ЧТО ГРЯДУЩЕЕ НАМ ГОТОВИТ: ИЗМЕНЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ БАНКА РОССИИ

Сергей Канивец
Ведущий консультант

ДиалогНаука

…ПОГОВОРИМ:

- про ГОСТы
- про Пшки
- о проектах и немного о вступивших изменениях

…ПОГОВОРИМ:

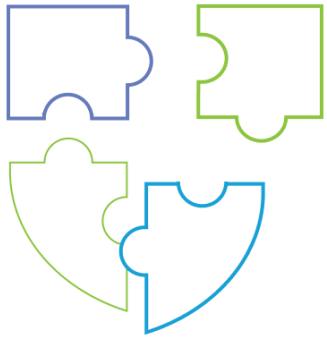
- про ГОСТы
- про Пшки
- о проектах и немного о вступивших изменениях

…НЕ ПОГОВОРИМ:

- о других ГОСТах
- о других Пшках
- об Ушках
- об МРках

ПРО ГОСТ .1

1. Общие требования
2. Термины
3. Процессы системы ЗИ
4. ЖЦ АС
5. Направления ЗИ



1 **Общие требования**

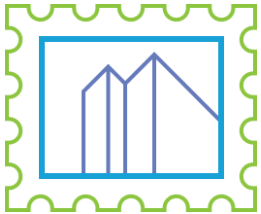
2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

- Изменена область применения стандарта – теперь + иностранные банки и лица, оказывающие проф.услуги на фин.рынках (БКИ, КРА, Аудиторские организации)
- Убрали приложение Б (про орг. меры при обработке ПДн)
- Установлена необходимость фиксации в ВНД выбора мер ЗИ, который включает в себя:
  - ✓ порядок применения мер;
  - ✓ состояние их реализации;
  - ✓ сроки реализации;
  - ✓ обоснование исключения/добавления



- Установлена возможность объединять объекты ИИ в 1 контур безопасности (но…)

1 Общие требования

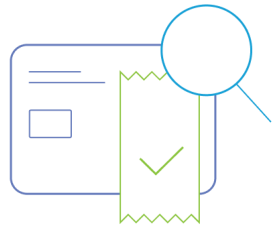
2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

- Нивелирована избыточность терминов вокруг объектов инфраструктуры – теперь там же объект ИИ
- АРМ пользователей/эксп.персонала ➔ физ. АРМ пользователей/ эксп.персонала (в т. ч. устройства, с которых осуществляется УД)



- К объектам доступа добавлены мобильные устройства
- К ресурсам доступа добавлены СУБД, ОС, средства контейнеризации и контейнеры
- Добавлены новые термины, в частности: мобильное устройство, машинный носитель информации, терминальный режим работы, контейнеры

1 Общие требования

2 Термины

3 **Процессы системы ЗИ**

4 ЖЦ АС

5 Направления ЗИ

Процесс 1

- Добавлены меры в отношении технич. УЗ
- Декомпозиция мер про регистрацию событий и контроль действий
- Исключены программные сервисы из мер про множественную аутентификацию и прерывание сессии
- Временный пароль можно передавать в открытом виде
- Пароль пользователей – 10 символов
- Хранение паролей в менеджерах
- Декомпозиция мер про контроль состава ИТ-активов и их корректного размещения
- Добавлены меры про резервное копирование

1 Общие требования

2 Термины

3 **Процессы системы ЗИ**

4 ЖЦ АС

5 Направления ЗИ

Процесс 2

- Уточнили, что при взаимодействии теста и прода из требования можно исключить средства централизованного управления и мониторинга
- Перенесли меры в/из другие(-х) процессы(-ов)

1 Общие требования

2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

Процесс 3

- Выявление уязвимостей как Т так и О
- Регламентируется порядок и сроки устранения уязвимостей
- Уязвимости должны устраняться для 4 ур
- В перечень объектов, в отношении которых проводится поиск уязвимостей добавлены мобильные устройства
- В отношении МУ – контроль состава и исключение установки и запуска ПО

1 Общие требования

2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

Процесс 4

- В меру про гипервизоры добавили «и/или на уровне ВМ»
- СЗИ ВВК требуются теперь и для мобильных устройств

1 Общие требования

2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

Процесс 5

- Уточнили, что взаимодействие с сетью Интернет предполагает в т.ч. передачу информации с использованием мессенджеров, средств аудио/видео связи, средств удаленного управления – все, что работает через Интернет
- Уточнили, что контентный анализ должен осуществляться в отношении графических файлов (OCR)
- Убрали требование к маркировке МНИ

1 Общие требования

2 Термины

3 **Процессы системы ЗИ**

4 ЖЦ АС

5 Направления ЗИ

Процесс 6

1 Общие требования

2 Термины

3 **Процессы системы ЗИ**

4 ЖЦ АС

5 Направления ЗИ

Процесс 7

- Теперь это и про контейнеризацию и терминальный режим работы приложений и рабочих мест
- Доступ с использованием одной аутентификационной информации не к 1 ВМ, а к группе. Пред. редакция – к VDI
- СЗИ можно размещать не только на физике, но и в виртуализации (но…)
- Ну и про контейнеры:
  - ✓ запрет рута;
  - ✓ запрет использования хостовой ОС для иных целей;
  - ✓ запрет размещения одного хоста в разных контурах безопасности;
  - ✓ ограничение на использование устройств и МНИ в контейнерах;
  - ✓ ограничение ресурсов ПО;
  - ✓ изоляция пространства имен;
  - ✓ поиск уязвимостей в контейнерах;
  - ✓ + все те же меры про регистрацию

1 Общие требования

2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

Процесс 8

- Выделить отдельные сегменты для размещения объектов и ресурсов доступа, предназначенных для подключения устройств УД
- Добавлены требования к системе централизованного управления для устройств для УД
- Регистрация операций, связанных с осуществлением сеанса УД
- Необходимость закрепления устройств за работниками
- Необходимость шифрования информации на устройствах

1 Общие требования

2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 Направления ЗИ

ЖЦ АС

- Убрали ОУД?
- Добавлено требование об устранении уязвимостей по установленным правилам (на этапе ввода в эксплуатацию и на этапе эксплуатации)

1 Общие требования

2 Термины

3 Процессы системы ЗИ

4 ЖЦ АС

5 **Направления ЗИ**

Планирование

- Синхронизация с «выбором» мер

Реализация

- Уточнили РЗИ.3 про контроль на соответствие требованиям на этапе ввода в эксплуатацию
- Уточнили про СКЗИ – теперь одна мера для всех (без классов)

Контроль

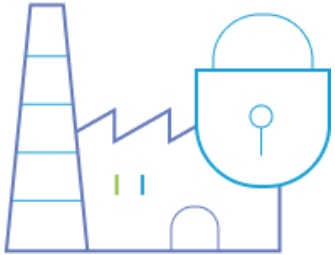
- Контроль активов – в т.ч. их размещения
- Контроль полноты тех. мер Т ➔ О

Совершенствование

- Обнаружение недостатков по результатам оценки выполнения требований

ПРО ГОСТ .2

1. Общие требования
2. Компенсирующие меры
3. Оценка
4. Нарушения
5. Отчет



1 **Общие требования**

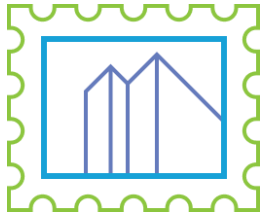
2 Компенсирующие меры

3 Оценка

4 Нарушения

5 Отчет

- Уточнены термины, в т.ч. проверяющая организация в части интерпретации независимости
- Уточнение оценки 0 и 1:
  - ✓ 0 - при отсутствии свидетельств *выбора, состояния, срока и порядка применения выбранных мер,* отсутствия тех. возможности, необоснованного превышения сроков, невозможности обеспечения условий)
  - ✓ 1 - выбрана (при предъявлении свидетельств выбора в виде фактического применения)



1 Общие требования

2 Компенсирующие меры

3 Оценка

4 Нарушения

5 Отчет

Вводится форма обоснования компенсирующей меры

Условное обозначение, номер и содержание меры ЗИ

Документ, утверждающий компенсирующую меру ЗИ

Обоснование применения:

1. Текущая реализация меры ЗИ
2. Ограничения, препятствующие выполнению исходной меры ЗИ
3. Угроза ЗИ, на нейтрализацию которой направлена исходная мера ЗИ
4. Способ (описание) нейтрализации угрозы ЗИ
5. Описание компенсирующей меры ЗИ
6. Проверка реализации компенсирующей меры ЗИ (корректности реализации)
7. Процесс соблюдения применения компенсирующей меры ЗИ (зафиксирован процесс реализации)

1 Общие требования

2 Компенсирующие меры

3 **Оценка**

4 Нарушения

5 Отчет

- Уточнена шкала для итоговой оценки – та же, что и для процессов
- Устранен пробел с расчетом оценки соответствия по процессам для одинаковых контуров безопасности
- Уточнен порядок расчета итоговой оценки для нескольких контуров безопасности
- Изменены формы таблиц для отражения результатов оценки
- Уточнили, что оценка снижается на 0,01 за каждый выявленный пункт из перечня указанных нарушений (было за каждый выявленный факт нарушения)

1 Общие требования

2 Компенсирующие меры

3 Оценка

4 **Нарушения**

5 Отчет

Добавлено 4 новых вида нарушения:

- ✓ Не проведение или некорректное проведение (без обоснования границ и модели нарушителя) тестирования на проникновение и анализа уязвимостей.
- ✓ Отсутствие реализации требований к безопасности удаленного доступа, мобильных (переносных) устройств.
- ✓ Выявление на момент проверки отсутствия фактов реализации выбранных и запланированных к реализации мер ЗИ (для каждой установленной меры).
- ✓ Неустранение уязвимостей критичного и высокого уровня в установленные сроки

1 Общие требования

2 Компенсирующие меры

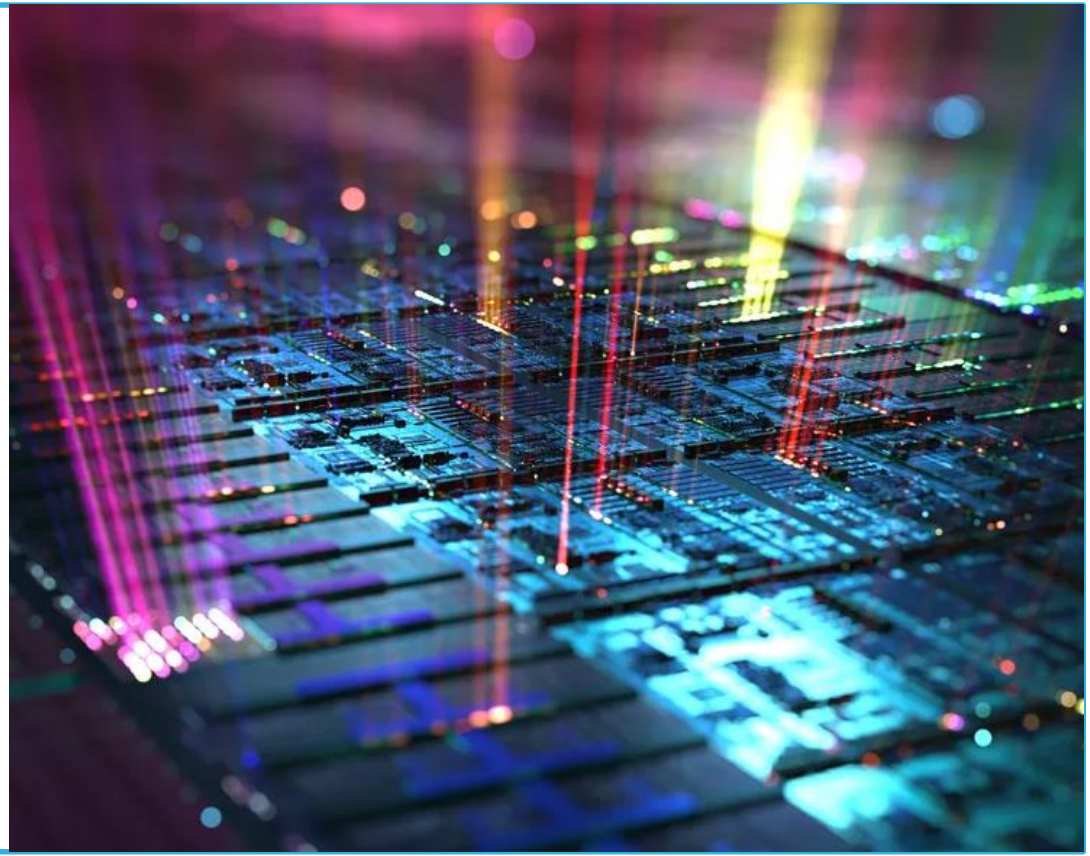
3 Оценка

4 Нарушения

5 **Отчет**

- Обновлено содержимое отчета – добавлено:
  - ✓ перечень областей оценки соответствия ЗИ, в которых возможен конфликт интересов;
  - ✓ перечень услуг, предоставленных за 3 года, или предоставляемых проверяемой организации с обоснованием отсутствия конфликта интересов
- Добавлена возможность передачи отчета в электронном виде, снабженном УКЭП
- Убрали необходимость подписания каждого свидетельства – вынесли в конец процесса/подпроцесса

ПРО иные ГОСТы



1

ГОСТ .5

- Обеспечение операционной надежности. Методика оценки соответствия ГОСТ. 4

1 ГОСТ .5

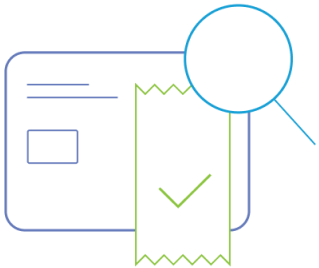
- Обеспечение операционной надежности. Методика оценки соответствия ГОСТ. 4

2 ГОСТ .X

- Требования к проверяющим организациям и руководящие указания по проведению оценки соответствия
- СТО – Оказание услуг по оценке соответствия требованиям ИБ (2023)
  - ✓ Требования к проверяющей организации;
  - ✓ Требования к лицам, входящим в проверяющую группу;
  - ✓ Требования к процессу оценки соответствия

ПРО 851-П

с 01.10



- Регистрация действий клиентов:
  - ✓ дата и время начала и окончания соединения сессии;
  - ✓ идентификатор устройства;
  - ✓ идентификационная информация для адресации АС, ПО;
  - ✓ географическое местоположение устройства (при наличии)
- Применение сертифицированных средств ЭП и УЦ для УНЭП (как для обеспечения целостности, так и для подтверждения составления ЭС уполномоченным лицом)
- Прием заявлений клиентов:
  - ✓ через мобильные приложения о каждой операции без согласия (для справки, прил.1);
  - ✓ о случаях недобровольного зачисления наличных на банковские счета третьих лиц с использованием преобразованных данных платежной карты посредством банкоматов или иных технических устройств

ПРО проект 821-П

- Гармонизация с 851-П
- Переводы ДС с использованием БПДн
- Применение ГЛОНАСС при регистрации событий (в т.ч. резервирование инфраструктуры + ГОСТ .1, установлен лимит расхождения в секундах)
- Сроки информирования Банка России о выявленных инцидентах ЗИ
- Утверждены/уточнены требования к отчетности для субъектов
- Изменения технологических участков для БПА и ОУПИ (ОЦ)
- Проведение работ по ОУД4 при внесении изменений в исходный текст
- Право не проводить сертификацию ПО или оценку по ОУД4 в случае если будет сертификация процессов разработки по ГОСТ 56939-2024

Спасибо за внимание

?