infotecs

Ландшафт требований по защите информации для финансовых организаций

Владимир Голованов

Становление методологии регулирования. «Разминка»

С 2000 по 2014: стандарты и рекомендации Центрального банка РФ по информационной безопасности (http://www.cbr.ru/credit/Gubzi_docs/stnd/ , http://www.cbr.ru/credit/Gubzi_docs/met/):

- СТО БР ИББС-1.0-2014,Стандарт Банка России: «Обеспечение ИБ организаций БС РФ. Общие положения» (6-ая редакция, с 2004 г.);
- СТО БР ИББС-1.1-2007, Стандарт Банка России: «Обеспечение ИБ организаций БС РФ. Аудит информационной безопасности СТО БР ИББС-1.1-2007»;
- РС БР ИББС-2.0-2007, Рекомендации в области стандартизации Банка России «Обеспечение ИБ организаций БС РФ. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».

Статус: Добровольное применение

Основа: ISO/IEC 27001/27002; ISO/IEC TR 18044; NIST SP 800-30; практики of KPMG, PWC, E&Y; guides of UKAS (British); практики организаций БС РФ и Банка России.

Фундаментальные точки эволюции

2011 год: принятие Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», включающего статью 27 «Обеспечение защиты информации в платежной системе» - прецедент права введения Банком России обязательных требований по ЗИ для финансового сектора. (Положение Банка России № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»).

2018 год: Указанием Банка России от 7 мая 2018 г. № 4793-У внесены изменения в Положение Банка России от 9 июня 2012 г. № 382-П, определившие начало фундаментальных новаций в «ландшафте» требований ЗИ.

Федеральный закон от 27.06.2011 года № 161-ФЗ «О национальной платежной системе»

Требования № 161-ФЗ, Статья 27. Обеспечение защиты информации в платежной системе:

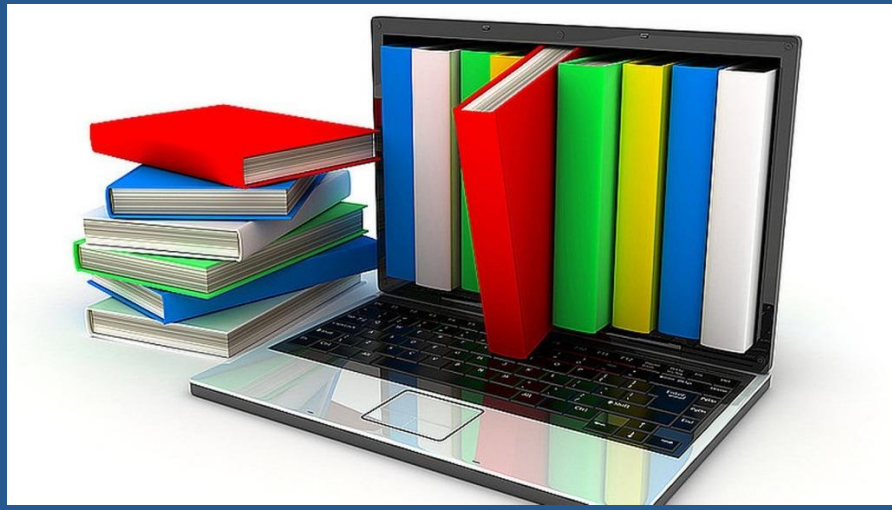
1. ОПДС, банковские платежные агенты (субагенты), операторы услуг информационного обмена ….. *обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных* ….Правительство Российской Федерации устанавливает требования к защите указанной информации. (**ПП-583**);

2. Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются ……..и без права ознакомления с защищаемой информацией. (**ФСБ и ФСТЭК**);

3. ОПДС, банковские платежные агенты (субагенты), операторы услуг информационного обмена, *поставщики платежных приложений*, ……. обязаны *обеспечивать защиту информации при осуществлении ПДС в соответствии с требованиями, установленными Банком России*, согласованными с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи. Контроль …… осуществляется Банком России в рамках надзора в НПС в установленном им порядке, согласованном с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи. (**ЦБ РФ, 382-П, 2831-У**).

Практика регулирования по 382-П. Как это работало

- «Традиционный» банковский надзор имел затруднения с контролем исполнения «технических» требований Положения 382-П (*квалификация*: бухгалтеры, экономисты);
- Ряд норм (самооценка и пр.) «не работали» как ожидалось. Не был учтен фактор конфликта интересов;
- Ситуация с хищениями денежных средств продолжала ухудшаться как вследствие отсутствия прогресса с защищённостью, так и ухудшения ситуации с качеством платежных приложений;
- Требовалось внесение изменений в концепцию обязательных требований по ЗИ.



Факторы, способствующие внесению принципиальных изменений

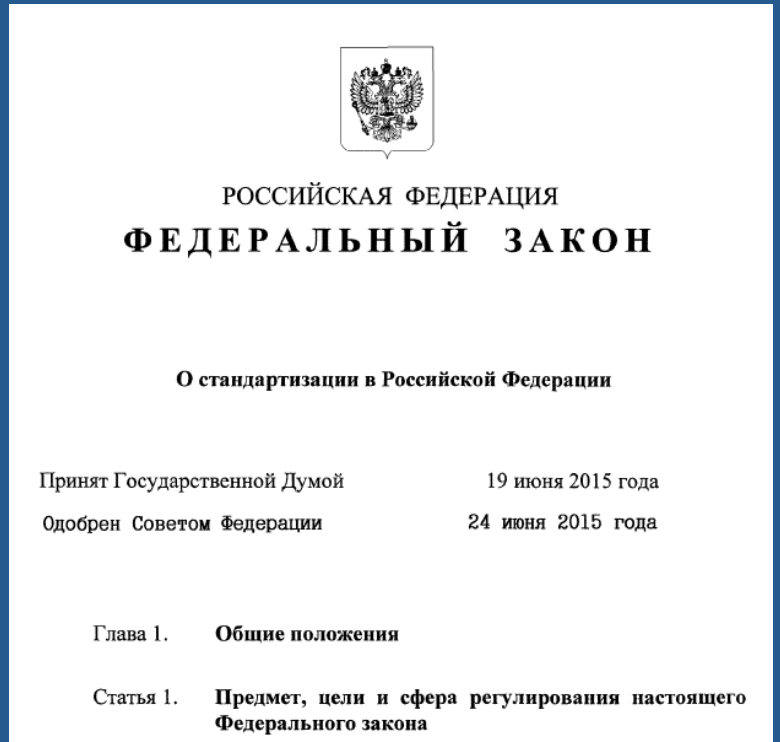
2015 год, ФЗ «О стандартизации в РФ»

Статья 27. Применение ссылок на национальные стандарты и информационно-технические справочники в нормативных правовых актах

1. Нормативные правовые акты могут содержать ссылки на официально опубликованные национальные стандарты……..

2. Применение ссылок на национальные стандарты и ……. в нормативных правовых актах допускается в целях обеспечения выполнения технических и функциональных требований нормативного правового акта ……

3. Ссылки на национальные стандарты в нормативных правовых актах применяются путем приведения в них наименования и обозначения национальных стандартов с указанием ….



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О стандартизации в Российской Федерации

Принят Государственной Думой 19 июня 2015 года

Одобрен Советом Федерации 24 июня 2015 года

Глава 1. **Общие положения**

Статья 1. **Предмет, цели и сфера регулирования настоящего Федерального закона**

2016 год. План мероприятий («дорожная карта») по реализации мер, направленных на предотвращение хищений денежных средств

Основными элементами «дорожной карты» являются:

- *совершенствование законодательства РФ* в части наделения Банка России правом по регулированию и контролю обеспечения ИБ в организациях кредитно-финансовой сферы;
- разработка и *ввод в действие национальных стандартов* РФ, *устанавливающих технические требования к обеспечению ИБ* организаций кредитно-финансовой сферы (далее – национальные стандарты ИБ) и определяющие методики оценки соответствия ИБ техническим требованиям национальных стандартов ИБ (далее – нац. стандарты оценки ИБ);
- *создание системы оценки соответствия ИБ* организаций кредитно-финансовой сферы требованиям национальных стандартов ИБ;
- *совершенствование нормативной базы Банка России* в части определения организационных и правовых основ по обязательному применению национальных стандартов ИБ в организациях кредитно-финансовой сферы …..;
- ……..

Реализация «Дорожной карты». Внесены изменения в три федеральных закона

27 июня 2018 года N 167-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О ВНЕСЕНИИ ИЗМЕНЕНИЙ
В ОТДЕЛЬНЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
В ЧАСТИ ПРОТИВОДЕЙСТВИЯ ХИЩЕНИЮ ДЕНЕЖНЫХ СРЕДСТВ

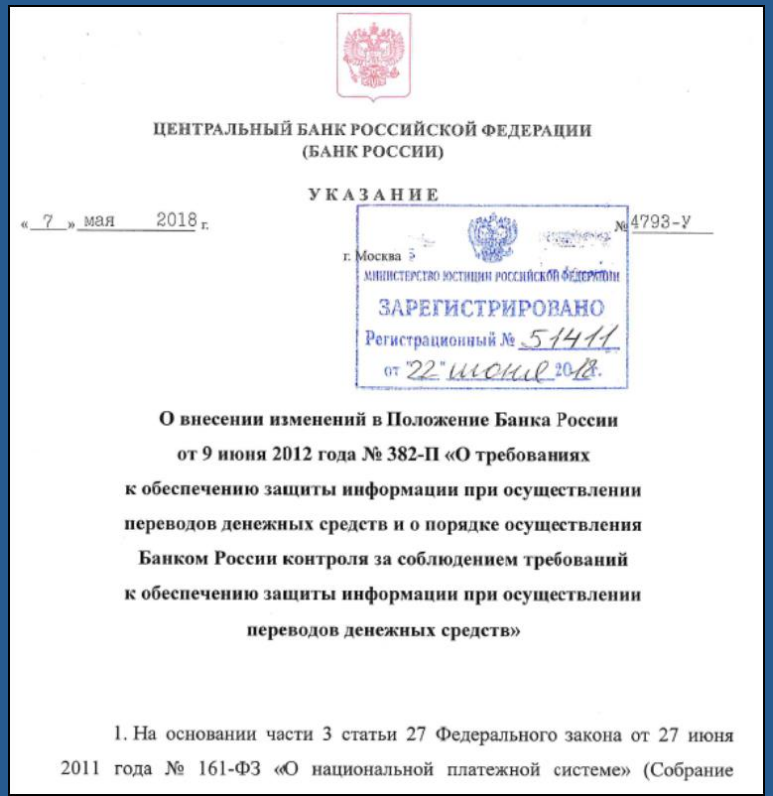
Принят
Государственной Думой
5 июня 2018 года

Одобрен
Советом Федерации
20 июня 2018 года

Статья 1

Внести в статью 26 Федерального закона "О банках и банковской деятельности" (в редакции Федерального закона от 3 февраля 1996 года N 17-ФЗ) (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, N 27, ст. 357; Собрание законодательства Российской

Реализация «Дорожной карты». Нормативная база, стандарты



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

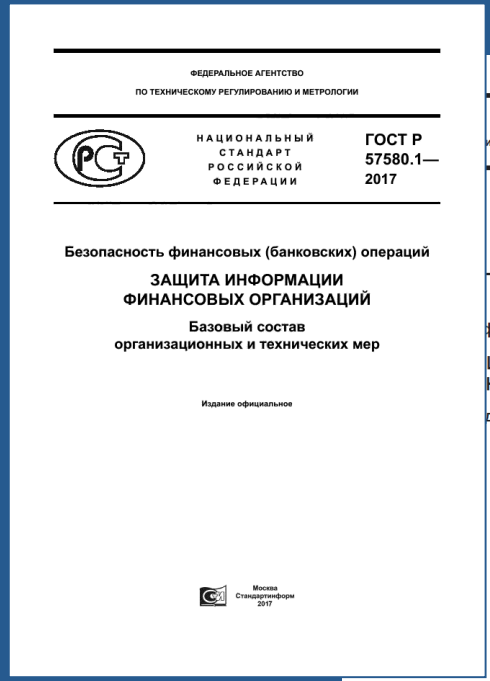
«7» мая 2018 г. № 4793-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 51411
от "22" июня 2018 г.

О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

1. На основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.1—2017

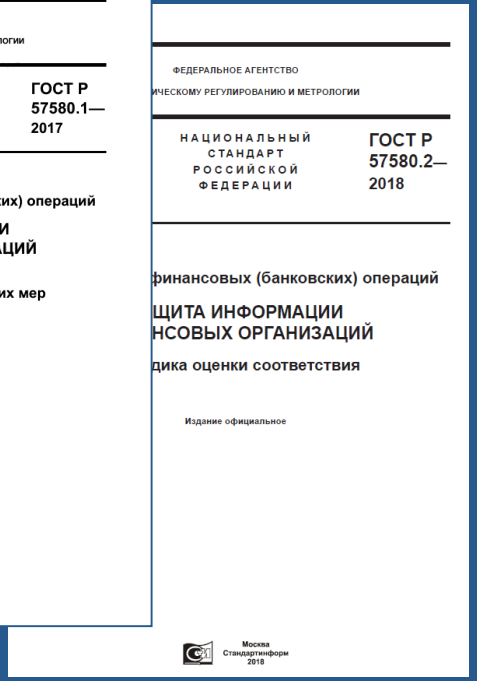
Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

Издание официальное

Москва Стандартинформ 2017



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.2—2018

финансовых (банковских) операций

ЩИТА ИНФОРМАЦИИ
НСОВЫХ ОРГАНИЗАЦИЙ

дика оценки соответствия

Издание официальное

Москва Стандартинформ 2018

Реализация «Дорожной карты». Нормативная база *(продолжение)*



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

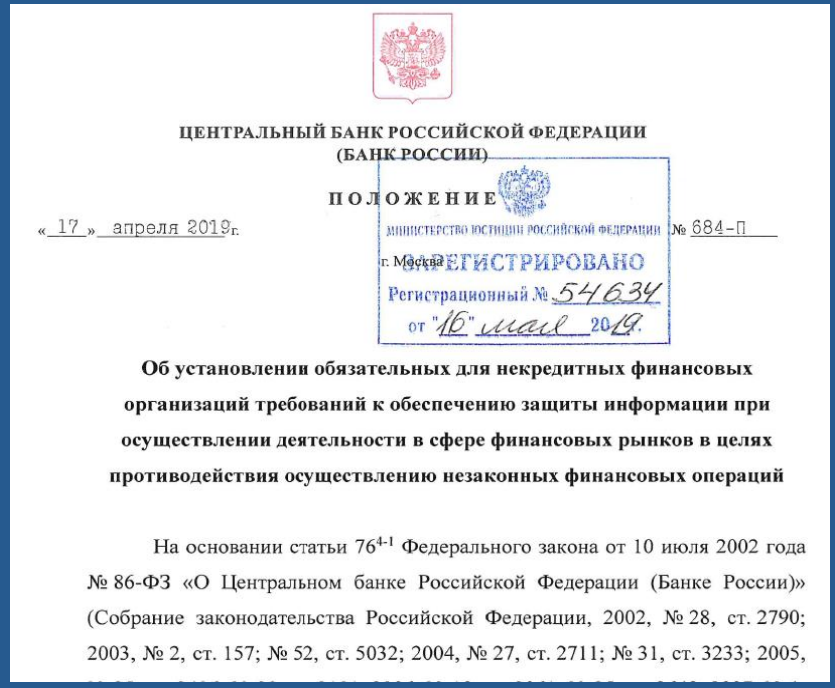
П О Л О Ж Е Н И Е

«17» апреля 2019 г. № 683-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54637
от "16" мая 2019.

Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«17» апреля 2019 г. № 684-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54634
от "16" мая 2019.

Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций

На основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005,

Эволюция требований Банка России. Комментарии Банка России



А.О. Выборнов,
зам. Директора
ДИБ ЦБ

Эволюция требований Банка России. Комментарии Банка России *(продолжение)*



А.О. Выборнов,
зам. Директора
ДИБ ЦБ

Что далее? Подключайтесь

РЕШЕНИЕ

заседания Подкомитета № 1 «Безопасность финансовых (банковских) операций» Технического комитета № 122 «Стандарты финансовых операций» (16 октября 2019 года)

1) Поддержать предложения Банка России о включении в Программу национальной стандартизации на 2020 год разработку следующих национальных стандартов:

- Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз. Общие положения (Шифр темы ПНС 1.9.122-1.004.20);
- Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз. Методика оценки соответствия (Шифр темы ПНС 1.9.122-1.005.20);
- Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Общие положения (Шифр темы ПНС 1.9.122-1.003.20);
- Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Методика оценки соответствия (Шифр темы ПНС 1.9.122-1.002.20).



Совершенствование надзора. Магнитогорский форум



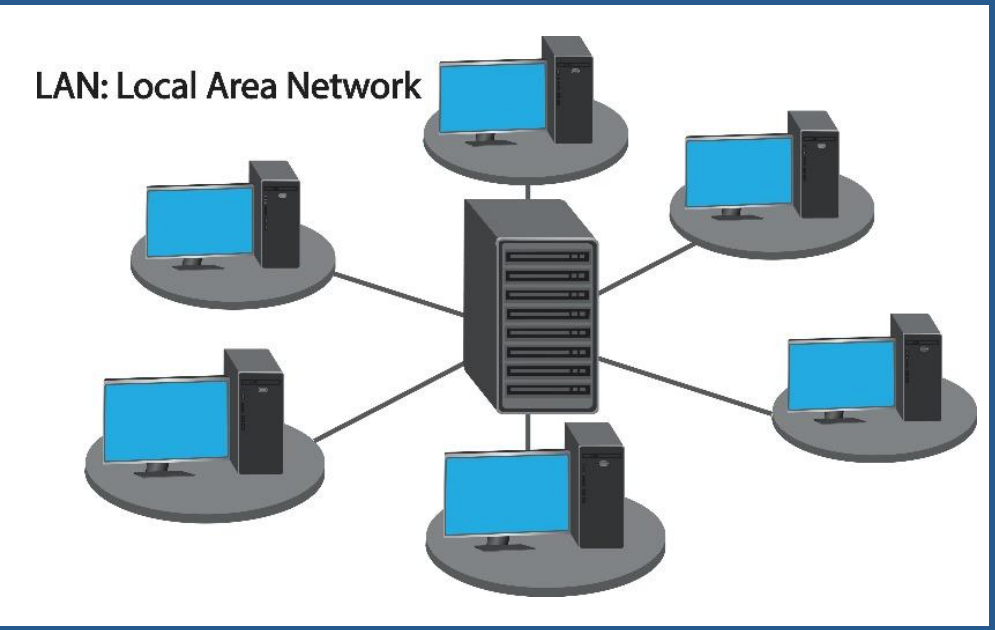
А.Б. Дудка,
начальник отдела проверок
ФинЦЕРТ ДИБ ЦБ

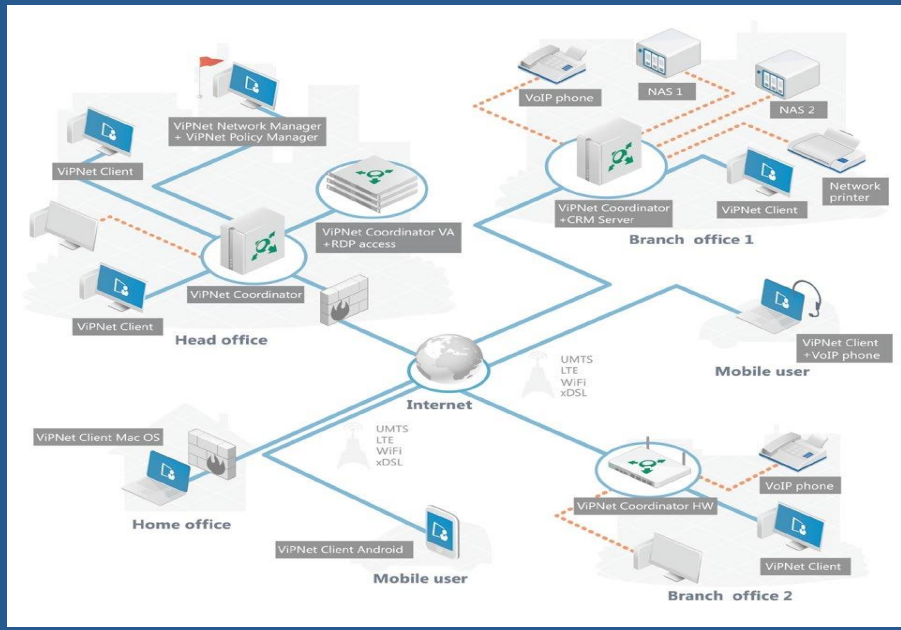
infotecs

Спасибо
за внимание!

Обеспечение безопасной удаленной работы сотрудников финансовых организаций в соответствии с рекомендациями Банка России

Изменение парадигмы информационного взаимодействия





Информационное письмо Банка России

- Защита удаленного мобильного доступа
- Бесперебойное выполнение чувствительных операций
- Использование автоматизированной системы обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (АСОИ ФинЦЕРТ)
- Регуляторные послабления Банка России



ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел. (499) 300-30-00

Кредитным организациям, некредитным финансовым организациям

От 20.03.2020 № ИН-014-56/17

на от

Информационное письмо о мерах по обеспечению киберустойчивости и информационной безопасности в условиях распространения новой коронавирусной инфекции (COVID-19)

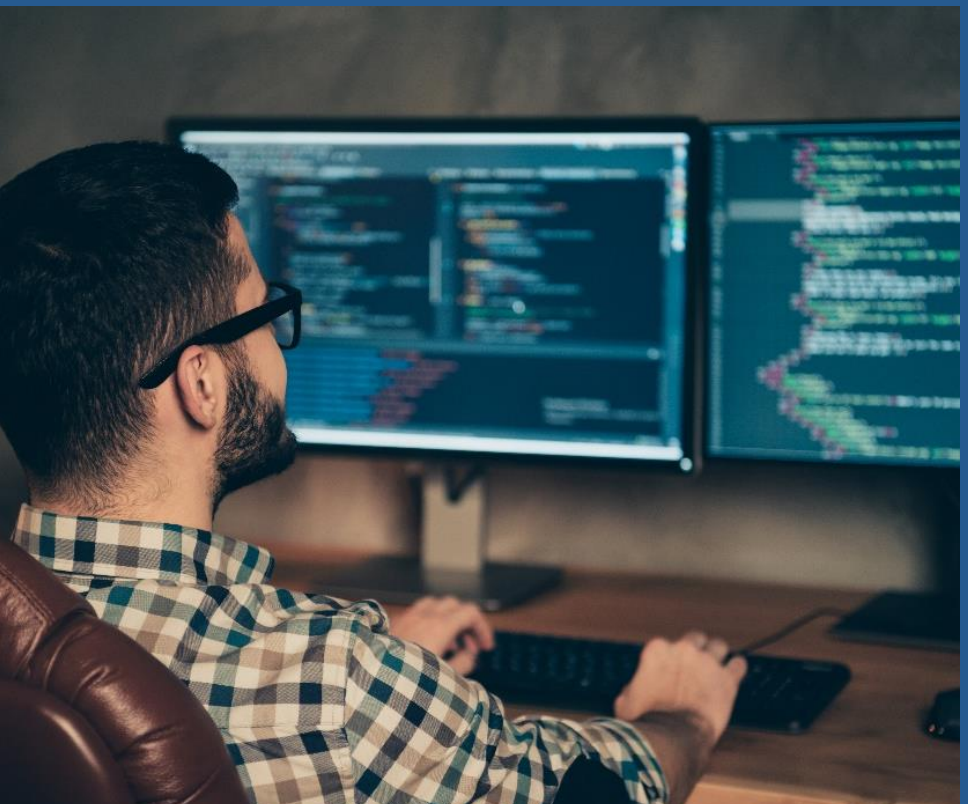
Защита удаленного мобильного доступа

- Применение технологий виртуальных частных сетей
- Применение многофакторной аутентификации
- Применение терминального доступа
- Мониторинг и контроль действий пользователей удаленного мобильного доступа

Сопутствующие организационные и технические меры – в соответствии с ГОСТ Р 57580.1-2017



Бесперебойное осуществление чувствительных операций



- Идентификация работников, задействованных в чувствительных операциях
- Организация режима работы, обеспечивающего минимизацию рисков нарушения бесперебойности чувствительных операций
- Выделение групп работников, поддерживающих и ожидающих привлечения к обеспечению бесперебойного режима работы выполнения чувствительных операций

Использование АСОИ ФинЦЕРТ

- Оперативное информационное взаимодействие с Банком России посредством автоматизированной системы обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (АСОИ ФинЦЕРТ)



Регуляторные послабления Банка России

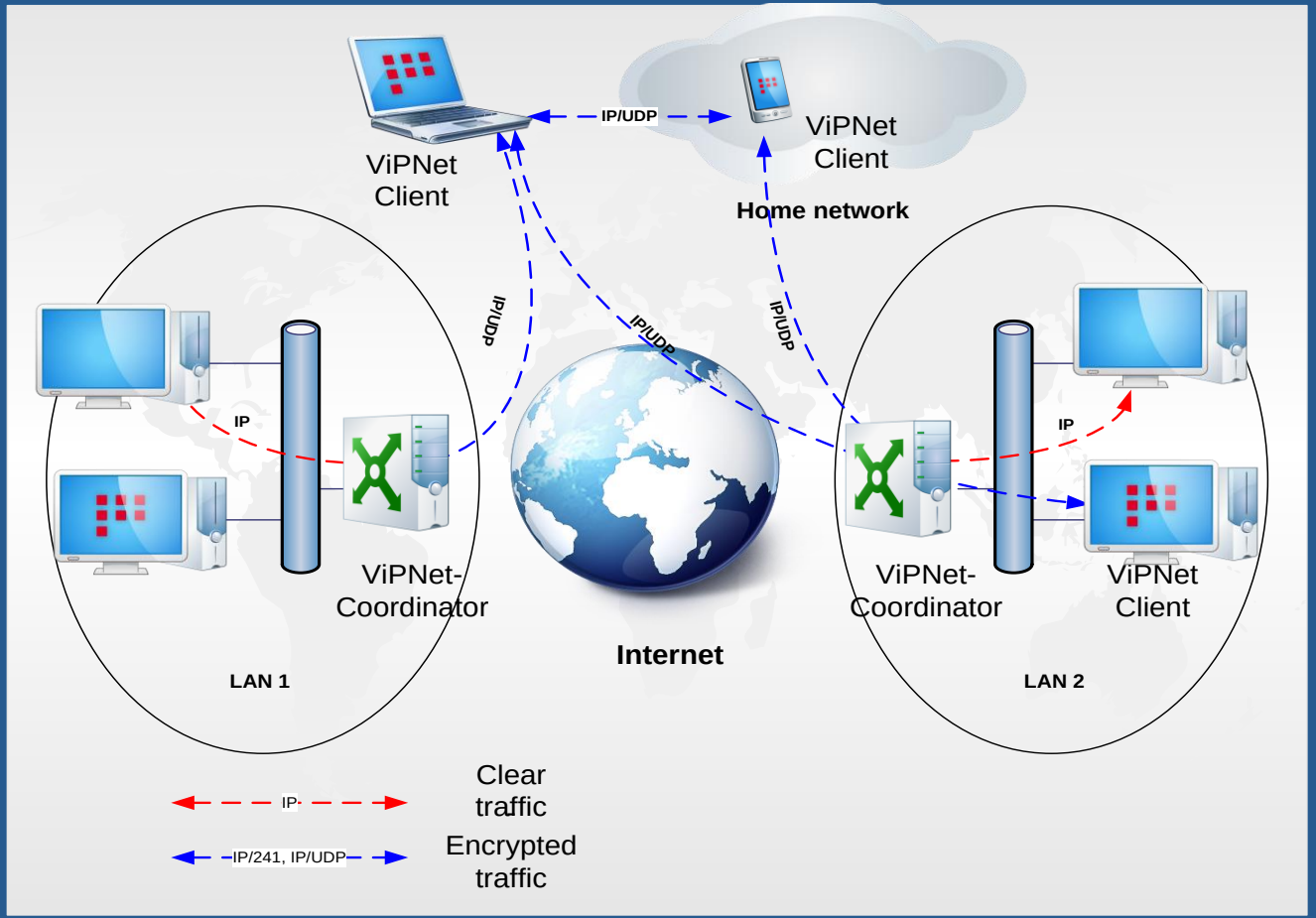
- Банк России воздерживается от применения мер, предусмотренных статьями 74, 76.5 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» в отношении финансовых организаций, допустивших нарушение требований



Подходы


Подходы
Домашний компьютер
Корпоративный ноутбук
Zero Trust
VPN
Минимум доступа
Управление политиками
EndPoint Security
Peer to Peer

Удаленный доступ



Защита периметра

- Межсетевой экран
- Stateful Packet Inspection
- NAT, Antispoofing
- Application Layer Gateway
- Proxy-server

- VPN Шлюз
- L3 VPN
- L2VPN (L2OverIP)
- Traversal NAT



- Сетевые сервисы
- DNS server
- NTP-server
- DHCP-server
- DHCP-Relay
- VLAN, QoS support

- Транспортный сервер
- Горячий резерв (failover)

ViPNet Client на каждом рабочем месте

- VPN-клиент для работы в защищенных сетях ViPNet
- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Поддерживает ОС Windows, Linux, MacOS, Android, iOS, Sailfish
- Имеет сертификаты ФСБ на СКЗИ по классам от КС1 до КС3

ViPNet Client for Windows | ViPNet Client for Linux | ViPNet Client for Android | ViPNet Client for iOS | ViPNet Client for MacOS | ViPNet Client for Sailfish

Линейка Endpoint Security

infotecs



ViPNet SafeBoot

программное
средство
доверенной загрузки



ViPNet SafePoint

классическое средство
защиты информации
от несанкционированного
доступа



ViPNet IDS HS

система обнаружения
вторжений уровня хоста

Подключение к рабочему компьютеру в офисе



ViPNet SafePoint:

- ограничение установки дополнительного ПО пользователем
- ограничение запуска обновлений имеющегося ПО
- ограничение изменений в значимые ветки реестра

ViPNet IDS HS:

- расширение политик аудита

Корпоративный ноутбук дома



ViPNet SafeBoot:

- доверенная загрузка

ViPNet SafePoint:

- политики доступа к локальным и внутрикорпоративным ресурсам
- организация изолированной программной среды
- наделение администратора ИБ полномочиями:
  - чтение запущенных процессов
  - принудительное завершение привилегированного процесса

ViPNet IDS HS:

- расширение политик аудита

ViPNet Connect для защиты коммуникаций

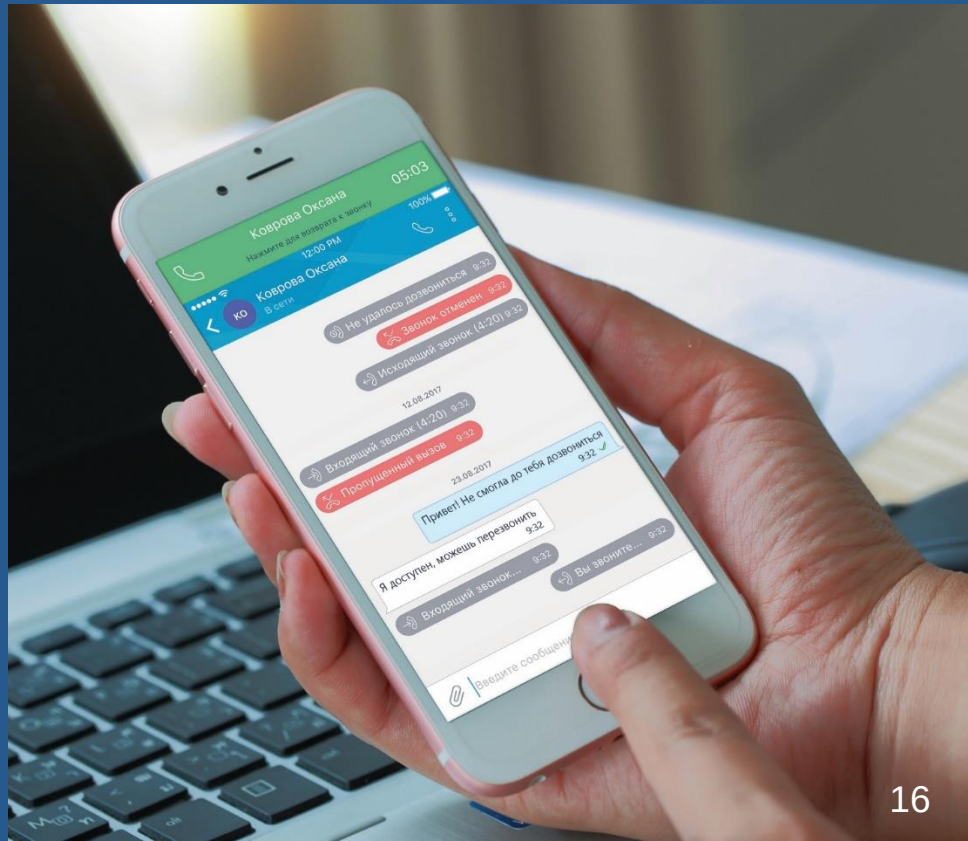


Изолированная система для организации защищенного контура корпоративных коммуникаций

Поддержка популярных платформ:
iOS, Android, Windows, macOS, Linux, Sailfish

Сценарии использования ViPNet Connect

- Замена GSM телефона для ведения конфиденциальных переговоров
- Замена штатного IP-телефона
- Внутрикорпоративный мессенджер
- Групповые чаты для различных задач
- Передача файлов и вложений без изменения их качества

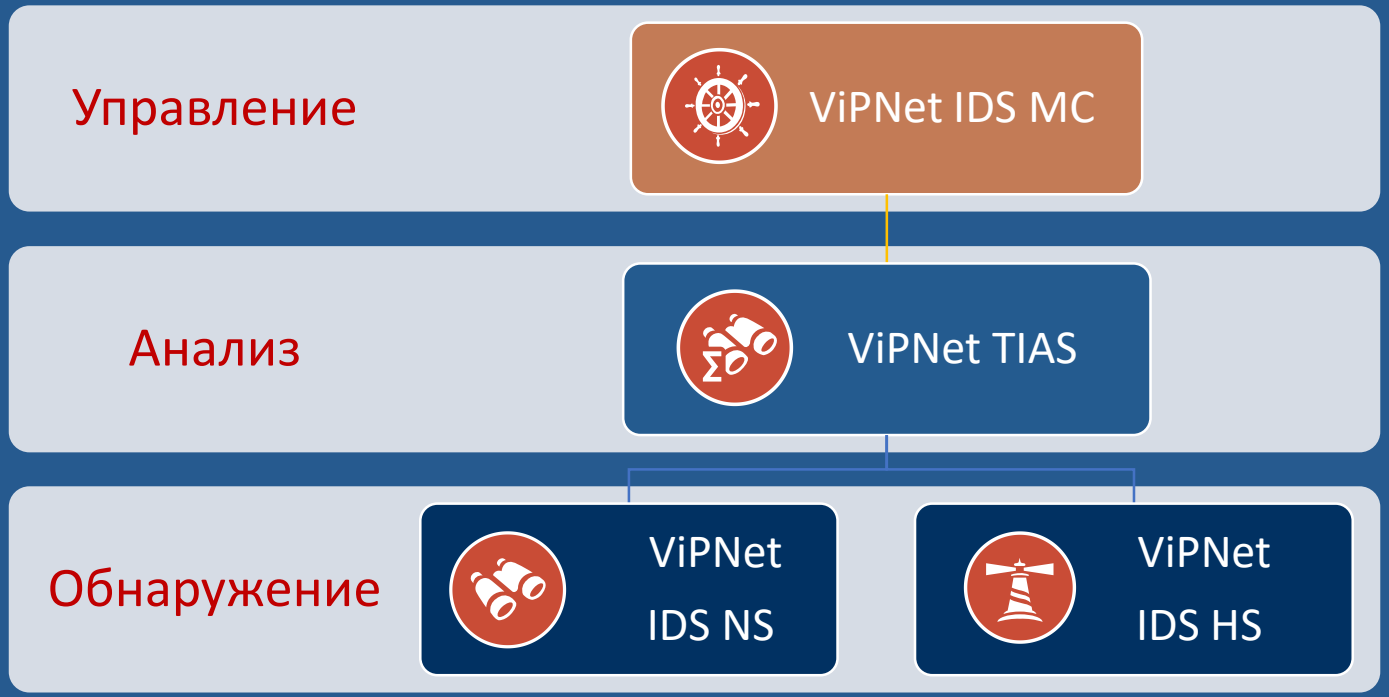


Проблема мониторинга и контроля действий пользователей



- Периметр «размыт»
- Поверхность атак увеличена
- В сети работают недоверенные устройства
- Специалисты ИБ сами на удаленной работе

Решение Threat Detection & Response



Полезные ссылки

- Все вебинары вы можете найти на нашем сайте - https://infotecs.ru/webinars/archive/
- Обеспечение защиты рабочих станций и серверов продуктами ИнфоТеКС. Обзор новых версий продуктов направления Endpoint Security - https://youtu.be/lF11vhPIyn4
- Обзор продуктов ViPNet для клиентских платформ - https://youtu.be/4JnHZ8Jogao
- ViPNet Connect — как защитить свои корпоративные коммуникации - https://youtu.be/LCHbp4Tf3gw
- Социальная инженерия на практике. Проектный опыт «Перспективного мониторинга» - https://youtu.be/FWMSrBWEa5k

infotecs

Спасибо
за внимание!

infotecs

Оценка соответствия финансовых организаций требованиям 683-П и 684-П, включая требования ГОСТ Р 57580.1.

Часть 1. Внешняя оценка соответствия/ аудит защиты информации

Требования нормативных актов Банка России по защите информации

- Кредитные организации – Положение № 683-П
- Некредитные финансовые организации – Положение № 684-П



Технологические меры защиты информации



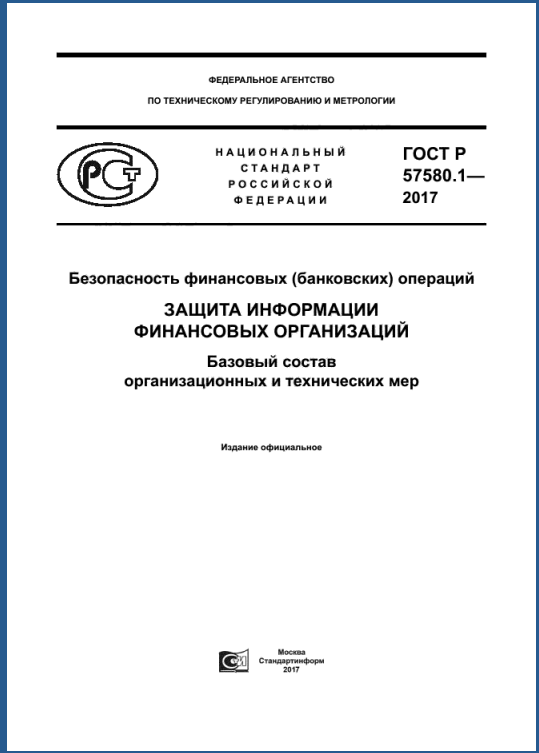
- требования к подписанию электронных сообщений
- требования к технологическим участкам (идентификация, аутентификация и авторизация клиентов, формирование (подготовка), передача и прием электронных сообщений, удостоверение права клиентов распоряжаться денежными средствами,…)
- требования к протоколированию на технологических участках
- требования к хранению защищаемой информации

С начала года в рамках проверок кредитных организаций надзором Банка России осуществляется контроль реализации технологических мер защиты информации

Меры защиты объектов информационной инфраструктуры

- Защита объектов информационной инфраструктуры в соответствии с требованиями ГОСТ Р 57580.1-2017
- Источники требований ГОСТ Р 57580.1-2017:
  - внутренние нормативные документы Банка России
  - Положение Банка России № 382-П
  - Нормативный документ «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный Приказом ФСТЭК России от 18 февраля 2013 г. № 21

Реализация требований ГОСТ Р 57580.1 позволяет осуществить большую часть мер Положения № 382-П и мер защиты персональных данных



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.1— 2017

Безопасность финансовых (банковских) операций

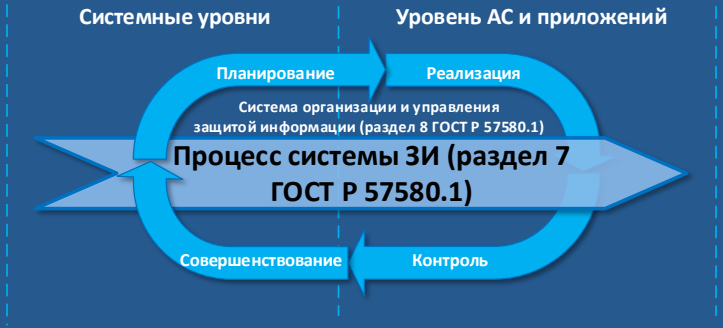
ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

Издание официальное

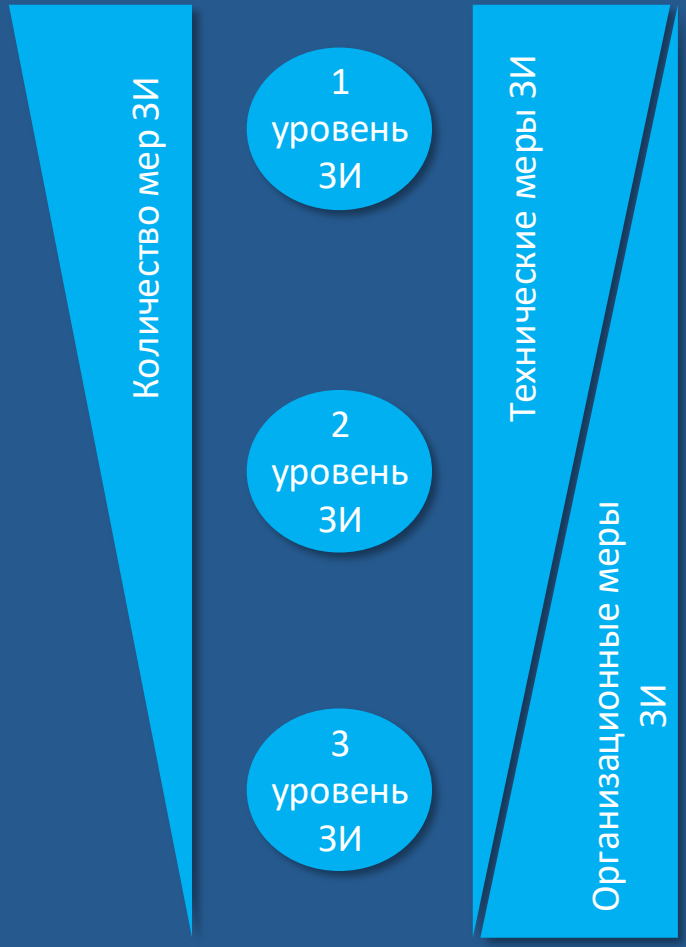
Москва
Стандартинформ
2017

Структура мер защиты информации ГОСТ Р 57580.1



- Структура мер защиты информации приводит к нелинейной модели оценки
- Меры системы организации и управления защитой информации будут оцениваться в отношении каждого из восьми процессов системы защиты информации

- Системные уровни. Распространяются меры защиты информации и меры организации и управления системой защиты информации – разделы 7 и 8 ГОСТ Р 57580.1:
  - уровень аппаратного обеспечения;
  - уровень сетевого оборудования;
  - уровень сетевых приложений и сервисов;
  - уровень серверных компонентов виртуализации, программных инфраструктурных сервисов;
  - уровень операционных систем, систем управления базами данных, серверов приложений;
- Уровень автоматизированных систем и приложений, эксплуатируемых для оказания финансовых услуг в рамках бизнес-процессов или технологических процессов финансовой организации. Распространяются меры защиты информации, меры организации и управления системой защиты информации и меры защиты информации на стадиях жизненного цикла АС – разделы 7, 8, 9 ГОСТ Р 57580.1



Уровни защиты информации

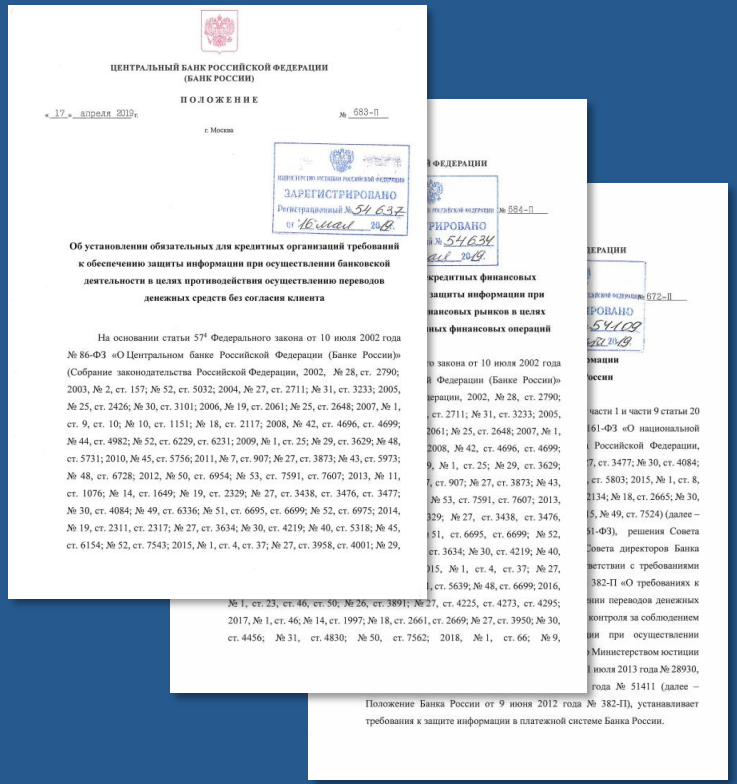
Уровень защиты информации определяет состав и вид требуемых мер защиты информации!!!

- Уровень 3 – минимальный (планировался для малых и микропредприятий)
- Уровень 2 – стандартный (примерно 60% мер защиты информации)
- Уровень 1 – усиленный (максимальное количество требований, максимальное количество технических мер защиты информации)

Контуры безопасности. Ключевое понятие

- Контур безопасности - совокупность объектов информатизации, определяемая областью применения настоящего стандарта, используемых для реализации бизнес-процессов и (или) технологических процессов финансовой организации единой степени критичности (важности), для которой финансовой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации)
- Уровень защиты информации финансовой организации для конкретного контура безопасности устанавливается нормативными актами Банка России
- В финансовой организации формируются один или несколько контуров безопасности, для которых может быть установлен разный уровень защиты информации

<u>На практике до настоящего времени в кредитных организациях и некредитных финансовых организациях не встречалось выделение контуров безопасности</u>



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«17» апреля 2019 г. № 683-П

г. Москва

ЗАРЕГИСТРИРОВАНО
Регистрационный № 54637
от 16 мая 2019

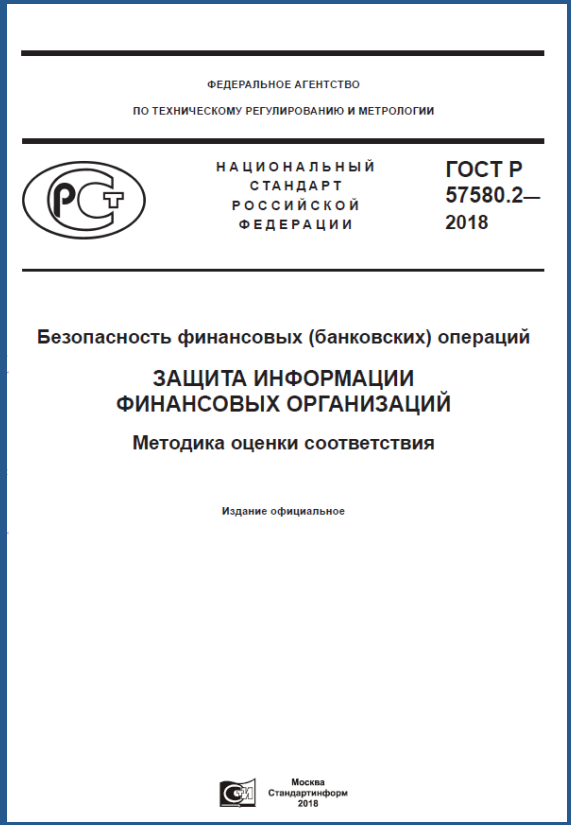
Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента

На основании статьи 57[4] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317; № 27, ст. 3634; № 30, ст. 4219; № 40, ст. 5318; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, ст. 37; № 27, ст. 3958, ст. 4001; № 29, ст. 4356, ст. 4357; № 41, ст. 5639; № 48, ст. 6699; 2016, № 1, ст. 23, ст. 46, ст. 50; № 26, ст. 3891; № 27, ст. 4225, ст. 4273, ст. 4295; 2017, № 1, ст. 46; № 14, ст. 1997; № 18, ст. 2661, ст. 2669; № 27, ст. 3950; № 30, ст. 4456; № 31, ст. 4830; № 50, ст. 7562; 2018, № 1, ст. 66; № 9, ст. 1283; № 18, ст. 2560; № 27, ст. 3956; № 30, ст. 4547; № 32, ст. 5110; № 49, ст. 7524) (далее – Федеральный закон № 86-ФЗ), решения Совета директоров Банка России, оформленного протоколом от 15 марта 2019 года № 7, в целях обеспечения соответствия с требованиями

Положение Банка России от 9 июня 2012 года № 382-П, устанавливает требования к защите информации в платежной системе Банка России.

Оценка соответствия ЗИ

- Методика ГОСТ Р 57580.2-2018 не распространяется на оценку реализации технологических мер защиты информации и требований к эксплуатации СКЗИ
- Методика ГОСТ Р 57580.2-2018 распространяется на оценку реализации мер защиты объектов информационной инфраструктуры
- Назначение ГОСТ Р 57580.2-2018:
  - установление единых требований к методике и оформлению результатов оценки соответствия ЗИ финансовой организации
  - установление способов оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1–2017
  - вычисление уровней соответствия ЗИ [процессов ЗИ]
  - определение итоговой оценки соответствия ЗИ финансовой организации требованиям ГОСТ Р 57580.1


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.2— 2018

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Методика оценки соответствия

Издание официальное

Москва
Стандартинформ
2018

Шкалы оценок

Выбор финансовой организацией каждой организационной или технической меры защиты информации, входящих в систему защиты информации (раздел 7 ГОСТ Р 57580.1) оценивается по следующей шкале:

- «0» – мера защиты информации не выбрана (выставляется при отсутствии свидетельств выбора)
- «1» – мера защиты информации выбрана (выставляется при предъявлении свидетельств выбора)

При наличии любого вида свидетельств о выборе меры защиты информации на любом количестве объектов информационной инфраструктуры области оценки соответствия, выбор данной меры защиты информации будет оценен значением «1»

Полнота реализации каждой из мер защиты информации, входящих в систему организации и управления защитой информации финансовой организации и установленных в разделе 8 ГОСТ Р 57580.1–2017, оценивается по следующей шкале:

- «0» – мера защиты информации полностью не реализуется (не найдено свидетельств реализации всех мер защиты информации процесса системы защиты информации ни на одном объекте информационной инфраструктуры);
- «0.5» – мера защиты информации реализуется не в полном объеме (реализованы не все меры защиты информации процесса системы защиты информации или меры защиты информации реализованы не на всех возможных объектах информационной инфраструктуры);
- «1.0» – мера защиты информации реализуется в полном объеме (реализованы все меры защиты информации процесса системы защиты информации и меры защиты информации реализованы на всех объектах информационной инфраструктуры)

Уровень соответствия защиты информации. Все не так просто

- Уровень соответствия показывает степень соответствия **реализации процессов защиты** информации требованиям ГОСТ Р 57580.1.

  Не путать уровень соответствия и уровень защиты информации!!!

- Уровень соответствия определяется для каждого из восьми процессов защиты информации, а не для итоговой оценки соответствия ЗИ

- Требование обеспечения уровня соответствия защиты информации не ниже 4-го говорит о том, что каждый из восьми процессов защиты информации должен иметь оценку соответствия более 0,85

- 4-й уровень соответствия: организационные и технические меры процесса системы защиты информации реализуются в полном объеме на постоянной основе. В основном реализованы контроль и совершенствование реализации организационных и технических мер процесса системы защиты информации

Ei	Уровень соответствия
Ei = 0	Нулевой
0 < Ei ≤ 0,5	Первый
0,5 < Ei ≤ 0,7	Второй
0,7 < Ei ≤ 0,85	Третий
0,85 < Ei ≤ 0,9	Четвертый
0,9 < Ei ≤ 1	Пятый

Отчетность по результатам оценки соответствия

Раздел 8 ГОСТ Р 57580.2 устанавливает требования к содержанию отчетных материалов по результатам оценки соответствия защиты информации:

- отчет по результатам оценки соответствия
- приложения к отчету:
  - заполненные листы для сбора свидетельств оценки
  - перечень нарушений защиты информации, выявленных членами проверяющей группы в результате оценки соответствия защиты информации
  - рекомендации по совершенствованию защиты информации и устранению выявленных нарушений;
  - таблицы, содержащие числовые значения оценок процессов (подпроцессов) системы защиты информации и направлений защиты информации
  - копии документов проверяемой организации или документов третьих лиц на бумажных носителях, являющихся свидетельствами выполнения (невыполнения) требований защиты информации
  - машинные носители информации с электронными документами и файлами данных, являющихся свидетельствами выполнения (невыполнения) требований ЗИ

Сотни листов отчета.

Оформление сотен свидетельств выполнения (невыполнения) требований защиты информации

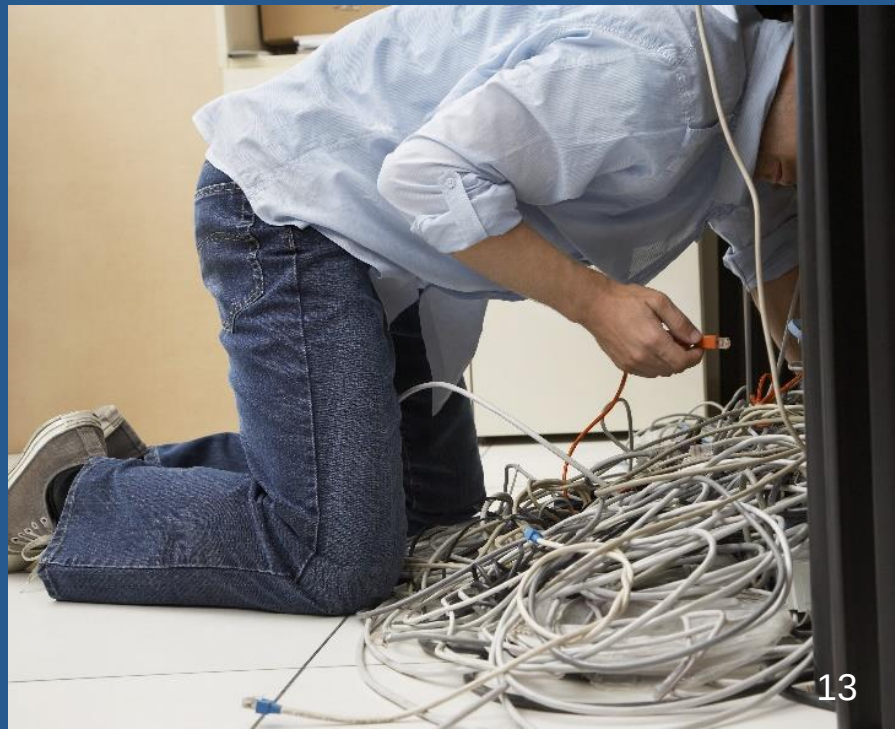
Стратегия работ по проведению оценки соответствия



- 2020 год - предварительная оценка соответствия:
  - позволяет выявить недостатки системы защиты информации и подготовиться к оценке соответствия
  - для удешевления не формируется полная отчетность по ГОСТ Р 57580.2, тем не менее отчетность составляет сотни листов
  - предоставляются рекомендации по приведению деятельности организации в соответствие с требованиями нормативных актов Банка России и ГОСТ Р 57580.1
  - более низкая цена по сравнению с оценкой соответствия с оформлением полной отчетной документации
- 2021 год и позже – оценка соответствия с оформлением полной отчетной документации:
  - для предоставления результатов в Банк России
  - отчетные материалы формируются в соответствии с требованиями раздела 8 ГОСТ Р 57580.2

Что после предварительной оценки соответствия?

- для НФО сформировать Службу информационной безопасности (если не сформирована)
- сформировать план мероприятий по реализации рекомендаций
- принять решение о закупке недостающих средств защиты информации
- принять решение о разработке недостающих и корректировке действующих внутренних регламентов с учетом закупленных технических средств ЗИ и их функциональности
- закупить и внедрить необходимые средства защиты информации
- ввести в действие внутренние регламенты и проверить правильность реализации процессов ЗИ



Факторы, влияющие на стоимости оценки соответствия



- стоимость работы в 2-3 раза выше стоимости оценки соответствия требованиям положения Банка России № 382-П
- большое количество проверяемых мер защиты информации (150 мер № 382-П и 371 мера системы защиты информации, 37 мер системы управления защитой информации и 28 мер защиты информации на стадиях ЖЦ АС)
- нелинейная модель оценки реализации мер защиты информации ГОСТ Р 57580.1
- как правило, в контур безопасности попадают сотни объектов информационной инфраструктуры

Факторы, влияющие на стоимости оценки соответствия



- не обойтись без работ на объекте Заказчика по сбору свидетельств реализации требуемых мер защиты информации
- обязательно участие при проведении оценки соответствия высококвалифицированных специалистов проверяемой организации. В противном случае – риск объективности оценки

Выбор подрядчика

- Нормативными актами Банка России установлен единственный критерий – наличие лицензии на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79
- Кроме того, зачастую предъявляются:
  - требования к опыту проведения аналогичных работ (подтверждается договорами и актами закрытия этапов, подтверждается рекомендательными письмами, отзывами о работе)
  - требования к квалификации работников внешней организации (подтверждается сертификатами, стажем работы)

Заказ комплекса работ у единого подрядчика (оценка соответствия, тестирование на проникновение, ОУД4) позволяет получить скидку на комплекс работ.

infotecs

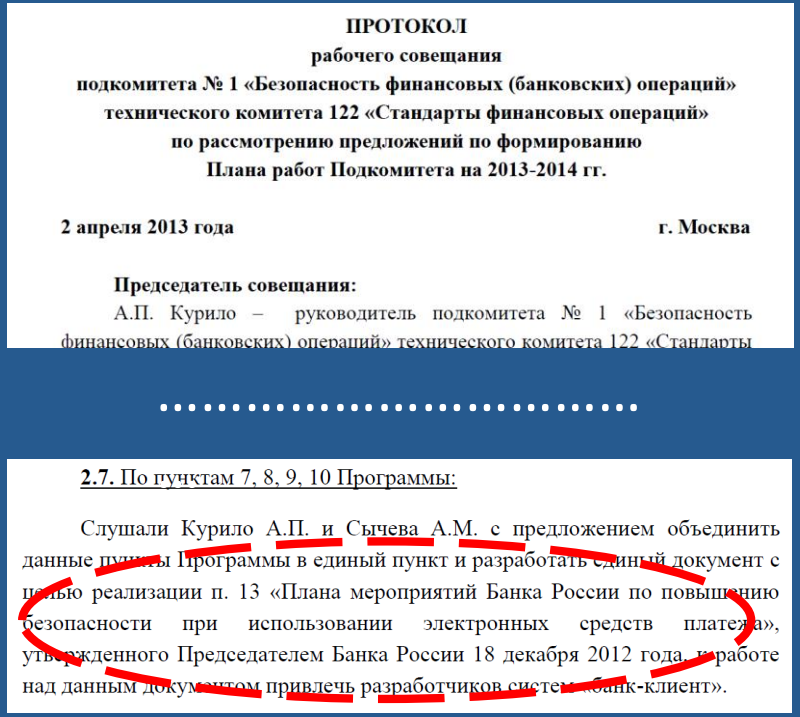
Спасибо
за внимание!

Оценка соответствия финансовых организаций требованиям 683-П и 684-П, включая требования ГОСТ Р 57580.1.

Часть 2: Работы по анализу уязвимости прикладного программного обеспечения требованиям ОУД4

Источники введения данных требований

- Регулятора не устраивал неуклонный рост с начала 2000-х числа использования злоумышленниками дефектов электронных платежных инструментов
- Участники рынка финансового программного обеспечения (производители, посредники, пользователи) не спешили исправлять ситуацию, аргументируя «ненужными» расходами
- С 2012 Регулятор вынужден был реагировать доступными ему методами



ПРОТОКОЛ
рабочего совещания
подкомитета № 1 «Безопасность финансовых (банковских) операций»
технического комитета 122 «Стандарты финансовых операций»
по рассмотрению предложений по формированию
Плана работ Подкомитета на 2013-2014 гг.

2 апреля 2013 года **г. Москва**

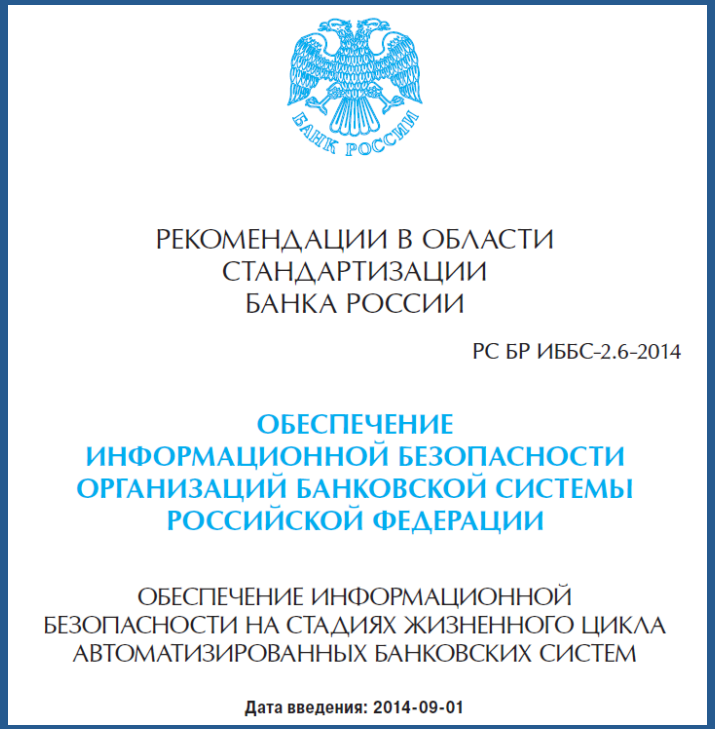
Председатель совещания:
А.П. Курило – руководитель подкомитета № 1 «Безопасность финансовых (банковских) операций» технического комитета 122 «Стандарты

.....

2.7. По пунктам 7, 8, 9, 10 Программы:

Слушали Курило А.П. и Сычева А.М. с предложением объединить данные пункты Программы в единый пункт и разработать единый документ с целью реализации п. 13 «Плана мероприятий Банка России по повышению безопасности при использовании электронных средств платежа», утвержденного Председателем Банка России 18 декабря 2012 года, по работе над данным документом привлечь разработчиков систем «банк-клиент».

2014 год. Рекомендации Банка России



БАНК РОССИИ

РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.6-2014

ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА
АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Дата введения: 2014-09-01

В соответствии с Планами работ Подкомитета №1 Технического комитета 122 «Стандарты финансовых операций» на 2013-2014 гг. были разработаны соответствующие рекомендации Банка России, включающие требования по всем необходимым работам
в части разработки «безопасного» программного обеспечения для финансовых операций, но…

2016 год. Нормативное регулирование

- Подготовка изменений в 382-П (4793-У)
- Включение требований в новые нормативные акты (683-П и 684-П)
- Разработка методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций»
- ……


ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)
УКАЗАНИЕ
«7» мая 2018 г. № 4793-У
г. Москва
ЗАРЕГИСТРИРОВАНО
Регистрационный № 51411
от "22" июня 2018.
О внесении изменений в Положение Банка России
от 9 июня 2012 года № 382-П «О требованиях
ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)
ПОЛОЖЕНИЕ
«17» апреля 2019 г. № 684-П
г. Москва
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54634
от "16" мая 2019.
Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций
На основании статьи 76[4-1] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005,
ПОЛОЖЕНИЕ
№ 683-П
г. Москва
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54637
от 16 мая 2019.

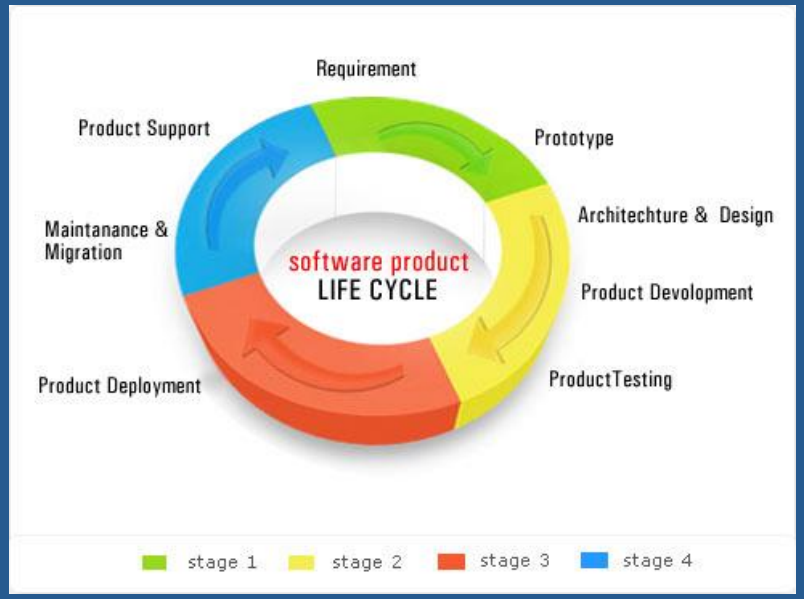
Работы по анализу уязвимостей по ОУД4 и в рамках эксплуатации. 382-П

infotecs

Возможная Модель ЖЦ

Тестирование на проникновение и анализ уязвимости ПРИ эксплуатации

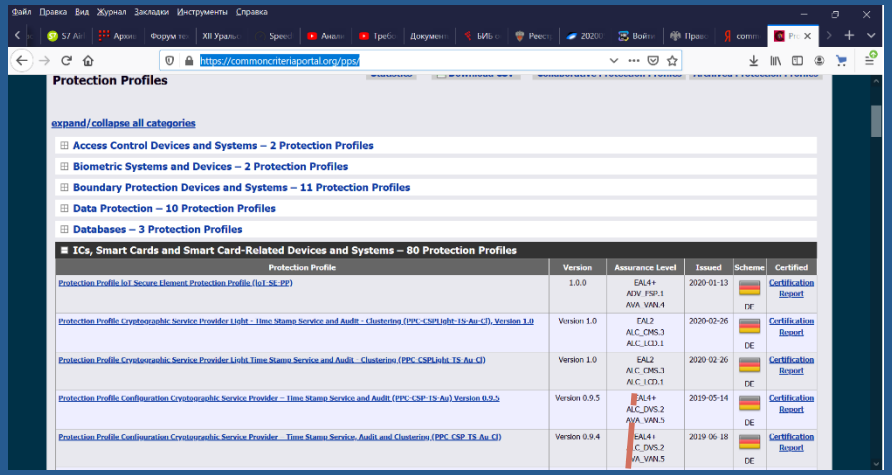
Показатель П.14.2



Работы по ОУД4 ПЕРЕД эксплуатацией

Показатель П.14.1

ОУД4. Излишняя строгость?



EAL4+
ALC_DVS.2
AVA_VAN.5

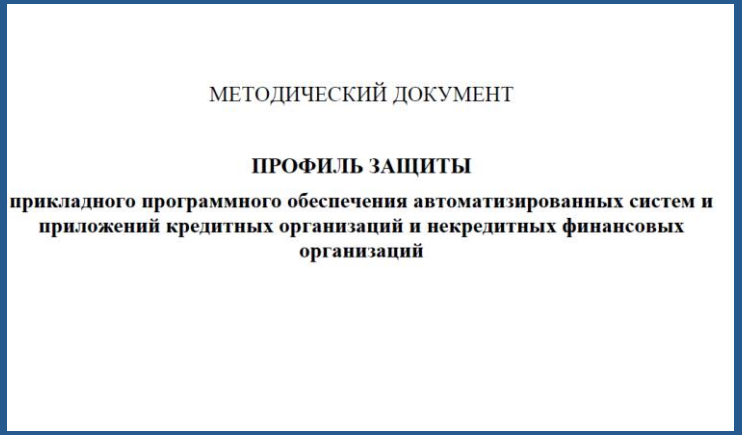
https://commoncriteriaportal.org/pps/

- Для смарт-карт и финансовых приложений с 1999 г. установилась практика оценок по уровню доверия не ниже ОУД4
- В европейском платежном пространстве действуют аналогичные требования (Single Euro Payments Area (SEPA) – единая зона платежей в евро, см. https://www.europeanpaymentscouncil.eu)
- По принятой еще в прошлом веке политике оценок доверия в безопасности:
  - До ОУД2 включительно – «коробочные продукты»
  - С ОУД4 и далее – «заказные разработки» (требуются тексты программ и пр.)

Методический документ «Профиль защиты прикладного ПО АС и приложений КО и НФО»

- Эквивалент источника требований для анализа уязвимости не ниже, чем по ОУД4
- Включает требования из ГОСТ Р 57580.1 (функциональные требования) и требования ОУД4 усиленные (поэтому ОУД4+)
- Усиление ОУД4 требованиями:

ADV_IMP.2 «Полное отображение представления реализации ФБО», **ALC_FLR.2** «Процедуры сообщений о недостатках», **AVA_VAN.5** «Усиленный методический анализ», *расширенный компонентами* **ADV_IMP_EXT.3** «Реализация ОО», **ALC_FPU_EXT.1** «Процедуры обновления программного обеспечения», **ALC_LCD_EXT.3** «Определенные разработчиком сроки поддержки», **AMA_SIA_EXT.3** «Анализ влияния обновлений на безопасность» и **AVA_CCA_EXT.1** «Анализ скрытых каналов»



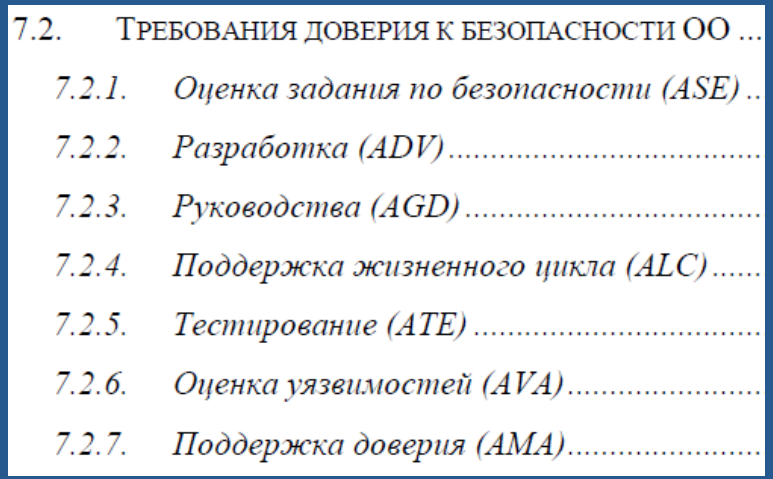
МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ

прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций

Одобрен на заседании ПК1/ТК122 12.12.2019 г.

Методический документ «Профиль защиты прикладного ПО АС и приложений КО и НФО» *(продолжение)*



7.2. ТРЕБОВАНИЯ ДОВЕРИЯ К БЕЗОПАСНОСТИ ОО ...

7.2.1. Оценка задания по безопасности (ASE) ..

7.2.2. Разработка (ADV) .....

7.2.3. Руководства (AGD) .....

7.2.4. Поддержка жизненного цикла (ALC) .....

7.2.5. Тестирование (ATE) .....

7.2.6. Оценка уязвимостей (AVA) .....

7.2.7. Поддержка доверия (AMA) .....

- Состав требований доверия определяет состав документации, разрабатываемой как в ходе проектных работ , так и по итогам тестирований релизов ДО их поставки дилерам и (или) пользователям
- Характер требований выводит на необходимость наличия у разработчика финансовых программ документов, из состава:
  - Конструкторских документов
  - Программных документов
  - Дополнительных специализированных отчетов по видам анализа и тестированиям

Методический документ «Профиль защиты прикладного ПО АС и приложений КО и НФО» *(продолжение)*

infotecs

Обобщенный состав обоснований соответствия (КД, ПД, ЭД, СпецДок.):

- Описание архитектуры безопасности ФинПр
- Полная функциональная спецификация
- Протоколы контроля представления реализации
- Документированные материалы по реализации ФинПр
- Проект ФинПр (**потребуется стенд**)
- Руководство пользователя по эксплуатации ФинПр
- Подготовительные процедуры
- Документация Управления Конфигурацией при проектировании и разработке
- Список элементов конфигурации для ФИНПР
- Документация поставки ФинПр
- Документация по безопасности разработки ФинПр

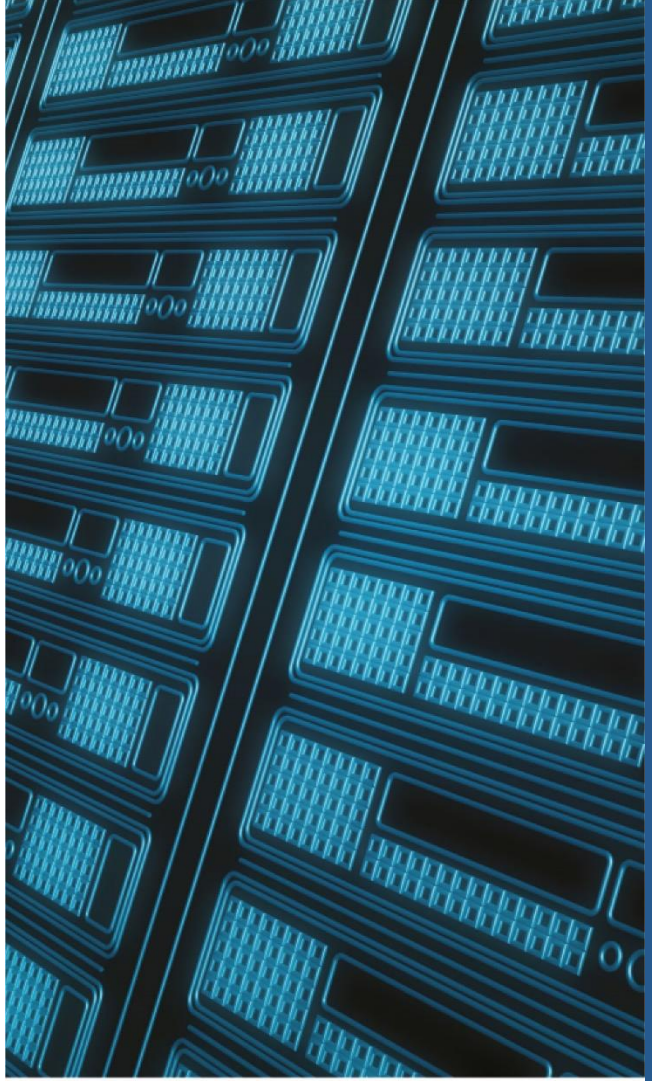
Задание по безопасности ФинПр

- Процедуры устранения недостатков (разработчиков, производителей) ФинПр
- Получение и отработка запросов на исправление недостатков безопасности
- Руководство по устранению недостатков ФинПр
- Описание технологии выпуска обновлений ФинПр
- Регламент обновления ФинПр
- Модель жизненного цикла
- Декларация о сроке поддержки ФинПр
- Описание инструментальных средств разработки
- Документация по тестированию ФинПр
- Тестовая документация по функциональному тестированию
- Документация по анализу скрытых каналов
- Документация по усиленному методическому анализу

Стоимость услуги

ПРОПОРЦИИ

- Разработка Задания по безопасности – около 30% контракта
- Проведение тестирований и анализа на уязвимость с разработкой необходимой отчётности, указываемой в ЗБ – оставшиеся 70%
- Разработка недостающих компонентов КД и ПД – по отдельному договору



infotecs

ДИАПАЗОН ЦЕН

- Проведение работ по безопасности и разработка соответствующей документации - от 1,5 до 2,5 млн. на каждое самостоятельное ФинПр
- При проведении работ для нескольких приложений применяются скидки
- Разработка недостающих компонентов КД и ПД – по отдельному договору (до 1 млн. руб)

Периодичность

- При выходе релиза – 100% стоимости
- При каждом внесении изменения, затрагивающего обработку защищаемой информации – от 30 до 70% полной стоимости работ. В противном случае обоснование, что выпускаемая версия обработку защищаемой информации не затрагивает – *пригодится для общения с надзором*

Альтернатива для снижения стомости работ:

- Внедрение SDLC, например, по ГОСТ Р 56939 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»
- Создание (из собственных сотрудников или найм) команды тестировщиков аналитиков ИБ. Экономически обоснованным может быть, если разрабатывается 2 и более собственных прикладных систем



ГОСТ Р 56939 как альтернатива. Что это на практике?

- Не «дешевое» удовольствие
- Потребует проектирования и внедрения с учетом оргполитик Разработчика нескольких десятков процессов, сопровождающих разработку и тестирование изделия на различных участках работ
- Наряду с прочим потребуется наладить на постоянной основе проведение работ и оформление их результатов по следующим видам, обосновывающим применение SDLC по ГОСТ Р 56939 (**фрагмент**):
  - порядок оформления исходного кода программы
  - сведения о результатах проведения статического анализа исходного кода программы
  - сведения о результатах проведения экспертизы исходного кода программы
  - сведения о результатах проведения функционального тестирования программы
  - сведения о результатах проведения тестирования на проникновение
  - сведения о результатах проведения динамического анализа кода программы
  - сведения о результатах проведения фаззинг-тестирования программы
  - описание процедур отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы
  - описание процедуры поиска разработчиком ПО уязвимостей программы
  - меры, используемые для защиты инфраструктуры среды разработки ПО и т.п.

С чего начать?

infotecs

Выбор за организацией

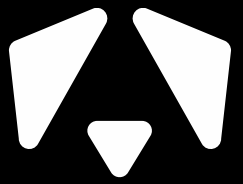
- Можно с пилотного проекта по ОУД4+ на одном из приложений (чтобы «попробовать»)
- На этой основе оценить потребность и собственные возможности по внедрению SDLC и тому, в чем и какая будет экономия относительно требований Профиля защиты от Банка России
- Рассмотреть организацию партнёрского долгосрочного сотрудничества с лицензиатом ФСТЭК на проведение работ по ОУД4 на постоянной (периодической по потребности) основе
- Спроектировать и внедрить процессы по SDLC и организовать партнёрское долгосрочное сотрудничество с лицензиатом ФСТЭК на определенный блок работ или (как альтернатива) создать собственную группу аналитиков/тестировщиков ИБ
- ……

ВАЖНО: хотелось бы обратить внимание на то, что бездействовать НЕ получится – это не надолго.

Внедрение той или иной из технологий обеспечения «безопасности» финансовых приложений – неизбежно

infotecs

Спасибо
за внимание!



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Периодическое тестирование на проникновение и анализ уязвимостей при эксплуатации

Сергей Нейгер

Менеджер по развитию бизнеса, «Перспективный мониторинг»

Как злые хакеры, только добрые

Сами определите поверхность атаки

amonitoring.ru/article/attack-surface/

Наш сайт → Статьи → Анализ поверхности атаки

Статья для журнала «Внутренний контроль в кредитной организации» № 2/2019.

Что точно не пентест по 382/683/684-П*

Пентест банка за 90 т. р.	«Фиктивный» пентест за 800 «Реальный» за 2 500	Отчёт сканера Nessus с новой обложкой

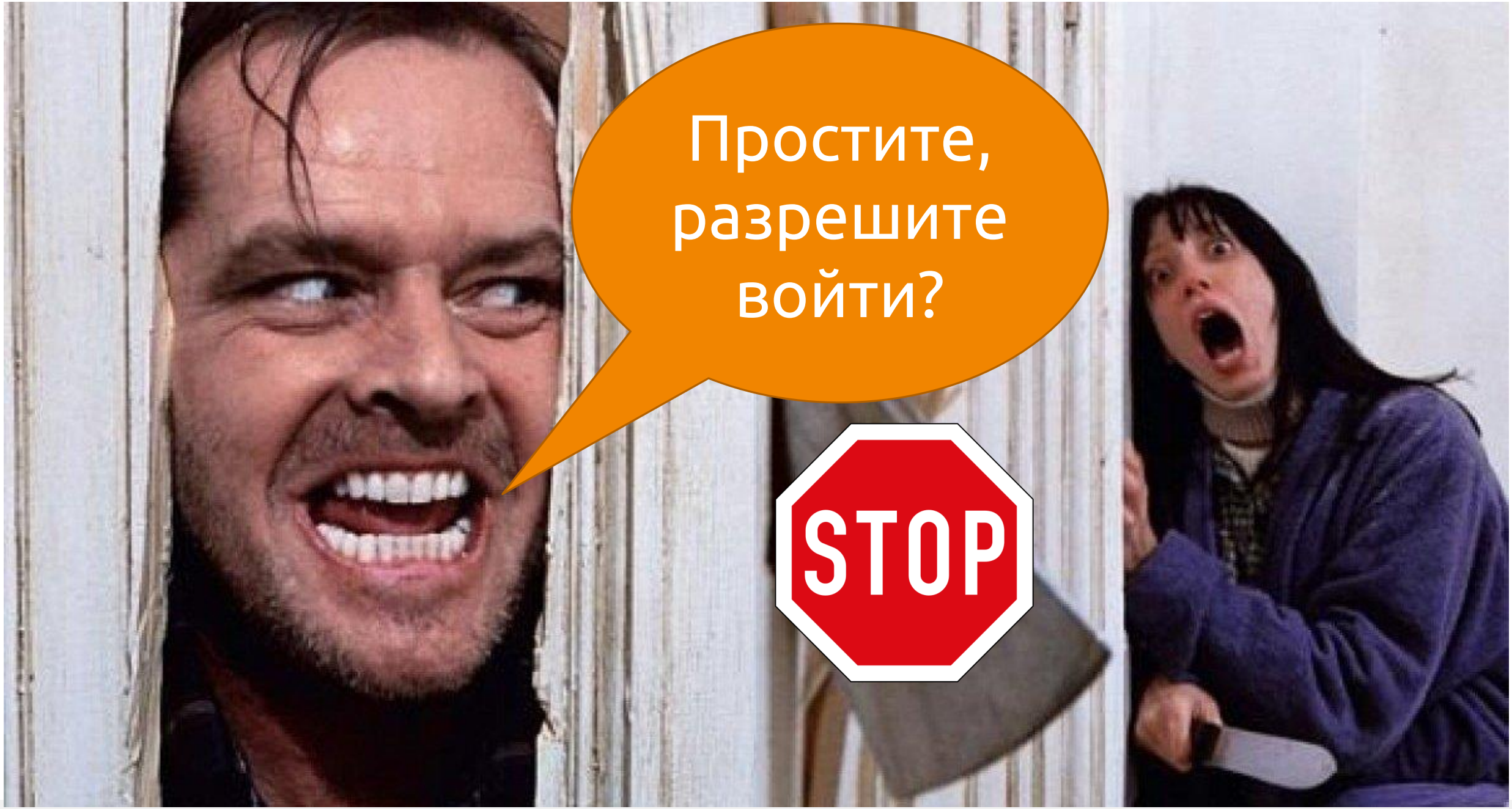
*По нашему мнению

Как мы видим пентесты по 382/683/684

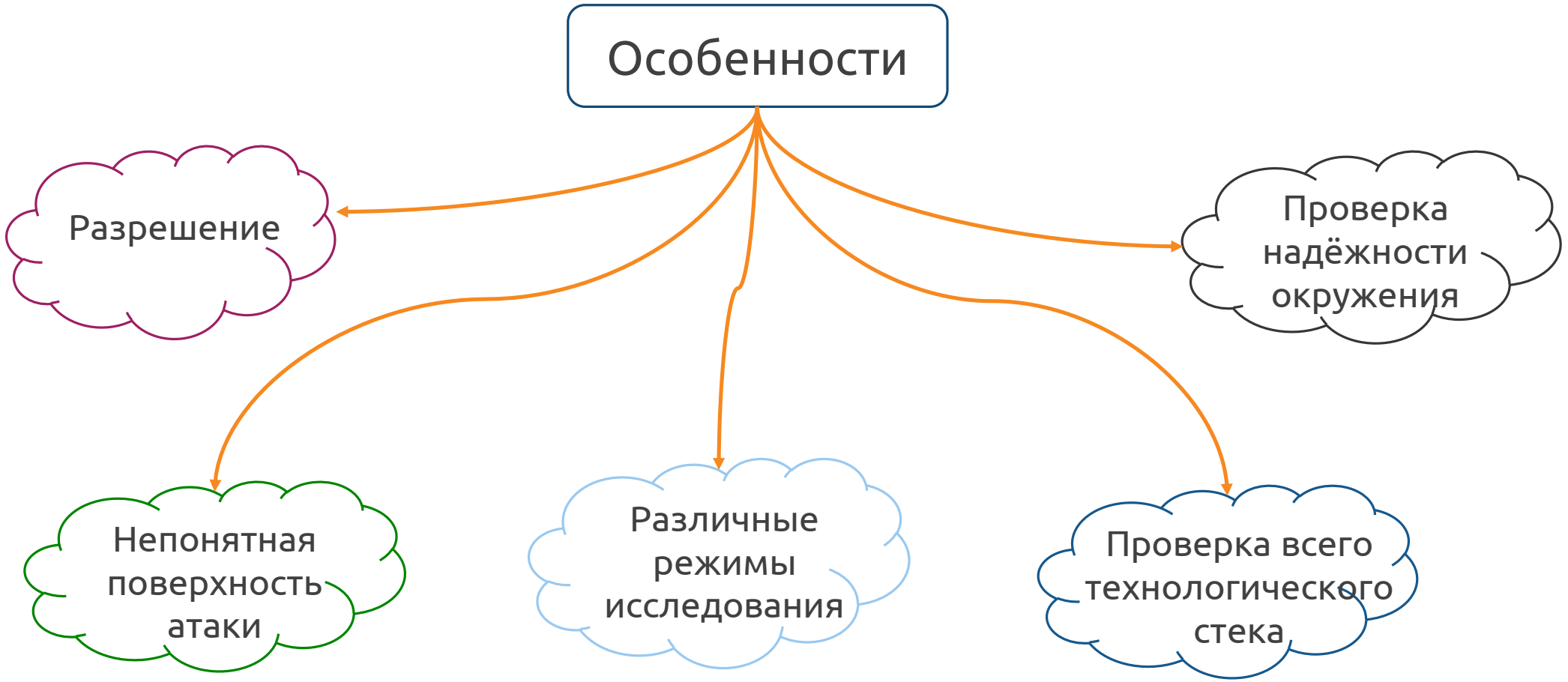
Модели тестирования

Внешний нарушитель	Внутренний нарушитель
Сайты и веб-приложения	«Ядерные» ИС
Внешний периметр	Серверы баз данных и приложений
Мобильные приложения	Типовые рабочие места
Проверка осведомлённости	Сетевое оборудование

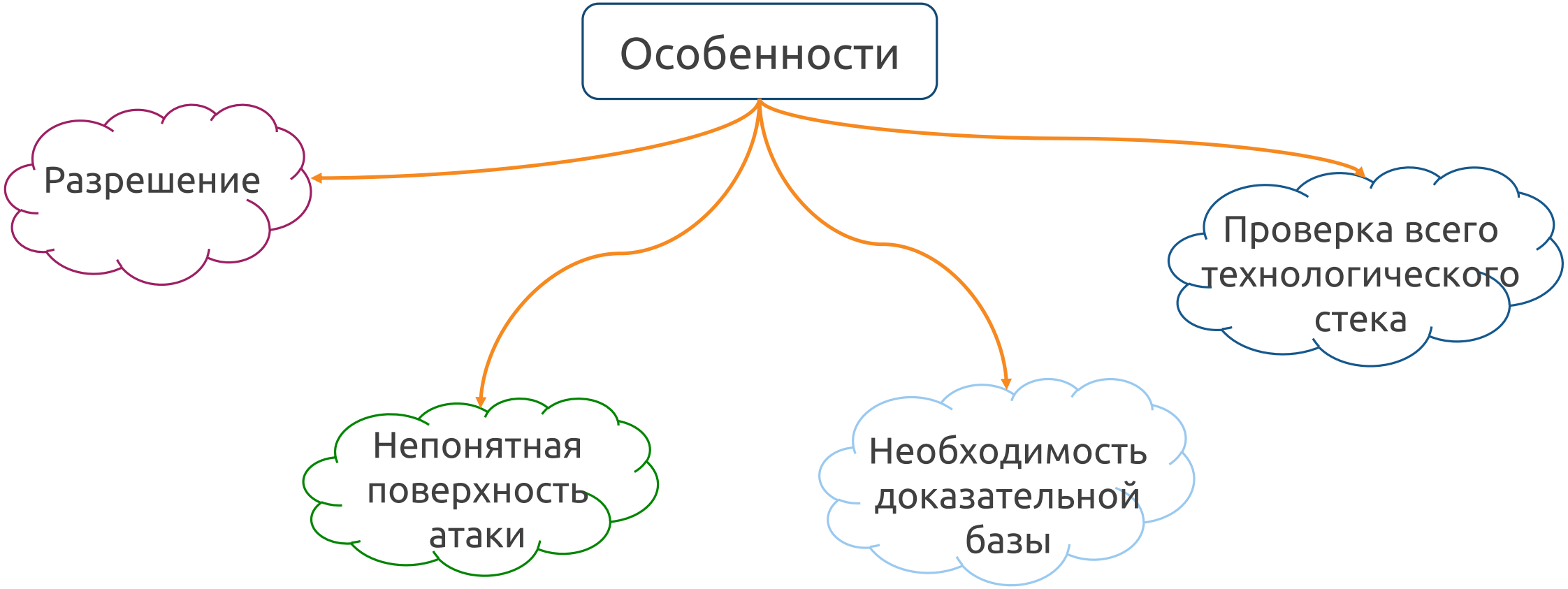



Простите, разрешите войти?
STOP

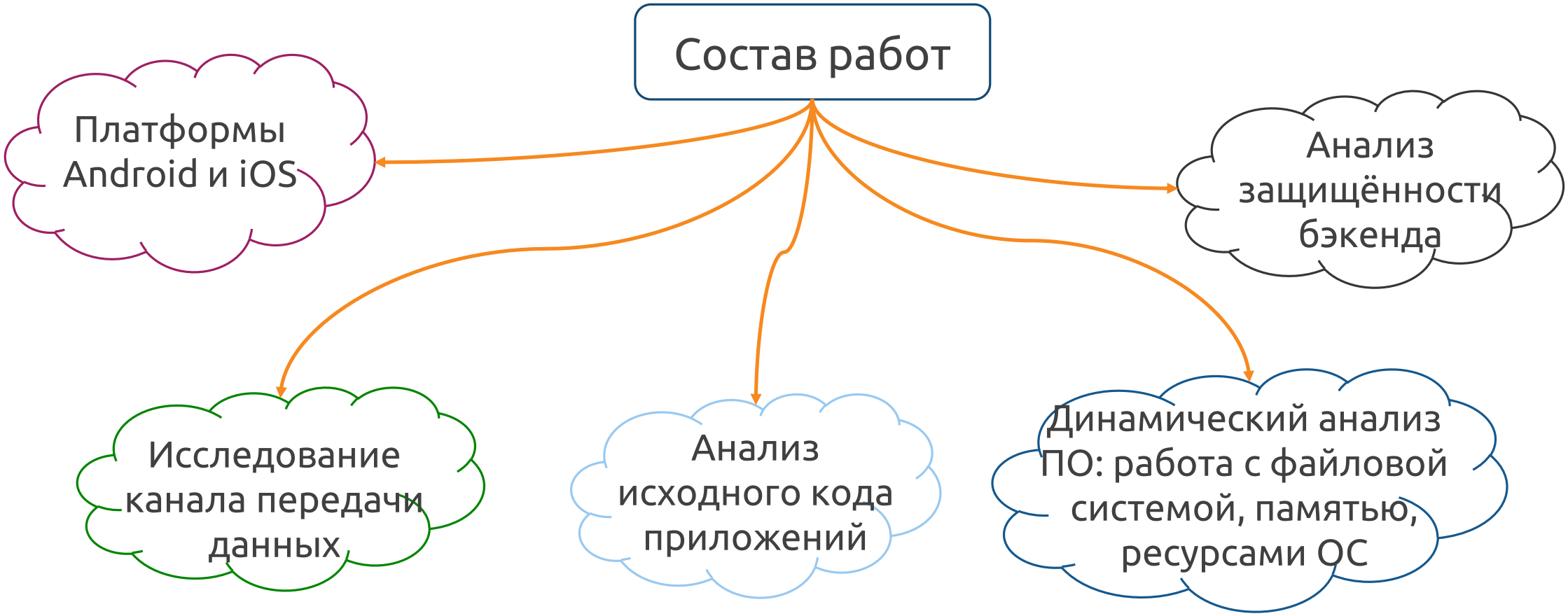
Веб


Особенности
Разрешение
Проверка надёжности окружения
Непонятная поверхность атаки
Различные режимы исследования
Проверка всего технологического стека

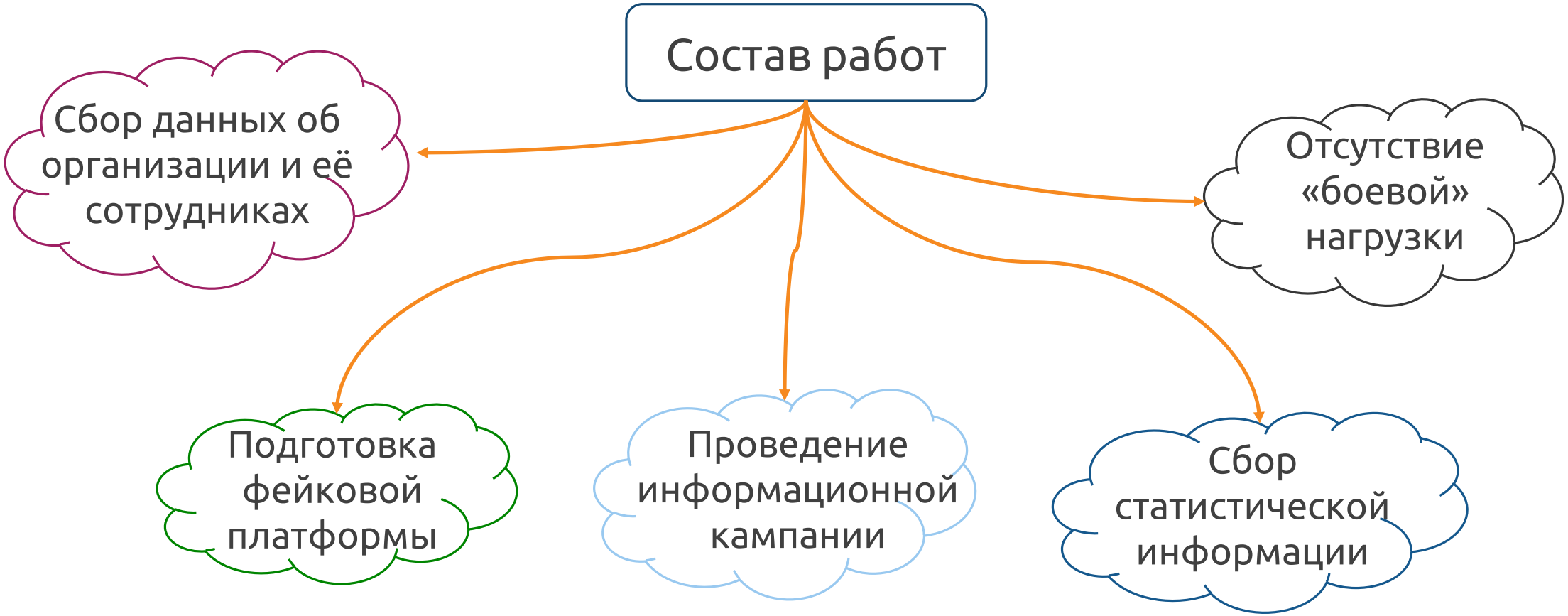
Внешний периметр



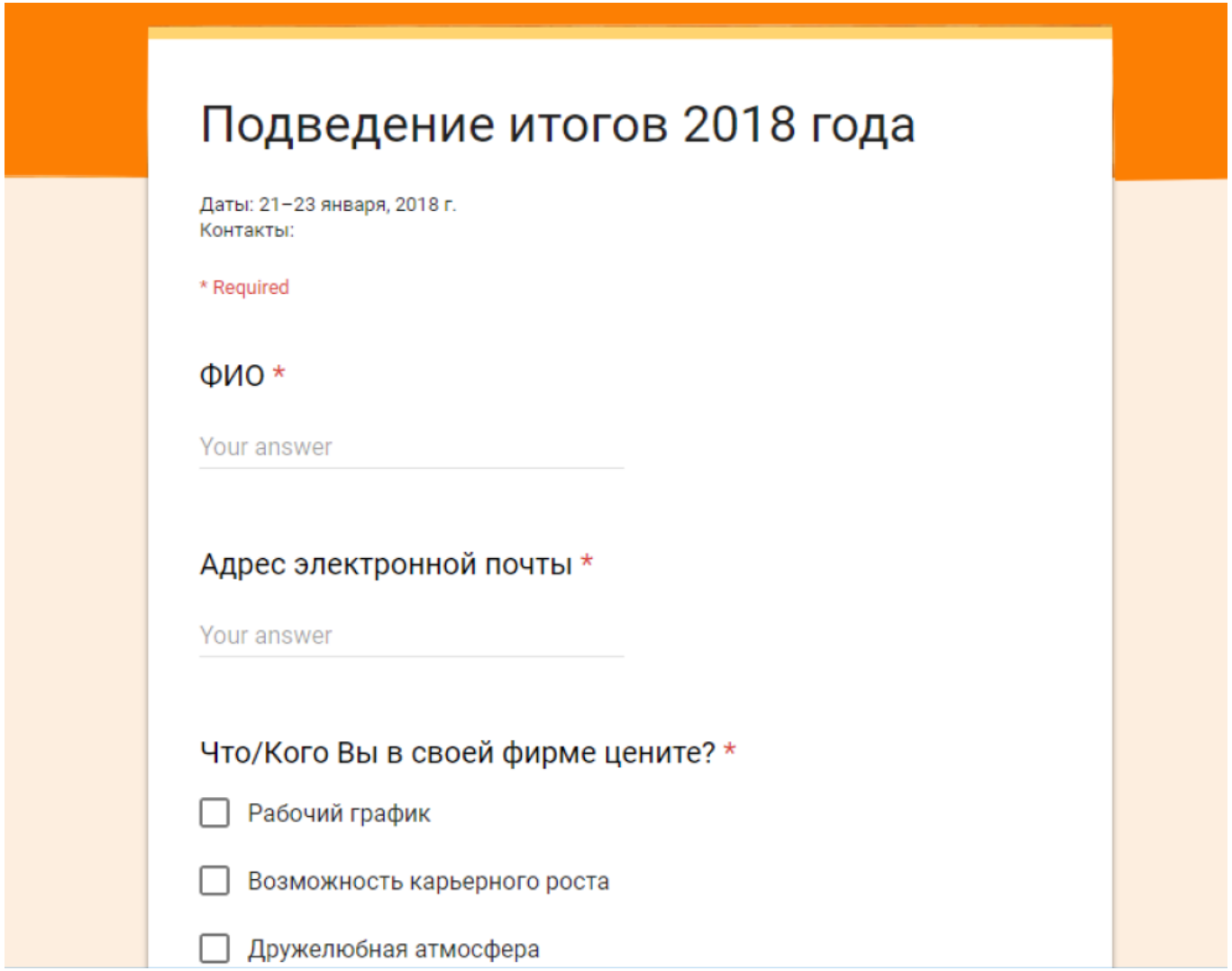
Мобильные приложения



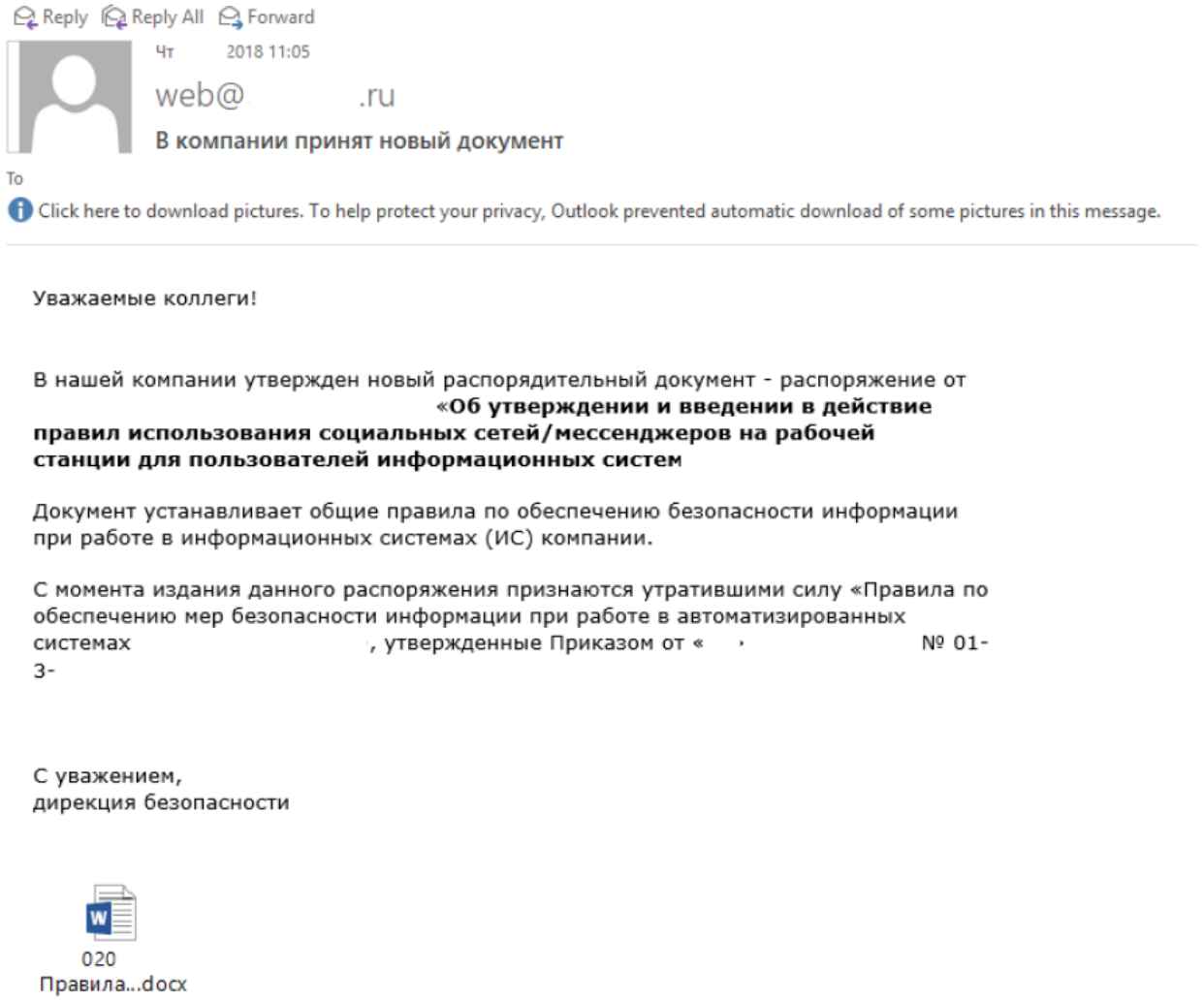
Проверка осведомлённости



Пример фишинговой формы



Пример фишингового письма



Reply Reply All Forward

Чт 2018 11:05

web@ .ru

В компании принят новый документ

To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Уважаемые коллеги!

В нашей компании утвержден новый распорядительный документ - распоряжение от «**Об утверждении и введении в действие правил использования социальных сетей/мессенджеров на рабочей станции для пользователей информационных систем**

Документ устанавливает общие правила по обеспечению безопасности информации при работе в информационных системах (ИС) компании.

С момента издания данного распоряжения признаются утратившими силу «Правила по обеспечению мер безопасности информации при работе в автоматизированных системах , утвержденные Приказом от « » № 01-3-

С уважением,
дирекция безопасности

020 Правила...docx

Сбор статистики



Подробности

Поиск:

Имя	Почта	Должность	Статус
Иоганн Тритемий	it@benediktiner.de	Аббат	Данные введены
Алан Тьюринг	bombe@cam.ac.uk	Тестировщик	Письмо отправлено
Уитфилд Диффи	publickey@icann.org	CISO	Письмо отправлено
Майкл Роджерс	bigboss@nsa.gov	Адмирал	Переход по ссылке

Пентестер перед погружением в ИТ-инфраструктуру банка



VS

Пентестер, разобравшийся в инфраструктуре банка



Спасибо за внимание!

И проверяйте себя!

Сергей Нейгер

Менеджер по развитию бизнеса

компании «Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru

