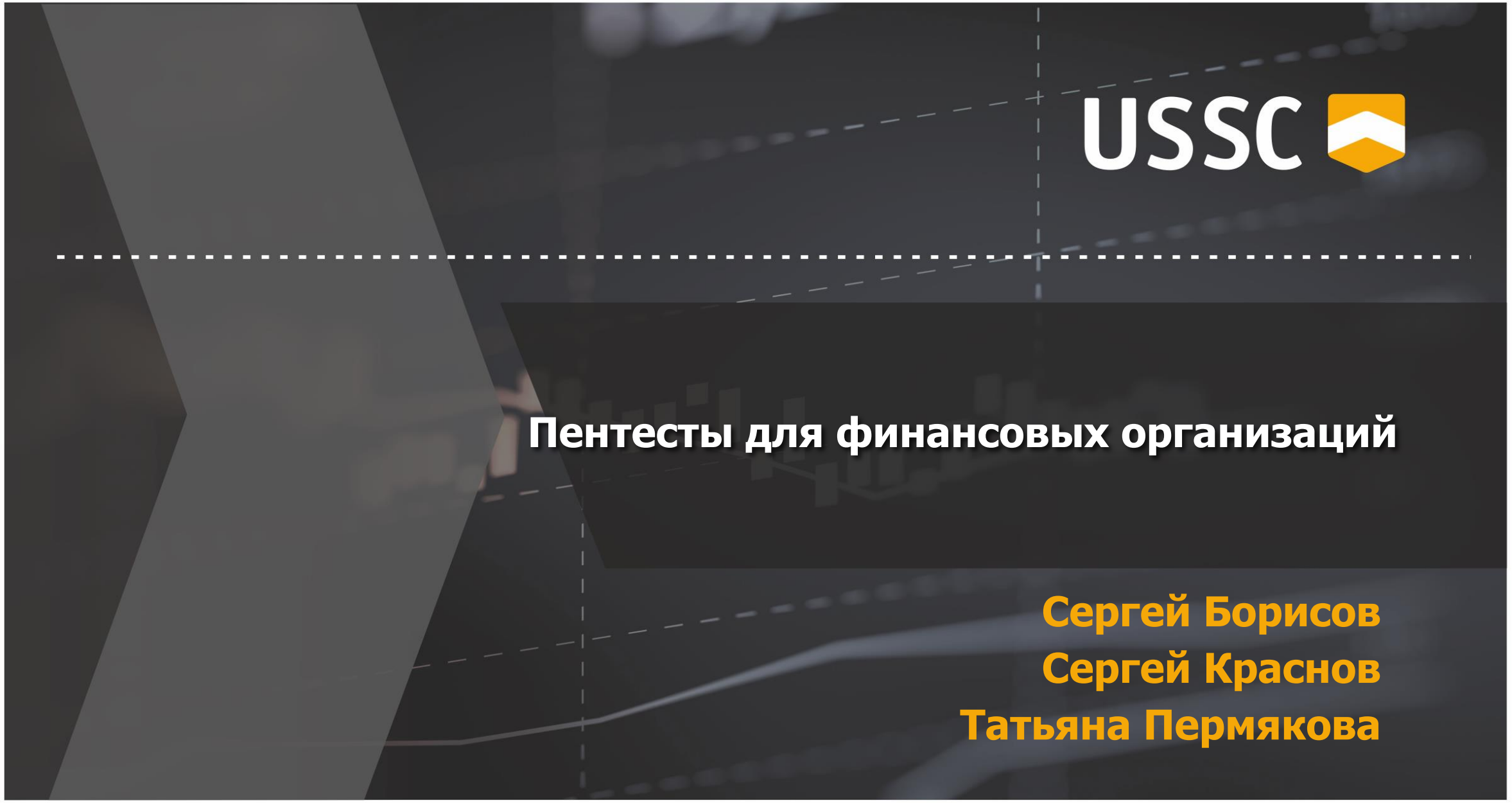

USSC
Пентесты для финансовых организаций
Сергей Борисов
Сергей Краснов
Татьяна Пермякова

График проведения вебинаров

№	Дата	Название
1	15.04	Требования Банка России по информационной безопасности некредитных финансовых организаций
2	22.04	Требования Банка России по информационной безопасности кредитных финансовых организаций
3	29.04	Анализ уязвимостей по требованиям к ОУД4
4	20.05	Обзор требований ГОСТ Р 57580.1-2017
5	17.06	Как проводится аудит по ГОСТ Р 57580?
6	08.07	Онлайн-сервис оценки соответствия ГОСТ Р 57580.2-2018
7	26.08	Требования к средствам криптографической защиты информации в финансовых организациях
8	16.09	Пентесты для финансовых организаций
9		Обзор изменений законодательства по защите информации финансовых организаций

Ведущие третьего выпуска

Сергей Борисов

Заместитель руководителя по ИБ

обособленного подразделения УЦСБ

г. Краснодар

Сергей Краснов

Руководитель направления Анализа защищенности

Аналитический центр УЦСБ

г. Екатеринбург

CEH, CHFI

Татьяна Пермякова

Аналитик

Аналитический центр УЦСБ

г. Екатеринбург

Блог: https://sborisov.blogspot.com

План

- [ ] Обзор нормативных требований
- [ ] Методы атак
- [ ] Виды проведения пентеста
- [ ] Примеры успешно проведенных пентестов
- [ ] Описание результатов тестирования

План

- [ ] Обзор нормативных требований
- [ ] Методы атак
- [ ] Виды проведения пентеста
- [ ] Примеры успешно проведенных пентестов
- [ ] Описание результатов тестирования

Требования положений Банка России

382-П	Операторы по переводу денежных средств Операторы услуг платежной инфраструктуры Операторы услуг информационного обмена	Ежегодное тестирование на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры	С 01.01.2020
683-П	Все кредитные финансовые организации	Ежегодное тестирование на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры	с 01.06.2019
684-П	Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации	Тестирование на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры на предмет проникновений	с 01.06.2019
672-П	Участники платежной системы Банка России	Уровень защиты информации по ГОСТ Р 57580.1-2017: • стандартный (уровень 2) для участников СБП • усиленный (уровень 1) для ОПКЦ	с 01.07.2021 с 06.04.2019

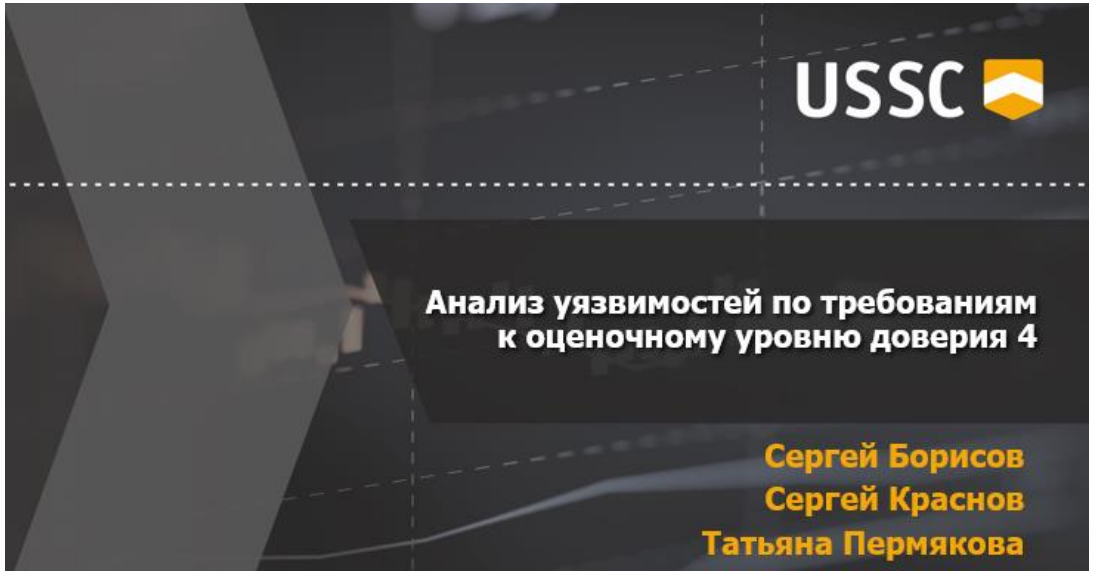
ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017
Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

	Мера СЗИ		УЗ информации		
			3	2	1
Ввод в эксплуатацию АС	ЖЦ.14	Реализация контроля защищенности АС, включающего*: • **тестирование на проникновение** • анализ уязвимостей системы защиты информации АС и информационной инфраструктуры промышленной среды	Н	О	О
Эксплуатация (сопровождение) АС	ЖЦ.20	Реализация проведения **ежегодного** контроля защищенности АС, включающего: • **тестирование на проникновение** • анализ уязвимостей системы защиты информации АС и информационной инфраструктуры промышленной среды	Н	О	О

** По решению ФО при модернизации АС проводится контроль защищенности только элементов информационной инфраструктуры, подвергнутых модернизации*

Пентест или анализ уязвимостей?



Тестирование на проникновение *VS* **Анализ уязвимостей**

Тестирования на проникновение: ПО и АС

В соответствии с Положениями ЦБ и ГОСТ Р 57580.1-2017

В отношении АС

Объекты информационной инфраструктуры

при модернизации АС
(по решению финансовой организации)

- **при вводе АС в эксплуатацию** (ЖЦ.14)
- **не менее 1 раза в год** (ЖЦ.20)

В рамках анализа уязвимостей ПО

- Прикладное ПО и приложения, распространяемое клиентам для осуществления банковских операций
- Прикладное ПО и приложения, обрабатывающие защищаемую информацию при приеме электронных сообщений

для каждого обновления ПО
(или для релизов, затрагивающих существенные изменения в части функционирования ядра, обеспечения ИБ)

Тестирование на проникновение АС

ГОСТ Р 57580.1-2017
Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

Объекты информационной инфраструктуры:

Объекты доступа:

- АРМ (пользователей и администраторов)
- серверное и сетевое оборудование
- системы хранения данных
- устройства печати и копирования информации
- объекты доступа, расположенные в общедоступных местах и т.д.

Субъекты доступа:

- базы данных
- сетевые файловые ресурсы
- виртуальные машины
- ресурсы доступа, относящиеся к сервисам электронной почты, WEB-сервисам финансовой организации в сетях Интранет и Интернет и т.д.

Совокупность объектов информационной инфраструктуры – **контур безопасности**

Тестирование платежных систем

USSC

Информационное дополнение:

Руководство по тестированию на проникновение

PCI Security Standards Council

	Сканирование уязвимостей	Тест на проникновение
Цель	Выявление и ранжирование уязвимостей (которые в случае эксплуатации могут привести к компрометации системы)	Определение способов эксплуатации идентифицированных уязвимостей (обхода или преодоления функций защиты)
Когда	• не реже 1 раза в квартал • после значительных изменений	• не реже 1 раза в год • при значительных изменения
Как	Автоматизированные инструменты в сочетании с ручной проверкой	Ручное тестирование, которое может включать использование автоматизированных инструментов
Результат	Перечень идентифицированных уязвимостей	Исчерпывающий отчет

Система контроля безопасности клиентов SWIFT

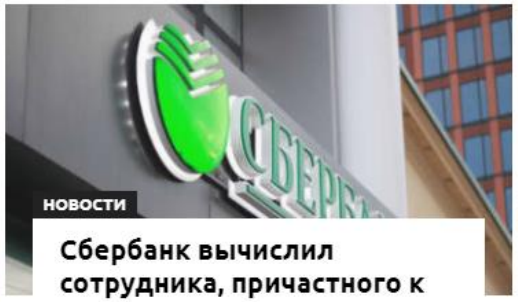
	Сканирование уязвимостей	Тест на проникновение
Цель	Выявление известных уязвимостей в локальной среде SWIFT	Проверить конфигурацию операционной безопасности и выявить бреши в безопасности
Когда	• не реже 1 раза в год • после значительных изменений	• не реже 1 раза в 2 года • после значительных изменений
Что	• ПК оператора • Все приложения и ОС, связанные со SWIFT	• ПК оператора: все оборудование, ПО и сеть • Уровень обмена данными • Все оборудование, ПО и сетевые компоненты (за исключением приложений для SWIFT, и центральные службы SWIFT)
Как	Сканирование с помощью автоматизированных инструментов (обновление профилей сканирования не менее, чем за месяц)	Тестирование опытным персоналом, независимым от команды, отвечающей за SWIFT (внутренняя Red Team или внешние ресурсы)

План

- [x] Обзор нормативных требований
- [ ] Методы атак
- [ ] Виды проведения пентеста
- [ ] Примеры успешно проведенных пентестов
- [ ] Описание результатов тестирования

Новости: регулярные утечки данных

СМИ: обнаружена утечка данных клиентов банка ВТБ



Сбербанк вычислил сотрудника, причастного к утечке пользовательских данных

Служба безопасности Сбербанка и правоохранительные органы закончили внутреннее расследование и обнаружили сотрудника, которы…

Банк UniCredit сообщил об утечке данных 3 000 000 клиентов

Утечка данных 3 млн пользователей произошла из-за компрометации всего одного файла. Проблема коснулась только клиентов UniCr…

Взлом Capital One привел к утечке данных 106 млн человек

Более 100 млн американцев и 6 млн канадцев пострадали в результате взлома компрометации Capital One. В руки третьих лиц попа…

Обнаружена утечка данных клиентов Альфа-банка, ОТП-банка и ХКФ-банка

Личные данные примерно 900 000 российских пользователей обнаружены в открытом доступе. Утечка включает данные о номере телеф…

Tesco Bank приостановил все онлайновые операции после компрометации 40 000 аккаунтов

В начале недели британский Tesco Bank подвергся кибератаке, в результате которой было похищено 2,5 млн фунтов.

Новости: взломы информационных систем

Индийский Cosmos Bank взломали, похищено более 13 000 000 долларов

Индийский Cosmos Bank взломали. Злоумышленники использовали клонированные карты для снятия наличных из банкоматов по всему м…

Десятки подозреваемых задержаны из-за массовых взломов банкоматов Santander

Преступные группы в трех американских штатах использовали баг в банкоматах банка Santander и обналичивали больше денег, чем …

Систему быстрых платежей использовали для кражи средств

В китайском налоговом ПО нашли еще один бэкдор

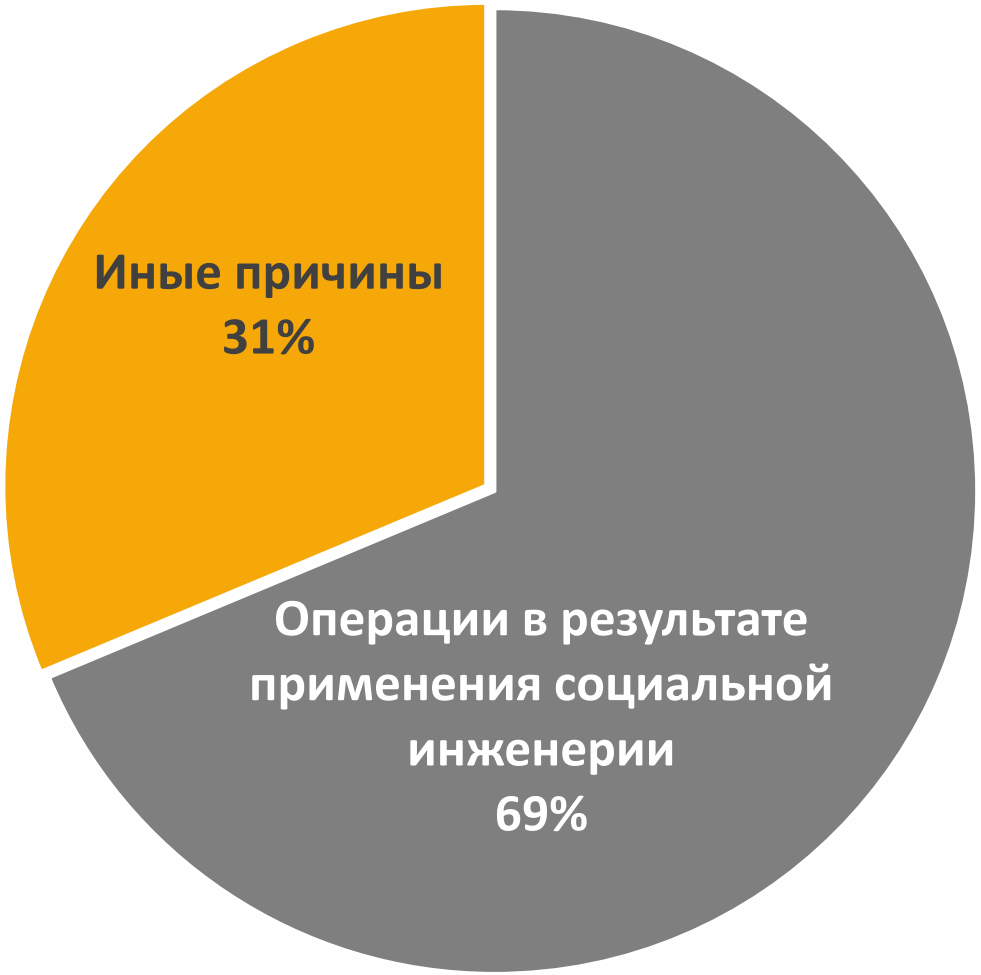
Совсем недавно специалисты Trustwave рассказывали о том, что неназванный китайский банк вынуждал западные компании устанавли…

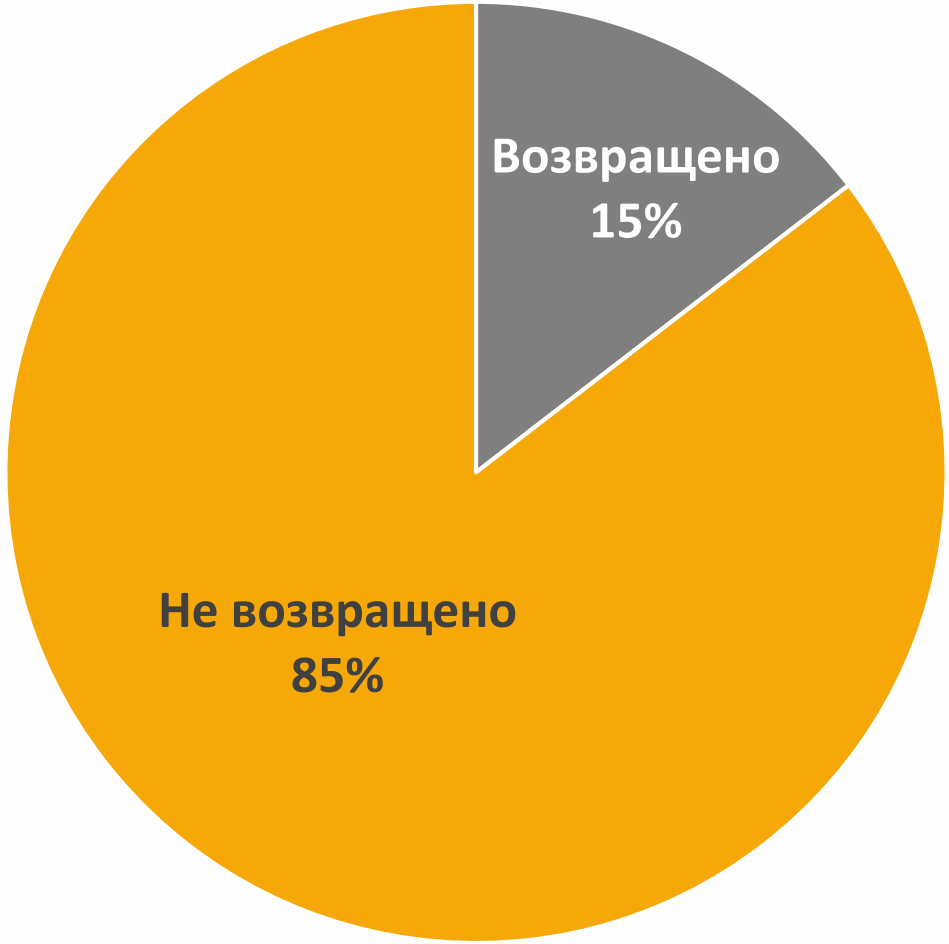
Статистика по инцидентам

БАНК РОССИИ
ФИНЦЕРТ

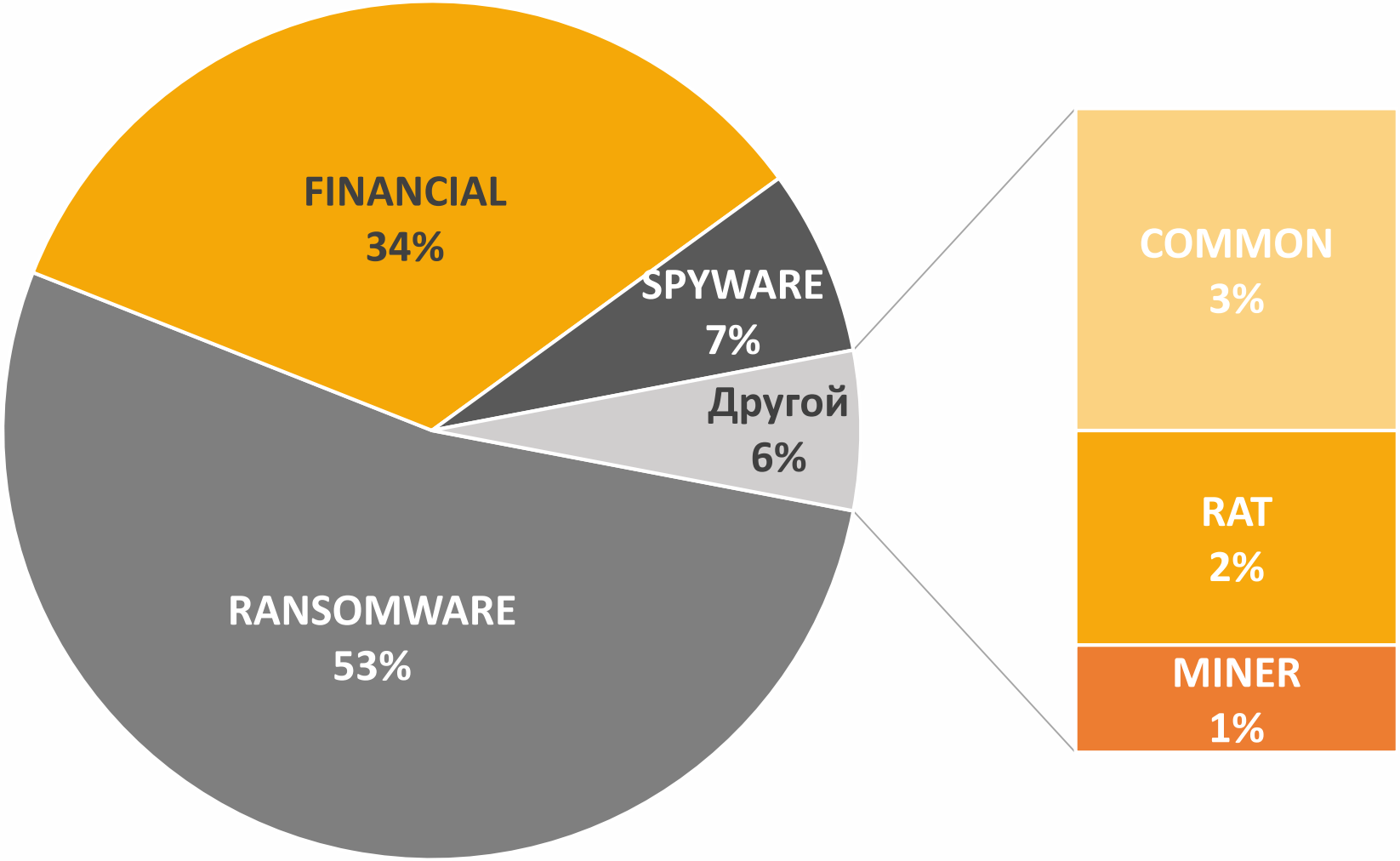
1. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год
2. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (1.09.2018 – 31.08.2019)
3. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году

Операции, совершенные без согласия клиентов

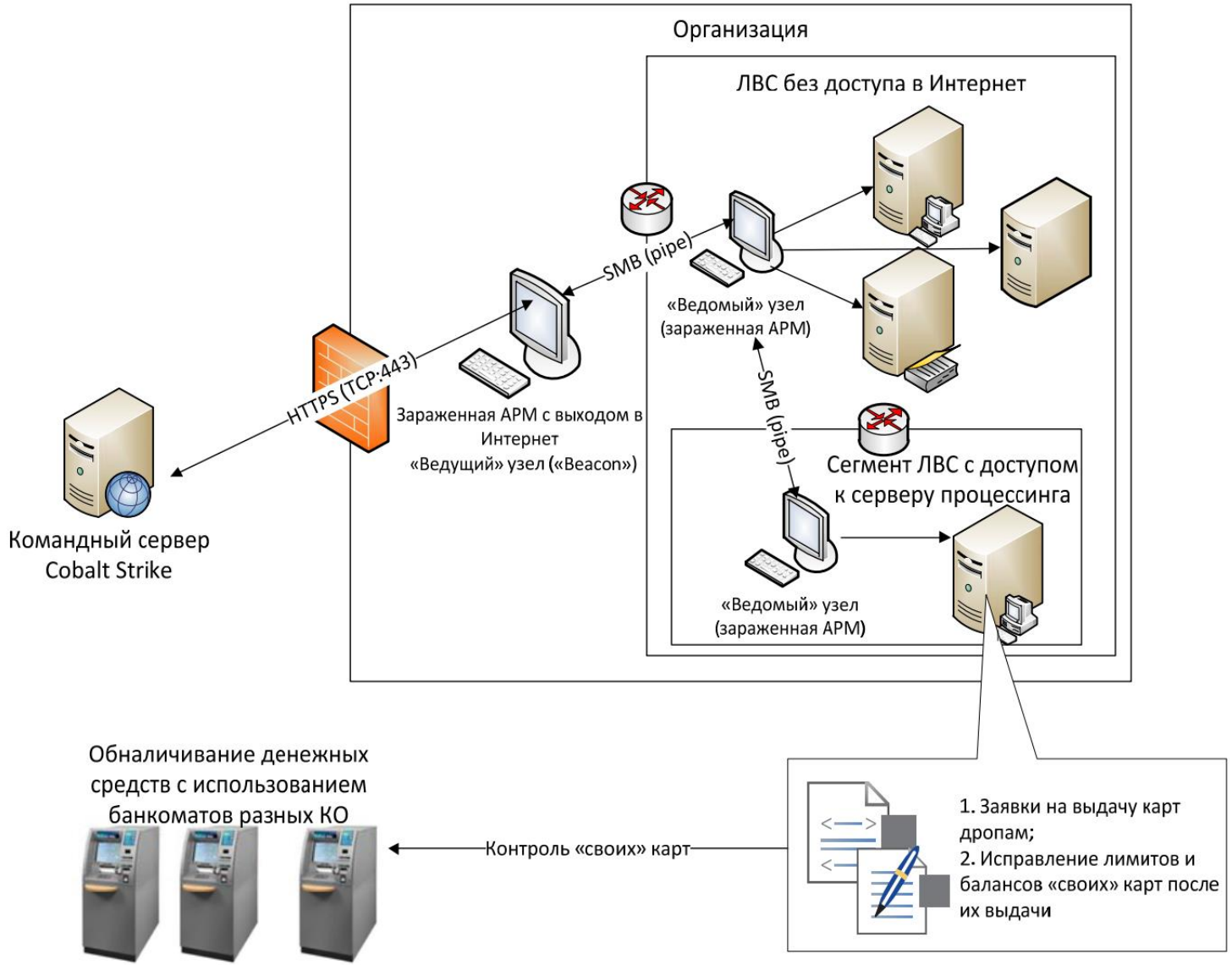




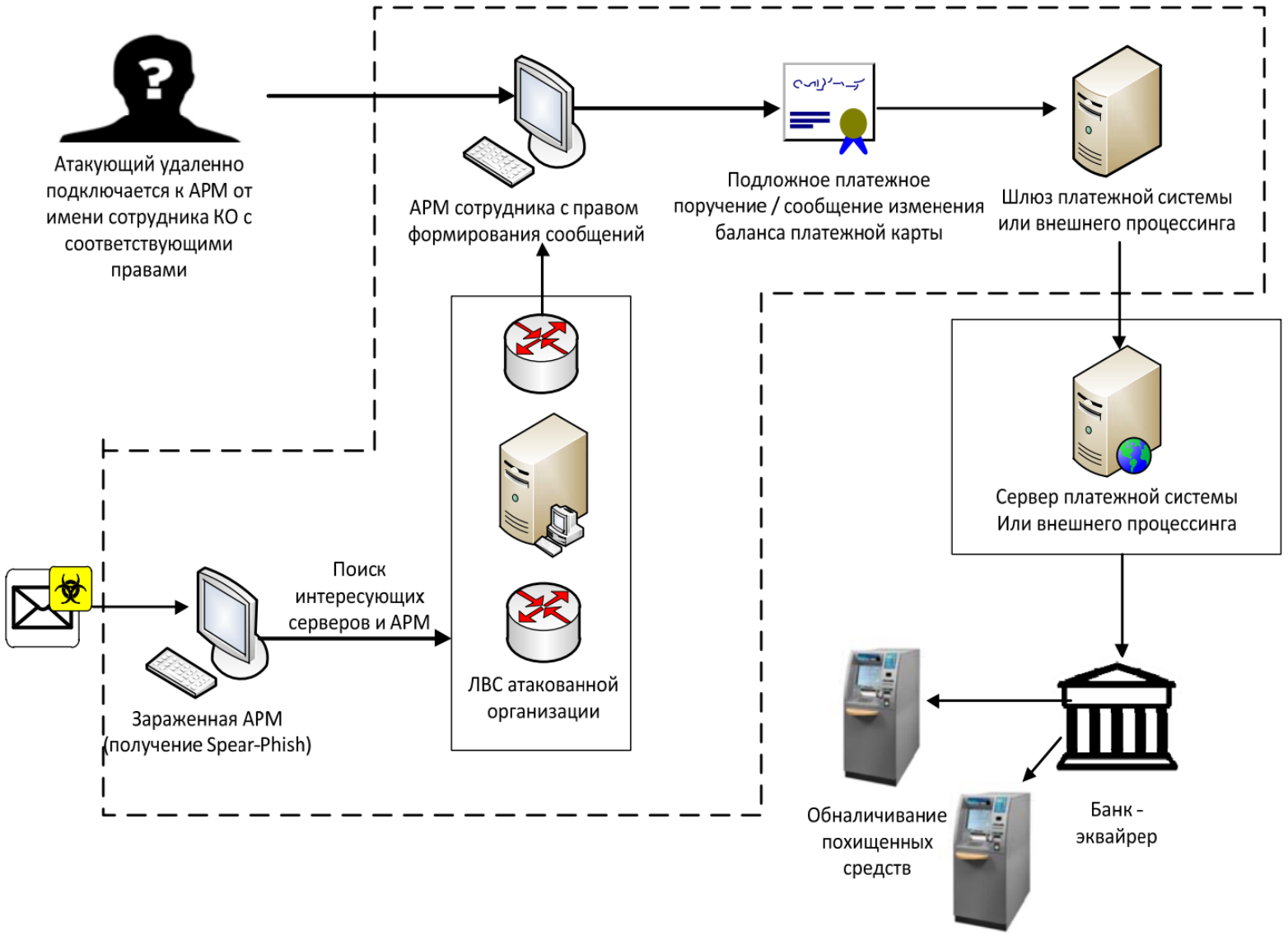
Атаки: распространение вредоносного ПО



Атаки: на инфраструктуру



Атаки: на инфраструктуру



Цели атак

USSC

Клиенты

Сотрудники

Инфраструктура

План

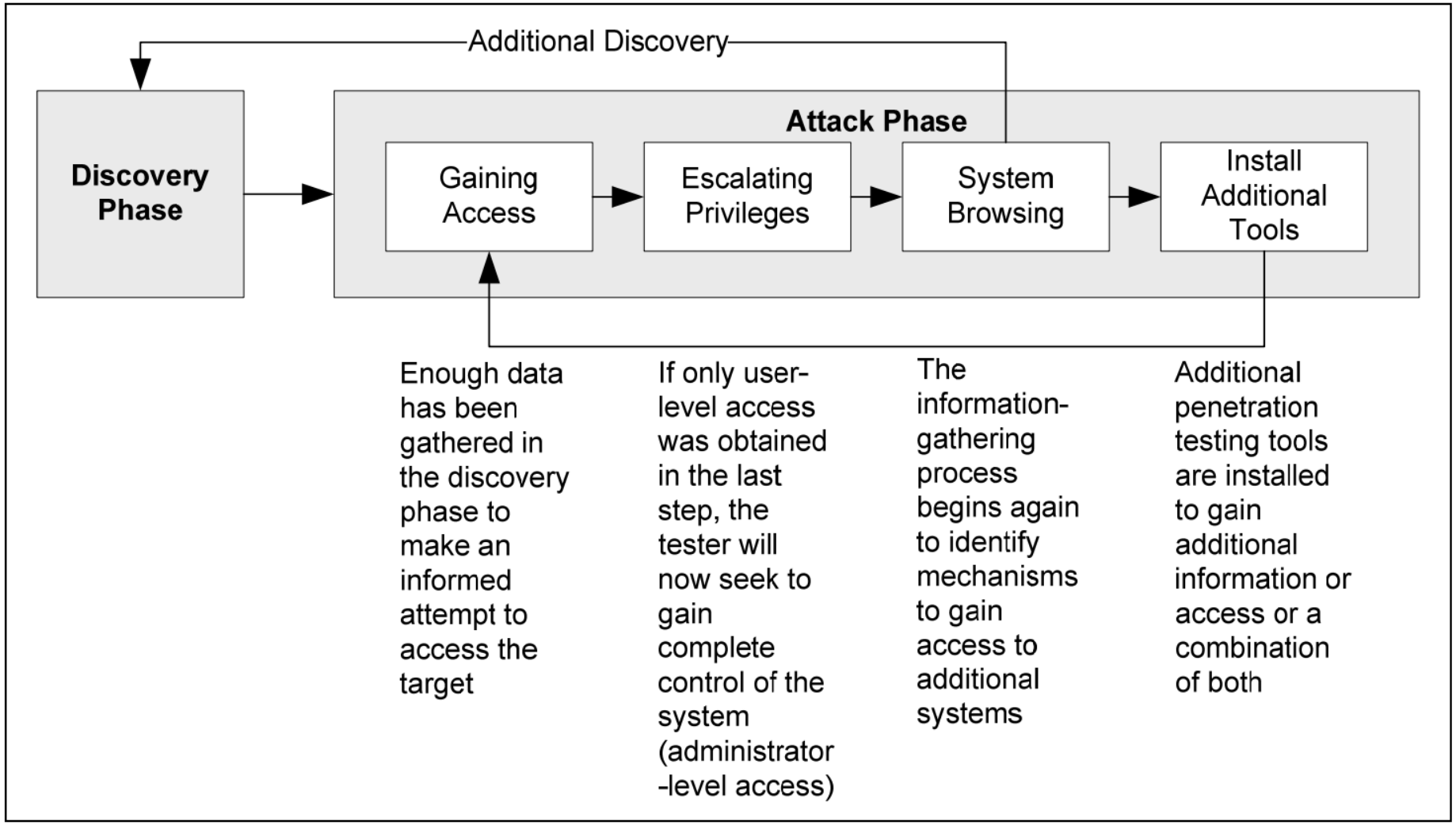
- [x] Обзор нормативных требований
- [x] Методы атак
- [ ] Виды проведения пентеста
- [ ] Примеры успешно проведенных пентестов
- [ ] Описание результатов тестирования

Анализ защищенности

USSC

1. Подготовительный этап
2. Сбор информации
3. Моделирование угроз
4. Поиск и анализ уязвимостей
5. Проведение атак
6. Исследование скомпрометированной системы
7. Составление отчета

NIST Special Publication 800-115



Доступные ресурсы

Внешние ресурсы:

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

Внутренние ресурсы:

- Беспроводные сети
- Корпоративная сеть
- Критичные ресурсы
- Инженерные сети

Человеческие ресурсы:

- Сотрудники
- Подрядчики
- Гости

★ Программные Продукты, Веб-сервисы

USSC

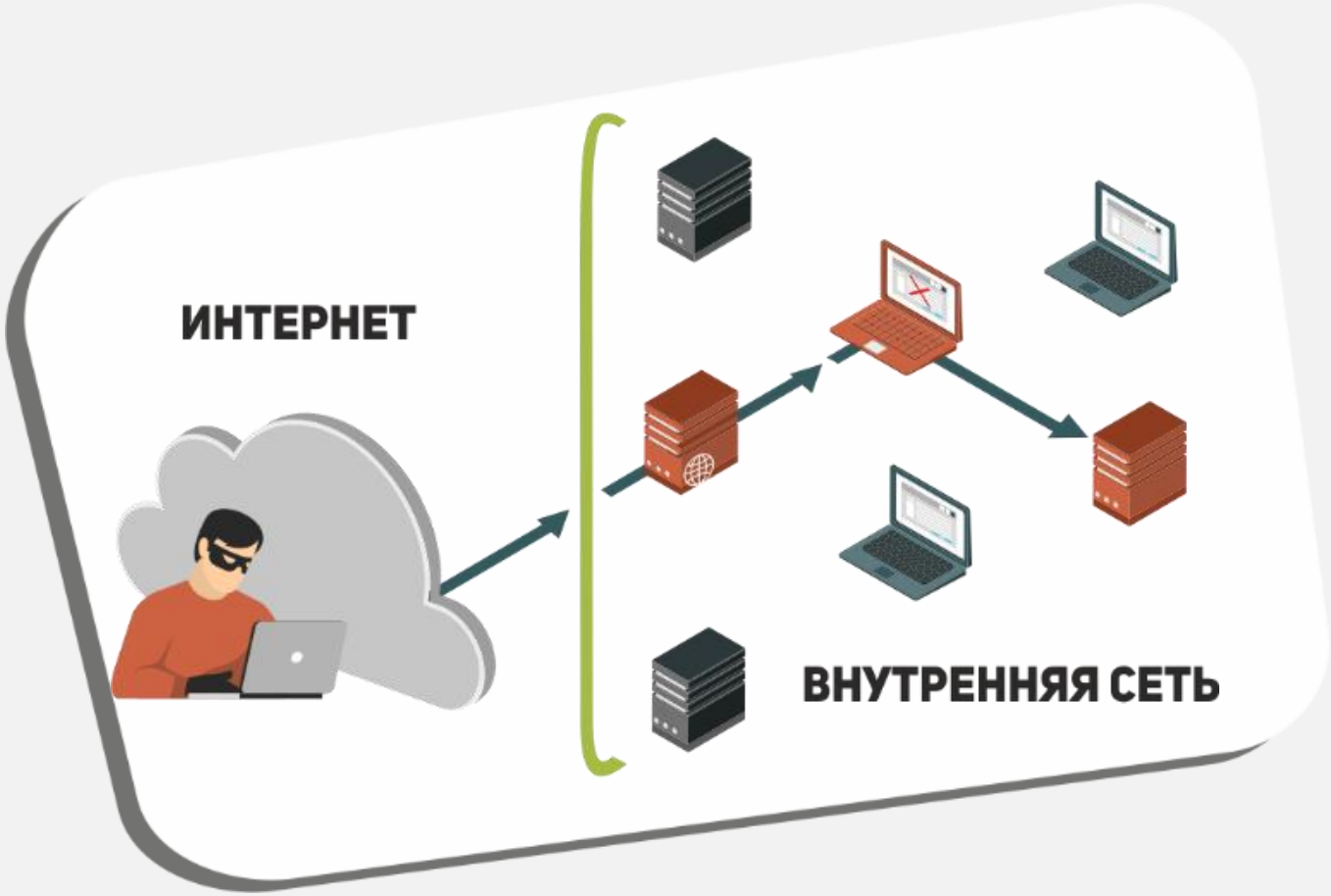
Анализ защищенности логического функционала веб-приложения

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

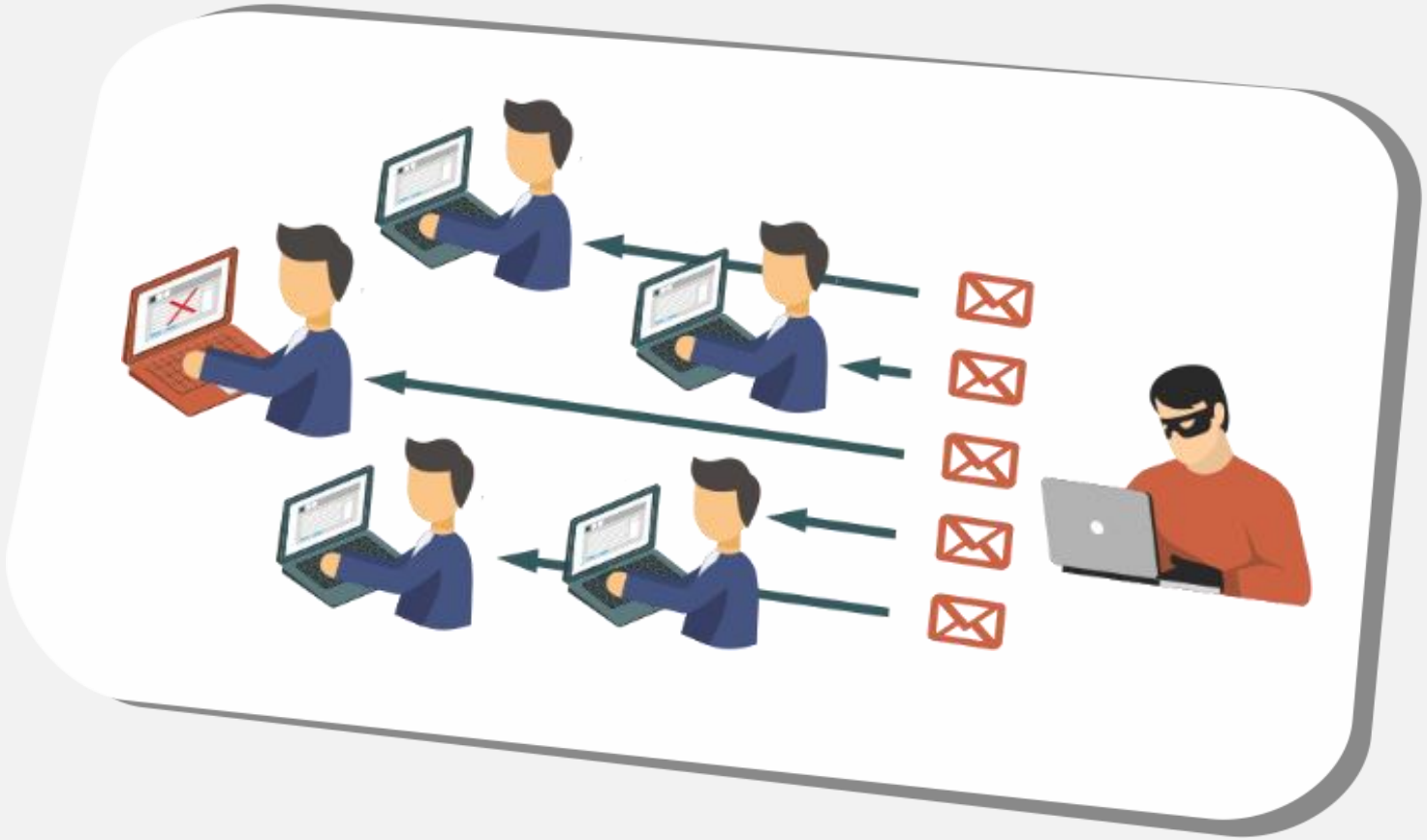
Анализ защищенности внешнего периметра

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)



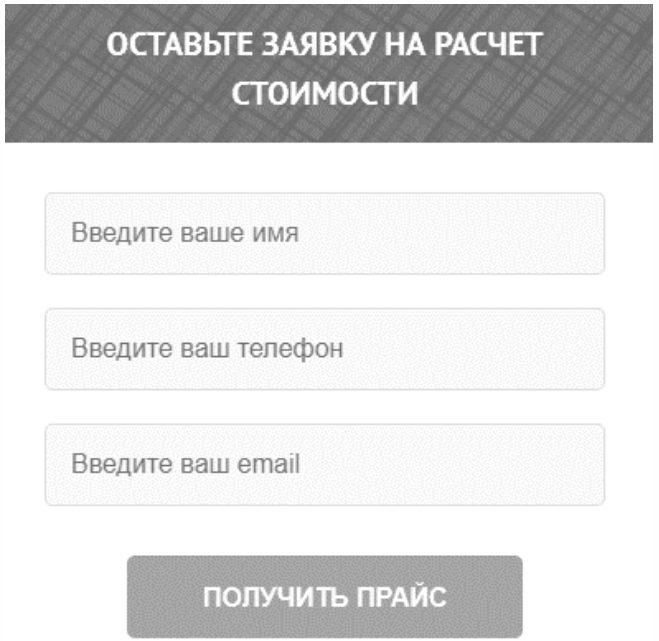
Тестирование методами социальной инженерии

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

Особенности

1. API-методы на отправку СМС-сообщений

2. Формы отправки заявок



План

- [x] Обзор нормативных требований
- [x] Методы атак
- [x] Виды проведения пентеста
- [ ] Примеры успешно проведенных пентестов
- [ ] Описание результатов тестирования

Уязвимости в распространяемом софте

USSC

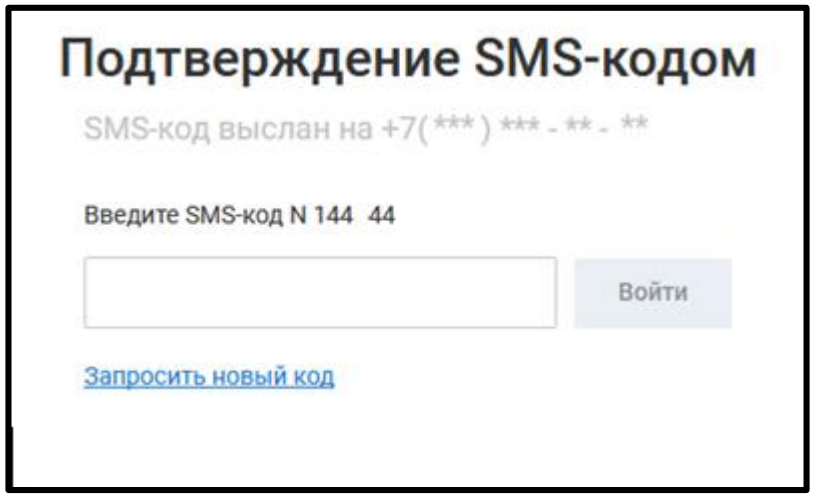
```
512     </function>
513     <function name="GetDriversListByType" type="function" declaration="function
        GetDriversListByType(DrvType : integer) : string;">
514       <param name="DrvType">Тип устройства. Варианты: DRIVE_UNKNOWN = 0;
          DRIVE_NO_ROOT_DIR = 1; DRIVE_REMOVABLE = 2; DRIVE_FIXED = 3; DRIVE_REMOTE = 4;
          DRIVE_CDROM = 5; DRIVE_RAMDISK = 6;</param>
515       <description><abstract>Список дисков по типу, разделённых запятой. Например:
          C,D,G</abstract><detailed> Только для Windows! Для остальных ОС вернет пустую
          строку </detailed></description>
516     </function>
517     <function name="ShellPrint" type="function" declaration="function
        ShellPrint(const FileName : string) : integer;">
518     </function>
519     <function name="ShellExecute" type="function" declaration="function
        ShellExecute(const Operation, FileName, Parameters, Directory : string; ShowCmd:
        Integer) : integer;">
520     </function>
521     <property name="LastFileName" indexdecl="" type="string" reader="" writer=""
        default="0" defaultid="" nodefault="0" storedid="">
522       <description><detailed>Последний файл, с которым работал данный объект
          Используется в функциях: SelectFile ReadMimeFileData
          WriteMimeFileData</detailed></description>
```

Response Headers view parsed

```
HTTP/1.0 200
Access-Control-Allow-Origin: *
Content-Type: text/html
Content-length: 107
Connection: close
Date: Thu, 10 Nov 2016 12:24:12 +0500
```

USSC.RU

Обход одноразовых паролей

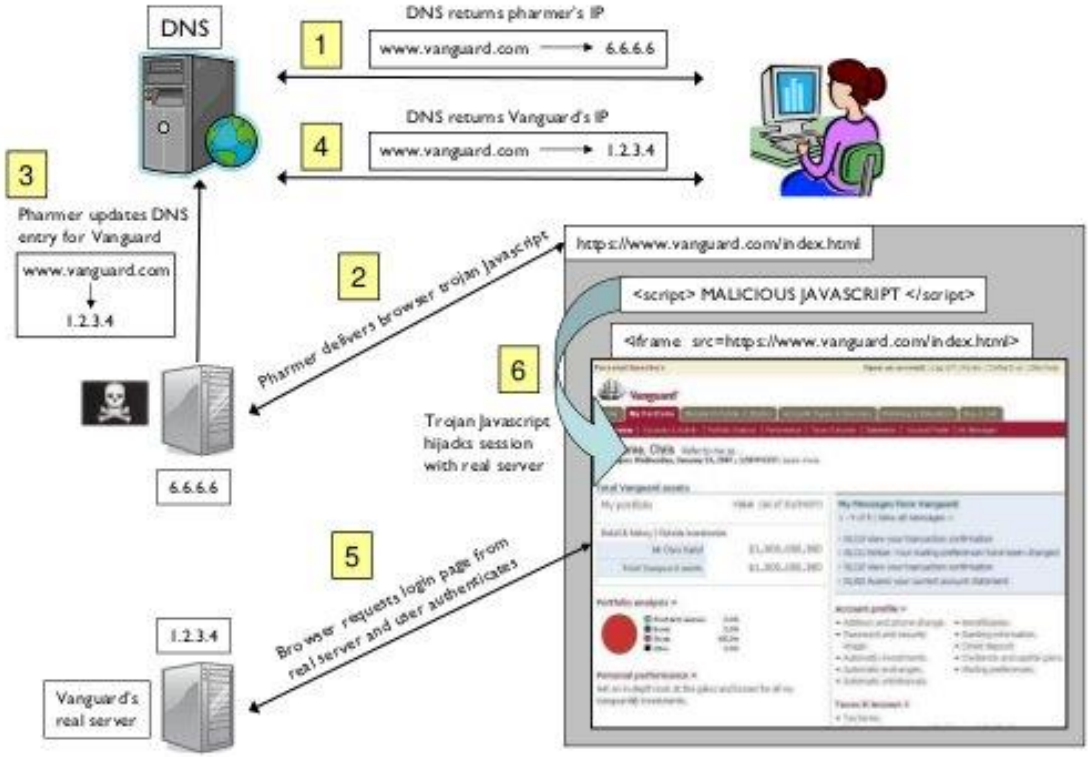


$$p = 1 - \frac{3}{10\,000}$$

$$p_k = p^k$$

k	1-P(k)
900	0.2367
1800	0.4173
3600	0.6605
7200	0.8847

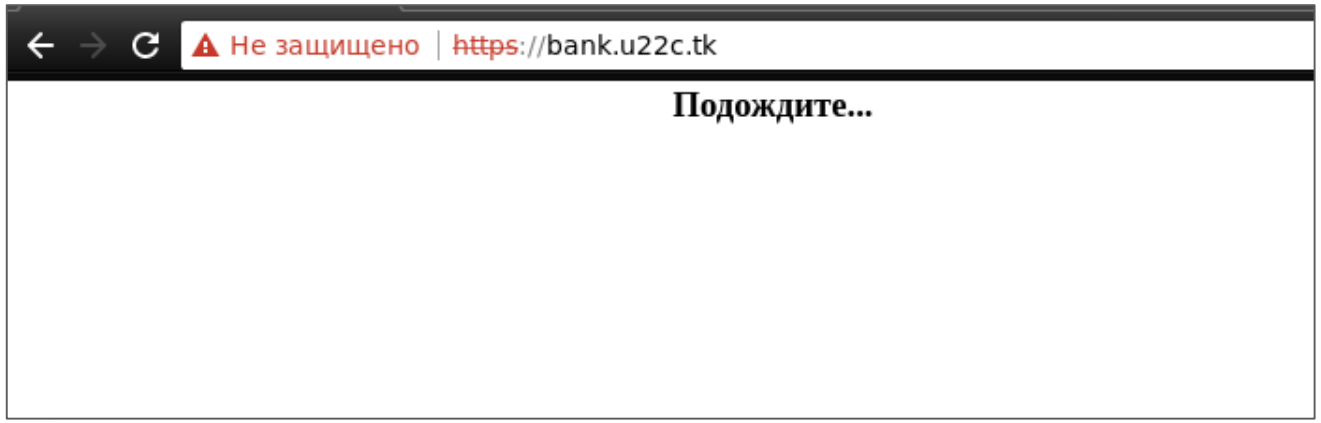
Перехват данных




```
;; QUESTION SECTION:
;bank.u22c.tk.                  IN      A

;; ANSWER SECTION:
bank.u22c.tk.           58      IN      A       127.0.0.1
bank.u22c.tk.           58      IN      A       [redacted]

;; Query time: 98 msec
```



План

- [x] Обзор нормативных требований
- [x] Методы атак
- [x] Виды проведения пентеста
- [x] Примеры успешно проведенных пентестов
- [ ] Описание результатов тестирования

Оформление результатов пентеста

1. Методика проведения тестирования:

- ✓ описание потенциала нарушителя
- ✓ порядок проведения тестирования (основные этапы)
- ✓ описание используемых инструментов (специального ПО)

2. Описание исследуемой инфраструктуры:

- ✓ описание сетевой инфраструктуры (сетевых узлов)
- ✓ описание исследуемых ПО и приложений
- ✓ и т.д.

3. Описание результатов тестирования:

- ✓ перечень актуальных уязвимостей
- ✓ результаты эксплуатации актуальных уязвимостей

4. Рекомендации по устранению актуальных уязвимостей

Наши предложения для финансовых организаций

USSC

Оценка соответствия требованиям ГОСТ Р 57580

Тестирование на проникновение

Анализ уязвимостей по ОУД

Онлайн-сервис дистанционной оценки соответствия ГОСТ Р 57580

Комплексные аудиты

Предварительный аудит и приведение в соответствие с требованиями регуляторов

О компании

Опыт

Специалисты компании УЦСБ свободно владеют различными методиками сетевых атак и имеют богатый опыт реализации мероприятий по анализу защищенности

Сертификации

Проектная команда - сотрудники с высшим профессиональным образованием по направлению подготовки 090100 «Информационная безопасность», имеющие сертификаты:

- Certified Information System Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Computer Hacking Forensic Investigator (CHFI)
- Offensive Security Certified Expert (OSCE)

О компании

Уральский центр систем безопасности (УЦСБ) – компания-эксперт в области безопасного использования информационных технологий. С 2007 года компания непрерывно развивается, наращивает компетенции и выполняет все более сложные проекты.

Компетенции

- **Информационные технологии**
- **Комплексы инженерно-технических средств охраны**
- **Анализ защищенности**
- **Сервисное обслуживание**
- **Информационная безопасность**
- **Информационные инфраструктуры**
- **Безопасность промышленных систем автоматизации и управления**

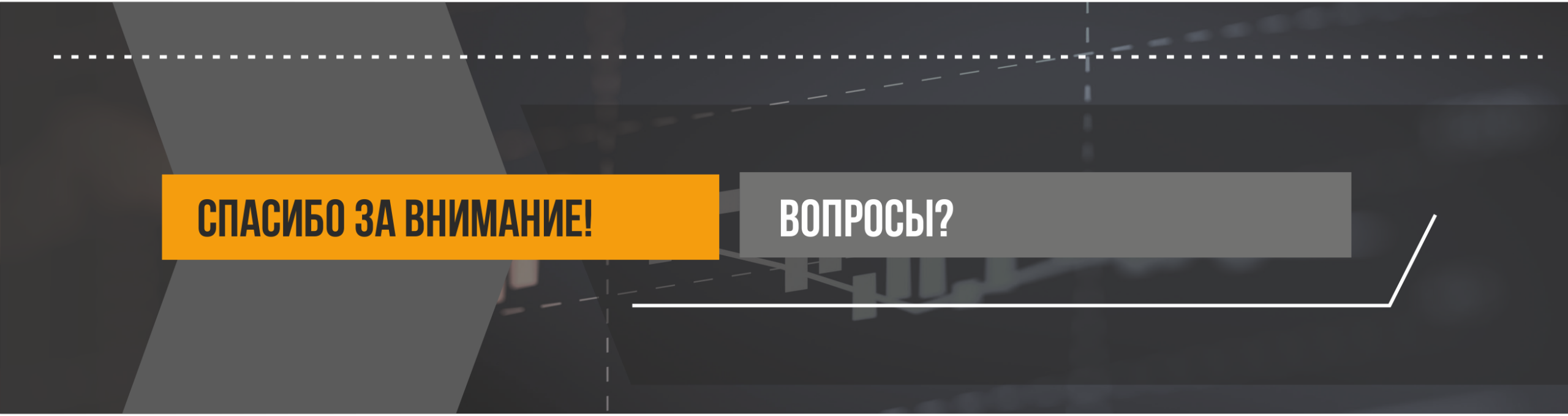
USSC.RU

620100, г. Екатеринбург, ул. Ткачей, д. 6
620100, г. Екатеринбург, ул. Ткачей, д. 23

Тел.: +7 (343) 379-98-34,
e-mail: info@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

USSC



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Борисов Сергей

Обособленное подразделение в г. Краснодар

sborisov@ussc.ru

Краснов Сергей

Аналитический центр

skrasnov@ussc.ru

Пермякова Татьяна

Аналитический центр

tpermyakova@ussc.ru