г. – Facebook-аккаунты Барака Обамы и Николя Саркози
2013 г. – газеты The New York Times (США), The Huffington Post (США)
2013 г. – интернет-сайт по подбору персонала для Корпуса морской пехоты США
2014 г. – сайты eBay и PayPal Великобритании
2014 г. – сайты британских газет The Sun и The Sunday Times

Атаки на сотрудников

Установка средств удаленного администрирования



Proxy – Man In The Middle



Диверсии


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/18/2013
10:29 AM
Time left
71 : 57 : 51
Next >>

Как повысить уровень защищенности

№	Способ	Особенности
1.	Внедрить средства защиты	• Можно быстро выполнить • Непонятно что внедрять • Невозможно оценить пользу
2.	Провести аудит ИБ	• Дает оценку всех процессов со стороны ИБ • Дает понимание угроз и рисков • Дает информацию о актуальных требованиях • Дает понимание что необходимо улучшить и как это сделать • Достаточно долго • Достаточно дорого
3.	Провести анализ защищенности	• Описание актуальных уязвимостей • Демонстрация опасности и описание рисков • Перечень первоочередных действий для защиты • Относительно быстро • Относительно дешево

Услуги по анализу защищенности:

1. Анализ защищенности **внешнего периметра**
2. Анализ защищенности **внутренней сети**
3. Анализ защищенности **логического функционала веб-приложения**
4. **Нагрузочное** стресс тестирование
5. Тестирование **методами социальной инженерии**

Среднестатистическая современная компания

Внешние ресурсы:

- Электронная почта
- Файлообменники
- Корпоративные сайты
- И др.

Внутренние ресурсы:

- Гостевые сети
- Корпоративная сеть
- Критичные ресурсы
- Инженерные сети

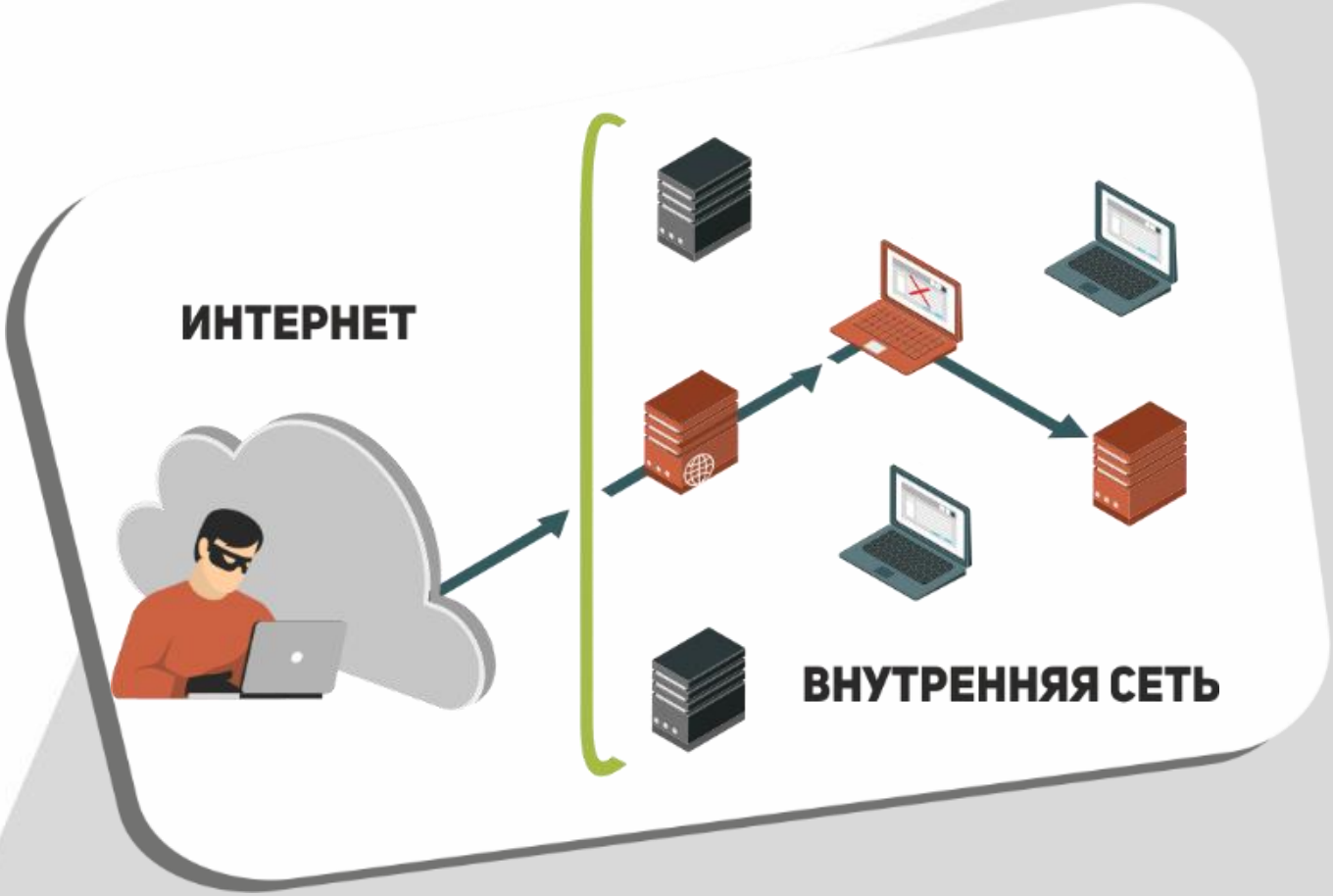
Человеческие ресурсы:

- Сотрудники
- Подрядчики
- Гости

★ Программные Продукты,
Веб-сервисы

Анализ защищенности внешнего периметра

Это обследование информационных ресурсов, доступных из сети Интернет. Проводится полная инвентаризация доступных ресурсов, выявляются уязвимости приложений, операционной системы и сетевой инфраструктуры.
Для веб-приложений проверяются только уязвимости конфигураций и уязвимости используемого программного обеспечения.
Логический функционал веб-приложений не проверяется

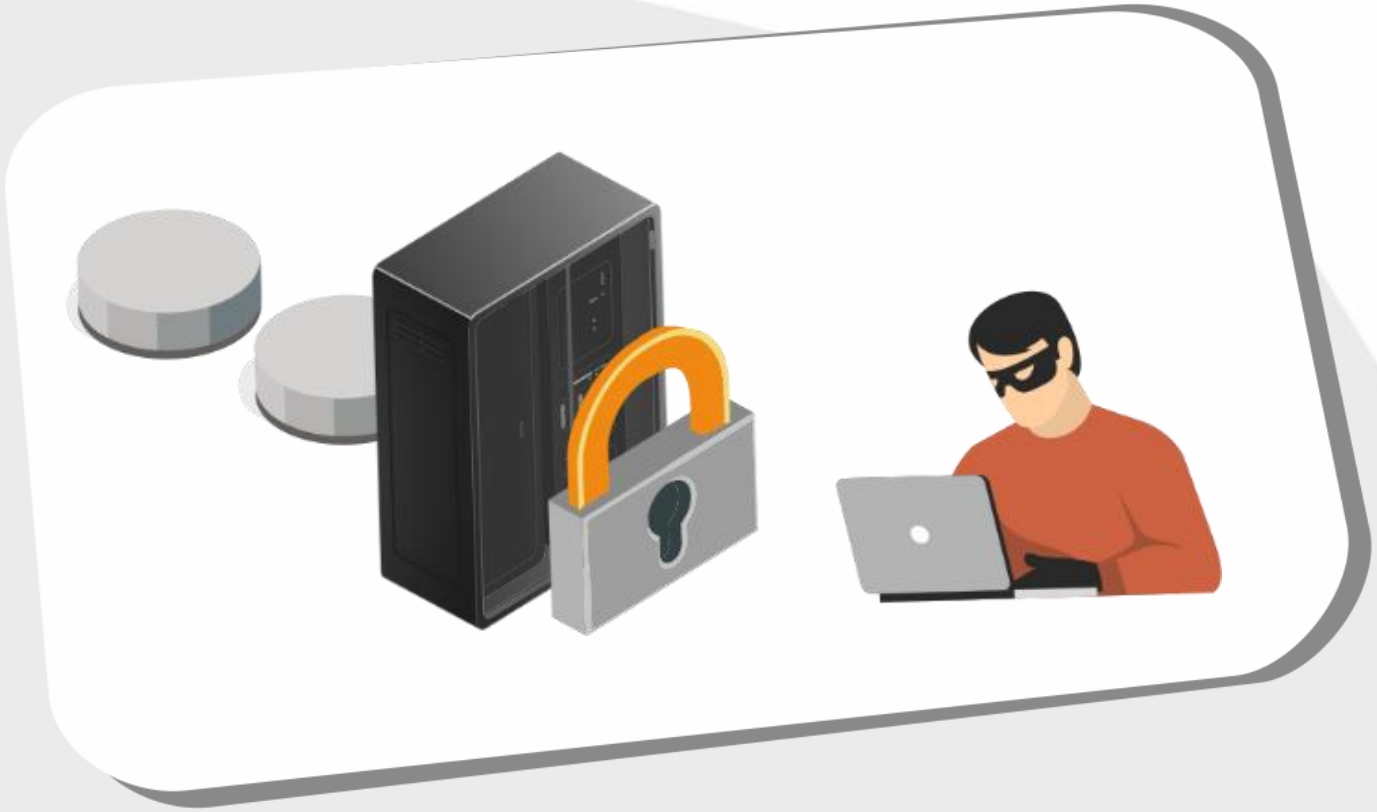


Анализ защищенности внутренней сети

Это обследование внутренней корпоративной сети, персональных компьютеров сотрудников, серверов и сетевого оборудования.
Так же, в данное обследование может входить анализ защищенности беспроводных сетей передачи данных (Wi-Fi)

USSC

Анализ защищенности логического функционала веб-приложения



Это обследование всего функционала веб-приложения и выявление уязвимостей, допущенных при его разработке. Так же, в данное обследование может входить анализ Исходного кода веб-приложения и анализ мобильных приложений

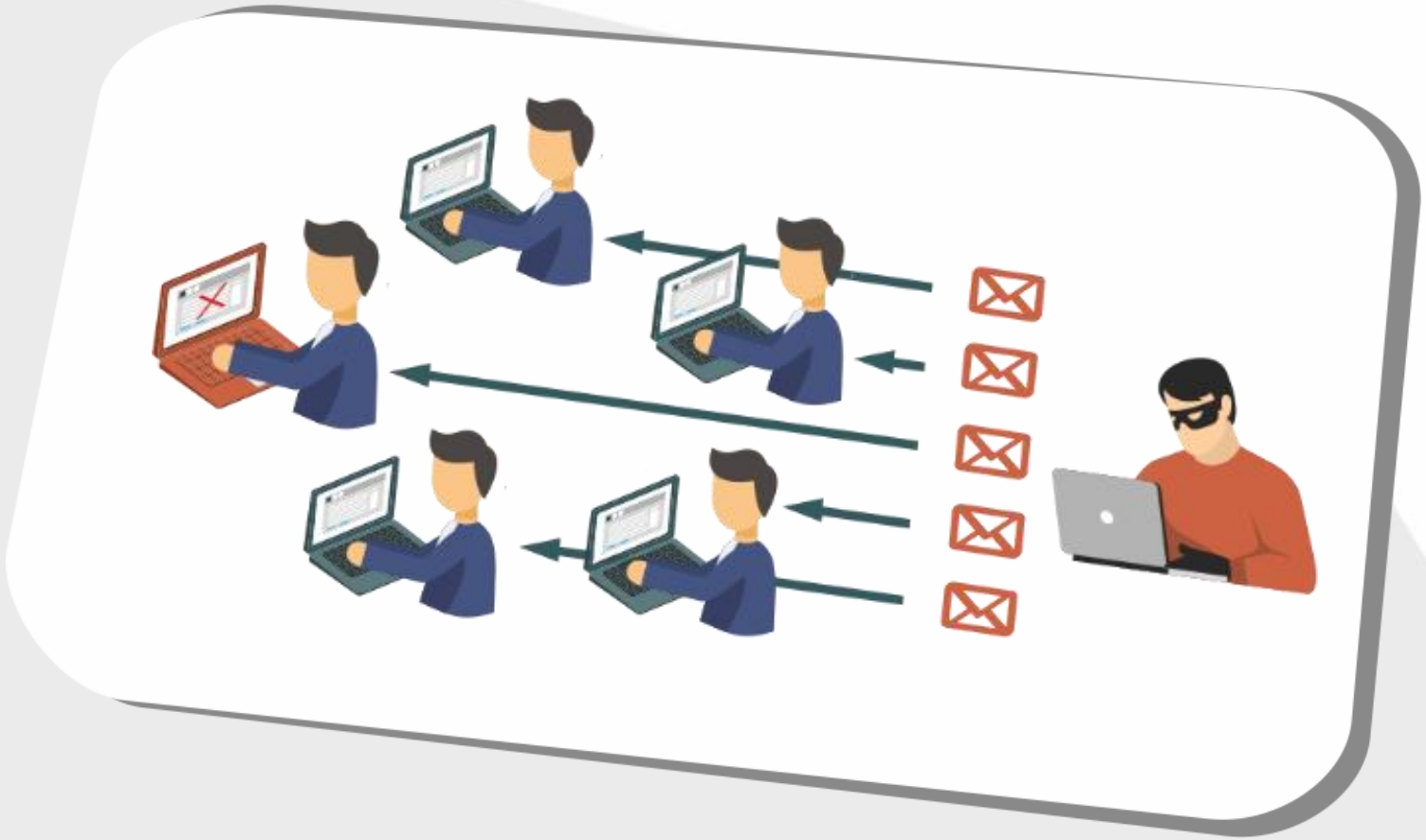
PENTEST.USSC.RU

Нагрузочное стресс тестирование

Это исследование времени отклика
веб-приложения при высоких и пиковых нагрузках на его функционал. Моделируются атаки типа «отказ в обслуживании» и отслеживается какое воздействие они оказывают

USSC

Тестирование методами социальной инженерии



Это проверка уровня осведомленности сотрудников в вопросах информационной безопасности. Моделируется вредоносная рассылка на адреса электронной почты сотрудников и отслеживается их реакция на данную рассылку

PENTEST.USSC.RU

А можно ли взломать Ваши информационные системы?

- На сколько хорошо вы знаете свои информационные системы?
- Вы уверены в безопасности решений поставщиков?
- Какие возможности есть у сотрудников компании?
- Готова ли ваша служба ИБ к реальному взлому?
- Все ли сотрудники знают, как нужно себя вести при инцидентах?

Наша команда

OFFENSIVE security OSCP

EC-Council CEH Certified Ethical Hacker

OFFENSIVE® security OSCE

C|HFI Computer Hacking Forensic INVESTIGATOR

О компании ООО «УЦСБ»

ООО «УЦСБ» – Уральский центр систем безопасности – межрегиональная специализированная компания, оказывающая услуги в области проектирования, разработки, внедрения и сервисной поддержки решений по обеспечению информационной безопасности современных информационных систем, инженерно-технических систем охраны, центров обработки данных и корпоративных сетей связи для банковских структур, операторов связи, государственных организаций, предприятий промышленного сектора и других отраслей экономики.

USSC

СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?

КОНТАКТЫ

Краснов Сергей

Руководитель направления
Анализа защищенности

pentest@ussc.ru

pentest.ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU

PENTEST.USSC.RU