



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Актуальные вопросы информационной безопасности для кредитных и некредитных финансовых организаций

Сергей Нейгер

Директор по развитию бизнеса

Татьяна Каргина

Менеджер по работе с заказчиками

Александр Новиченко

Руководитель направления OSINT

Алексей Глазков

Руководитель обособленного подразделения в г. Пенза



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ


Обобщённые результаты исследований защищённости по требованиям Банка России: на что стоит обратить внимание

Татьяна Каргина

Менеджер по работе с заказчиками, «Перспективный мониторинг»

О ЧЕМ ПОГОВОРИМ?




 Объекты исследования. Степени критичности уязвимостей.

 Клиентская часть ДБО

 Мобильные приложения

 Сервисы внешнего периметра

 Внутренний сетевой периметр

 Заключение

ОБЪЕКТЫ ИССЛЕДОВАНИЯ



Клиентская часть каналов ДБО

Мобильные приложения

Внешний периметр

Банковские информационные системы

Сервера инфраструктуры каналов ДБО

Сервера баз данных

Типовые рабочие места сотрудников

Сетевое оборудование

Точки доступа к беспроводной сети

СТЕПЕНИ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ



Критичный

злоумышленник получает полный доступ к атакуемой системе



Высокий

злоумышленник получает доступ с правами непривилегированного пользователя, доступ к файловой системе и получение наиболее критичной информации о системе



Средний

злоумышленник получает наиболее критичную информацию об атакуемой системе, информацию о пользователях включая их компрометацию или проводит атаку типа «Отказ в обслуживании»



Низкий

злоумышленник осуществляет сбор информации о системе и проводит атаку на пользователей или осуществляет перебор логинов к системе



Информационный

злоумышленник осуществляет сбор дополнительной информации о системе



КАКИЕ УЯЗВИМОСТИ НАХОДИЛИ



Межсайтовая подделка запроса

Возможность перебора кода аутентификации

Возможность перебора имен пользователей

Слабая парольная политика

Некорректная настройка CORS

Сессионный токен в локальном хранилище

Отсутствие HTTP заголовка X-Frame-Options

Некорректная настройка механизма управления сессиями.



Требования к конфиденциальности и хранению данных

Требования к криптографии

Требования к аутентификации и управлению сессиями

Требования к сетевому взаимодействию

Требования к устойчивости к атакам на стороне клиента

Требования к взаимодействию с операционной системой

Требования к качеству кода и настройкам сборки

КАКИЕ УЯЗВИМОСТИ НАХОДИЛИ



Отсутствие проверки PIN кода и хранение незашифрованных API ключей на локальном устройстве

Возможность получения легального имени пользователя при использовании функции восстановления пароля

Удаленный сервер не осуществляет проверку подлинности клиента

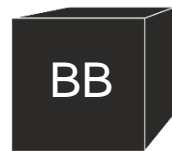
Наличие чувствительных данных в памяти

Некорректное управление cookie и хранение чувствительных данных

Уязвимость механизма отслеживания установленного приложения

Факты сохранения чувствительных данных на устройство в папку приложения и разделяемые папки

СЕРВИСЫ ВНЕШНЕГО ПЕРИМЕТРА



разведка



эксплуатация потенциальных уязвимостей



пост-эксплуатация потенциальных уязвимостей

КАКИЕ УЯЗВИМОСТИ НАХОДИЛИ



CVE-2019-0708 (Bluekeep)

Устаревшая версия Apache

Возможность перебора имен пользователей

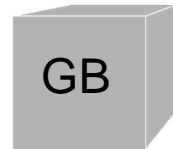
Хранимая XSS

Использование устаревших протоколов SSL/TLS

Отсутствие HTTP заголовка X-XSS-Protection

Создание пользователя в Bitrix

Отсутствие HTTP заголовка X-Content-Type-Option



исследование возможности компрометации доменной сети

исследование возможности компрометации АРМ сотрудников

исследование возможности компрометации беспроводной сети

КАКИЕ УЯЗВИМОСТИ НАХОДИЛИ



Доступ к сети Active Directory без учетной записи

Local Privilege Escalation

Oracle TNS poison

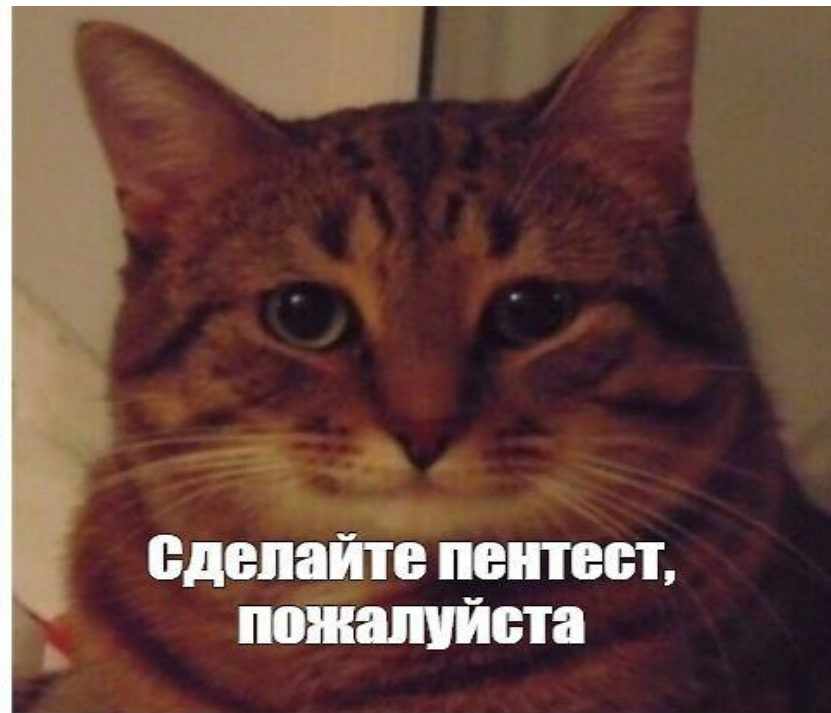
Включены протоколы LLMNR/NBT

Local File Inclusion

Дефолтная учетная запись Cisco OfficeExtend Access Point



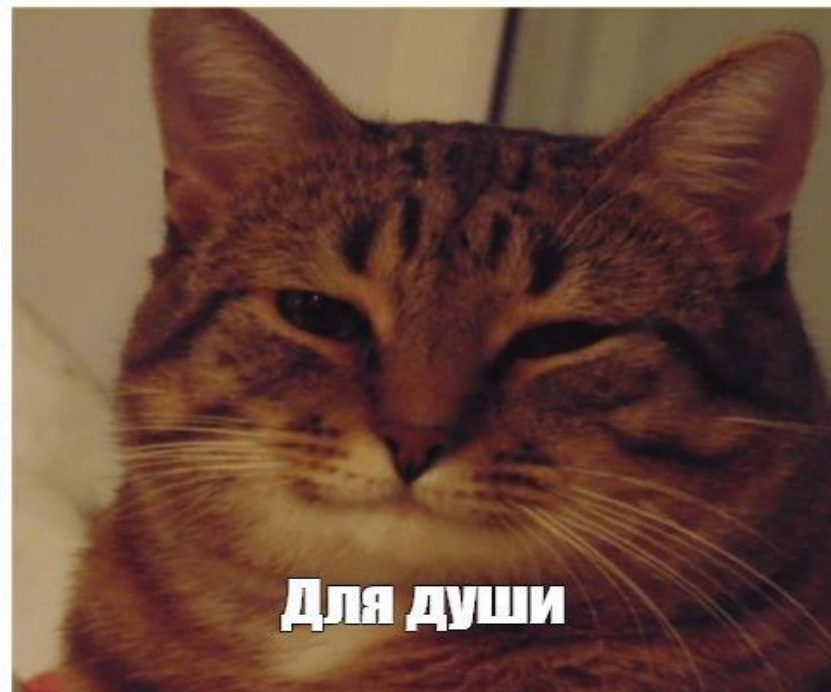
Здрасьте



**Сделайте пентест,
пожалуйста**



**Вам "для галочки" или
"для души"?**



Для души





Каргина Татьяна

Менеджер по работе с заказчиками
компании «Перспективный мониторинг»

Tatiana.Kargina@amonitoring.ru



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

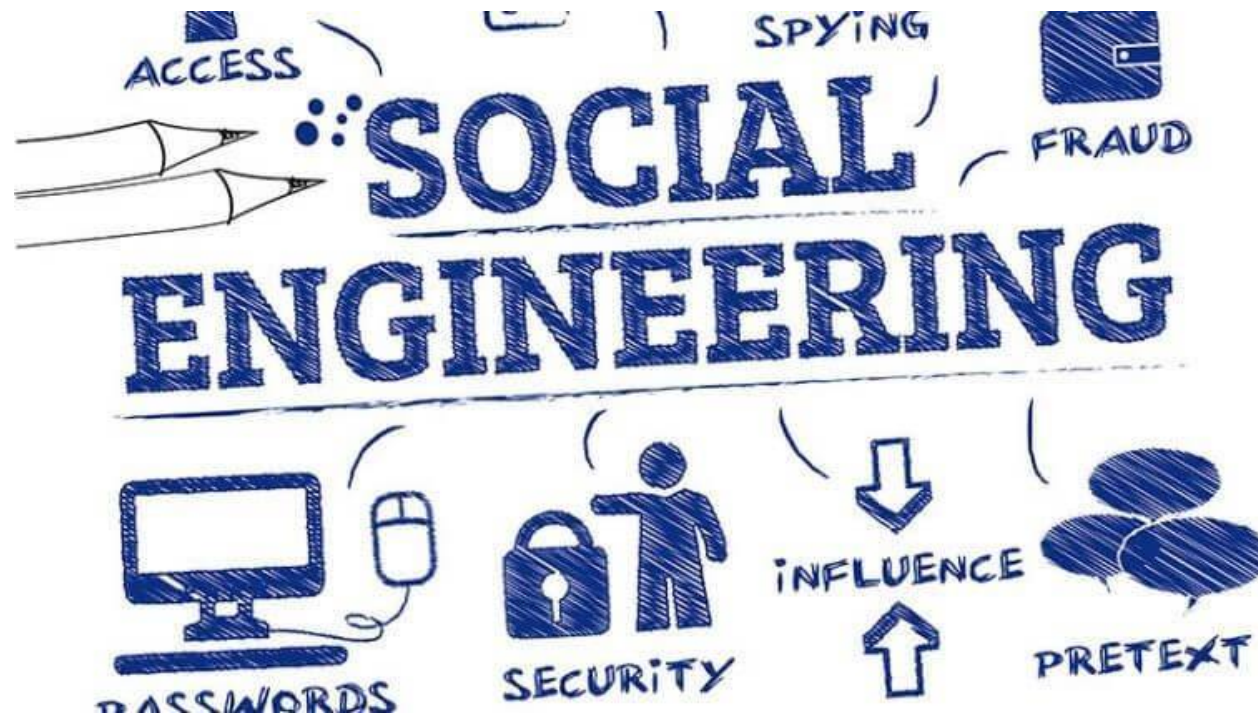
Социальная инженерия — главная угроза клиентам.

Основные актуальные техники обмана и методы противодействия.

Академическое определение



Психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.



Определение с точки зрения злоумышленников



Обман, обман и еще раз обман





За март 2021 г. зарегистрировано преступлений с [применением](#):

- 85 772 – сети «Интернет»
- 54 179 – средств мобильной связи
- 44 506 – пластиковых карт
- 11 226 – компьютерной техники
- 2 840 – программных средств
- 549 – фиктивных электронных платежей

По оценкам некоторых отделов МВД Москвы, на дистанционные мошенничества приходится до 90% всех случаев общеуголовного мошенничества, согласно отчетам районных МВД. А на кражи с банковских счетов — до половины всех [краж](#).



Один районный ОМВД одного из городов-миллионников.

За три месяца 2021 года в ОМВД поступило 102 заявления о мошеннических действиях.

Из них:

23 – получение кредитов третьими лицами

(в т.ч. с согласия потерпевшего, полученного путем обмана)

17 – звонок от имени сотрудников банка



Претекстинг – первоначальный сбор информации о жертве

Варианты:

- Покупка баз данных, похищенных из финансовых организаций
- Покупка массивов информации, утекших из государственных органов
- Предварительный «обзвон» по случайной выборке телефонных номеров
- Обход домов в поисках жертвы

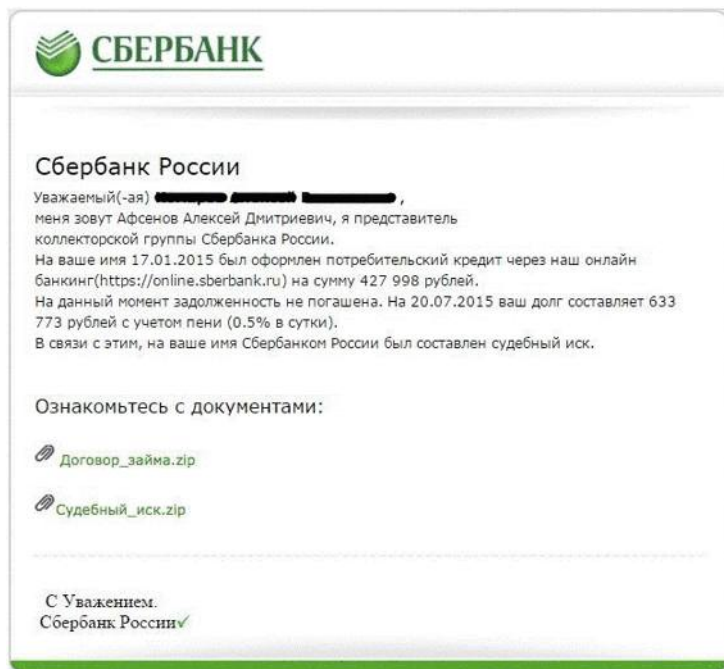


Фишинг. Поддельное отправление, с помощью которого достигается основная цель рассылки – переход на мошеннический ресурс или просто перевод денег по реквизитам мошенника.

Вишинг. Обман жертвы при общении по телефону.



Письма «под Госуслуги», банки, ПФР, МВД, ФССП, ФНС и любой другой набор букв



Информационное письмо

Федеральная служба судебных приставов
кому: мне

Сергей Александрович!

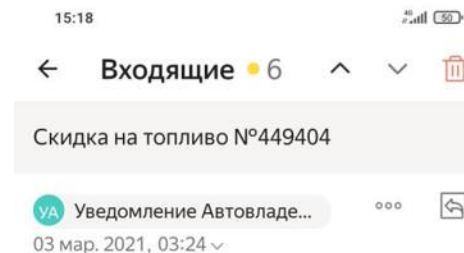
Ввиду того, что уведомить вас посредством почтовой связи, телефонии и СМС не представляется возможным, в соответствии с п.1 ст. 147 Гражданско-процессуального кодекса РФ (ГПК РФ) N 138-ФЗ от 14.11.2002 г. в настоящем письме исполнитель извещает вас о начале предварительного судебного производства по [иску о неисполнении кредитного обязательства](#).

Поскольку ваша финансовая задолженность не была урегулирована в добровольном порядке, мы вынуждены прибегнуть к принудительным мерам взыскания: направлению выездных групп по адресу регистрации, судебному разбирательству, иницированию исполнительного производства до полного погашения задолженности.

Информацию о ходе предварительного судебного производства и сроках рассмотрения, включая копию искового заявления, прилагаем.

Управление организации дознания
ФССП России

Приложение 1. [Копия искового заявления](#)



Нажмите кнопку "Включить",
чтобы активировать письмо.

госуслуги [Перейти на портал](#)

Здравствуйтесь!

В соответствии с изменениями в законодательстве утверждено постановление №78523/34/983799-ИП от [2021-03-01](#) "О топливных компенсациях владельцам транспортных средств", исполнительный приказ № 2-430/2021-231 от [2021-03-02](#).

Предоставляется скидка 50% на приобретение топливной карты



Обман по телефону под видом сотрудника службы безопасности банка, правоохранительных органов, государственных структур



Противодействие





- Информирование граждан
- Повышение осведомленности сотрудников финансовых организаций
- Организация немедленного реагирования на новые мошеннические схемы
- Взаимодействие правоохранительных структур и банковских организаций
- Технические меры противодействия утечкам данных граждан
- Проведение тренировочных мероприятий по детектированию и отражению атак на информационную инфраструктуру
- Мониторинг сети Интернет, направленный на выявление мошеннических ресурсов

Выполнение рекомендаций ЦБ (3-МР от 19.02.2021)



	****банк	****банк	****банк	****банк	****банк
Размещение информации в приложениях ДБО	0	0	0	0	0
Размещение информации в банкоматах	0	0	0	0	0
Размещение информации на сайтах	-	-	-	-	+
SMS информирование	0	0	0	0	0
Включение информации в рекламные материалы	0	0	0	0	0
Размещение информации в Интернете и соцсетях	в записи от конца 2020	-	-	+	-
Размещение информации в офисах	0	0	0	0	0
Информирование при звонке в колл-центр	-	-	-	-	-



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!

Александр Новиченко

Руководитель направления OSINT

Aleksandr.Novichenko@amonitoring.ru



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Практические аспекты оценки соответствия требованиям защиты информации Банка России

Алексей Глазков

Руководитель обособленного подразделения

«Перспективный мониторинг» в г. Пенза

Нормативные акты Банка России по защите информации



- **Положение Банка России от 17 апреля 2019 г. № 683-П** «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»
- **Положение Банка России от 4 июня 2020 г. № 719-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»
- **Положение Банка России от 23 декабря 2020 г. № 747-П** «О требованиях к защите информации в платежной системе Банка России»
- **Положение Банка России от 17 апреля 2019 г. № 684-П** «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»



Требования	Вступление в действие	Периодичность
Проведение оценки соответствия требованиям ГОСТ Р 57580.1 (№ 683-П, № 719-П)	01.01.2021 (третий уровень соответствия) 01.01.2022 (четвертый уровень соответствия)	Один раз в два года
Тестирование на проникновение (683-П, 719-П)	01.06.2019	Ежегодно
Проведение оценки соответствия требованиям ГОСТ Р 57580.1 (№ 747-П)	01.07.2021 (уровень соответствия не установлен) 01.01.2023 (четвертый уровень соответствия)	Один раз в два года
Сертификация / оценка соответствия ОУД4 прикладного ПО (719-П)	01.01.2022	По факту выпуска обновлений сертифицируемого прикладного ПО
Проведение оценки соответствия требованиям ГОСТ Р 57580.1 (№ 684-П)	01.01.2022 (третий уровень соответствия) 01.07.2023 (четвертый уровень соответствия)	Один раз в год (для усиленного уровня ЗИ) Один раз в три года (для стандартного уровня ЗИ)

Область оценки ГОСТ Р 57580.1



Для **кредитных организаций** область оценки требованиям ГОСТ Р 57580.1 в области действия № 683-П и № 719-П, как правило, **одинакова!!!**

Оценку требованиям ГОСТ Р 57580.1 в области действия **№ 747-П** отдельно проводить экономически **нецелесообразно!!!**

Целесообразно!!!

Оценка требованиям ГОСТ Р 57580.1 в области действия № 683-П, № 719-П, 747-П!!!

683-П, 719-П

- АБС и ДБО
- АРМ пользователей АБС и ДБО
- АРМ администраторов АБС и ДБО
- сетевое оборудование
- контроллер домена

747-П

- АРМ КБР-Н + АБС

Правила платежных систем

- АРМ взаимодействия с платежными системами

Приказ Минкомсвязи России от 25.06.2018 № 321

- инфраструктура ЕБС

Что еще включить в состав работ?



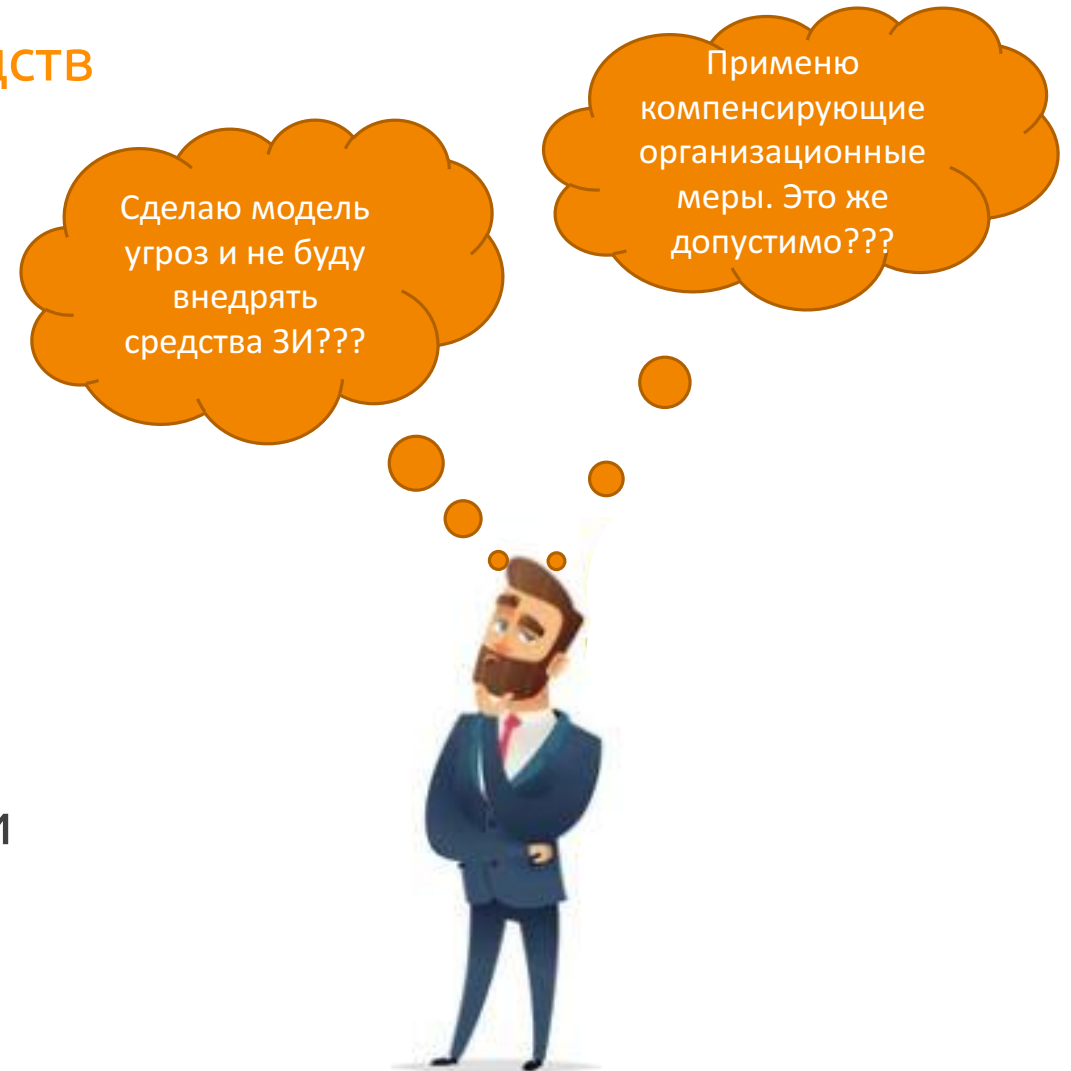
Целесообразно в состав работ включить оценку реализации технологических мер защиты информации и требований к применению СКЗИ!

Что необходимо для хорошей оценки?



Внедрение и применение технических средств защиты информации

- Система управления доступом
- Система учета информационных активов
- Антивирусные средства
- Средства межсетевого экранирования
- Средства обнаружения (предотвращения) вторжений
- Система мониторинга событий ЗИ
- Система управления инцидентами
- Система защиты платформ виртуализации
- Сканер уязвимостей
- Система управления мобильными устройствами



Что необходимо для хорошей оценки?



Документировать процессы ЗИ

- Разработать и ввести в действие внутренние нормативные документы для всех процессов ЗИ
- Определить область действия документов
- Регламентировать все организационные и технические меры защиты информации
- Определить в документах соответствие нормативным актам Банка России в области ЗИ и ГОСТ Р 57580.1

На что обратить внимание?



- Высокий уровень интеграции деятельности подразделений ИТ и ИБ
- Усиление контрольных функций Службы ИБ, в том числе, в области мониторинга ЗИ
- Повышение квалификации по всем процессам защиты информации
- Повышение осведомленности по всем процессам защиты информации
- Документальная фиксация всех решений по улучшению защиты информации
- Приобретение «коробочных» АБС и ДБО не отменяет требований к жизненному циклу автоматизированных систем

Аутсорсинг ИТ/ЗИ



Использование аутсорсинга ИТ/ЗИ не отменяет необходимости выполнения требований по защите информации

- Договор с поставщиком услуги содержит требование о проведении поставщиком оценки соответствия по требованиям ГОСТ Р 57580.1
 - Поставщик на периодической основе отчитывается о качестве оказания услуги
 - Поставщик услуги проходит оценку соответствия в области оказания услуги и предоставляет отчет потребителю услуг
 - При проведении оценки соответствия потребитель услуги предоставляет отчет проверяющей организации
- Договор с поставщиком услуг содержит детальные требования ЗИ на основе требований ГОСТ Р 57580.1
 - Поставщик на периодической основе отчитывается о качестве оказания услуги
 - Договор содержит требования о предоставлении всей необходимой информации при проведении контрольных мероприятий
 - Потребитель услуги имеет оперативный доступ к отчетной информации по потребляемой услуге
 - При проведении оценки соответствия потребитель услуги запрашивает у поставщика услуги требуемую информацию



Спасибо за
внимание!

Алексей Глазков

Руководитель обособленного
подразделения в г. Пенза

компании «Перспективный мониторинг»

Aleksey.Glazkov@amonitoring.ru

Вопросы



Сергей Нейгер

Директор по развитию бизнеса

Sergey.Neyger@amonitoring.ru

Алексей Глазков

Руководитель обособленного подразделения в г. Пенза

Aleksey.Glazkov@amonitoring.ru

Александр Новиченко

Руководитель направления OSINT

Aleksandr.Novichenko@amonitoring.ru

Татьяна Каргина

Менеджер по работе с заказчиками

Tatiana.Kargina@amonitoring.ru