СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНОГО И МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Начальник 2 управления ФСТЭК России
Лютиков Виталий Сергеевич

ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ, КОТОРЫЕ ВНОСЯТСЯ В ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, УТВЕРЖДЕННЫЕ ПРИКАЗОМ ФСТЭК РОССИИ ОТ 11 ФЕВРАЛЯ 2013 г. № 17

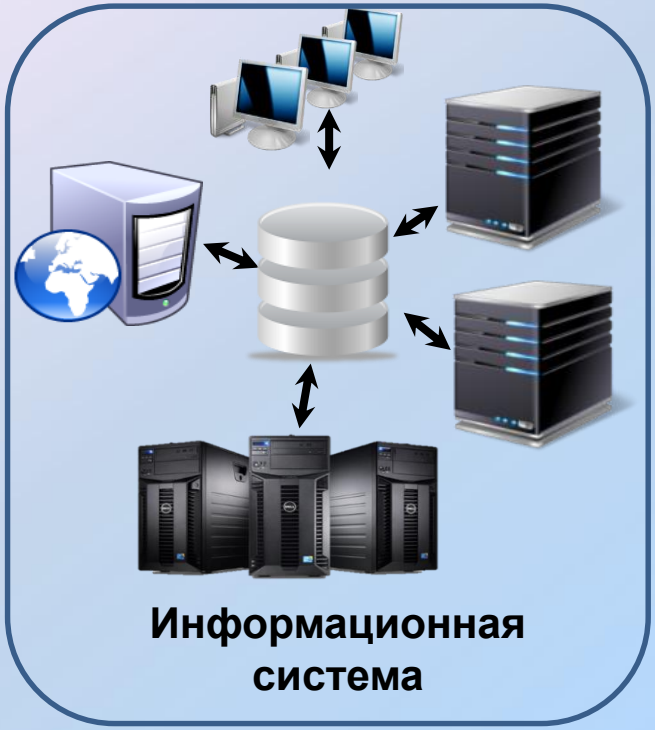
Действующая редакция	Новая редакция
Определение угроз безопасности на стадии формирования требований	Определение угроз безопасности информации – на стадии разработки системы защиты информации
Разрабатываемые организационно-распорядительные документы	Добавляется 5 новых документов, определяющих правила и процедуры (политики) защиты информации
Классы защищенности информационной системы	Устанавливается 3 класса защищенности информационной системы (самый низкий – 3, самый высокий - 1)
Состав мер защиты информации	Дополняется 9 новыми группами мер состав мер защиты информации

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

- Идентификация и аутентификацию субъектов доступа и объектов доступа
- Управление доступом субъектов доступа к объектам доступа
- Ограничение программной среды
- Защита машинных носителей информации
- Регистрация событий безопасности
- Антивирусная защита
- Обнаружение (предотвращение) вторжений
- Контроль (анализ) защищенности информации
- Целостность информационной системы и информации
- Доступность информации
- Защиту среды виртуализации
- Защита технических средств
- Защита информационной системы, ее средств, систем связи и передачи данных

- **Управление потоками информации**
- **Защита информации при использовании мобильных устройств**
- **Безопасная разработка программного обеспечения**
- **Управление обновлениями программного обеспечения**
- **Планирование мероприятий по обеспечению защиты информации**
- **Информирование и обучение персонала**
- **Анализ угроз безопасности информации и рисков от их реализации**
- **Выявление инцидентов и реагирование на них**
- **Управление конфигурацией информационной системы и ее системы защиты информации**

СООТВЕТСТВИЕ КЛАССА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И КЛАССА ЗАЩИТЫ СЗИ



Информационная система

Класс защищенности информационной системы	Класс защиты СЗИ
1	4
2	5
3	6

В информационных системах всех классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей

АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В соответствии с пунктами 14.3, 16.6 и 17.1 Требований о защите информации , не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17

Требования к мерам защиты информации в государственных информационных системах

Приказ ФСТЭК России от 14 марта 2014 г. № 31
«Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Методический документ ФСТЭК России (2016 год)

Меры защиты в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды

НОВЫЕ ДОКУМЕНТЫ НАЦИОНАЛЬНОЙ СИСТЕМЫ СТАНДАРТИЗАЦИИ

УТВЕРЖДЕНЫ РОССТАНДАРТОМ

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»;

ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»

НАПРАВЛЕНЫ В РОССТАНДАРТ

ГОСТ Р XXXXX-20XX «Защита информации. Защита информации при использовании технологии виртуализации. Общие положения;

ГОСТ Р XXXXX-20XX «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

ПОДГОТОВЛЕНЫ К НАПРАВЛЕНИЮ В РОССТАНДАРТ

ГОСТ Р ИСО/МЭК ТО 15446-201X «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»;

ГОСТ Р ИСО/МЭК ТО 20004-201X «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045

Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей»

Часть 2. Тестирование проникновения»

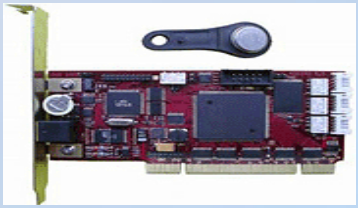
ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Утвержденные:

Требования к системам обнаружения вторжений, утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638
(12 профилей защиты к системам обнаружения вторжений)

Требования к средствам антивирусной защиты, утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28

(24 профиля защиты к средствам антивирусной защиты)



Требования к средствам доверенной загрузки, утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119

(10 профилей защиты к средствам доверенной загрузки)

Требования к средствам контроля съемных машинных носителей информации, утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87 (10 профилей защиты к средствам контроля съемных машинных носителей информации)

Требования к межсетевым экранам, утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9

ТРЕБОВАНИЯ К МЕЖСЕТЕВЫМ ЭКРАНАМ

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 9 февраля 2016 г. № 9

**Требования
к межсетевым экранам**

**Применяются
с 1 декабря 2016 г.**

- Устанавливают 5 типов межсетевых экранов
- Учитывают актуальные угрозы безопасности информации
- Предъявляют дополнительные требования доверия
- Устанавливаются требования к среде функционирования
- Учитывают современные технологии межсетевого экранирования
- Устанавливают требования по самозащите межсетевых экранов
- Предусматривают глубокий анализ протоколов при фильтрации

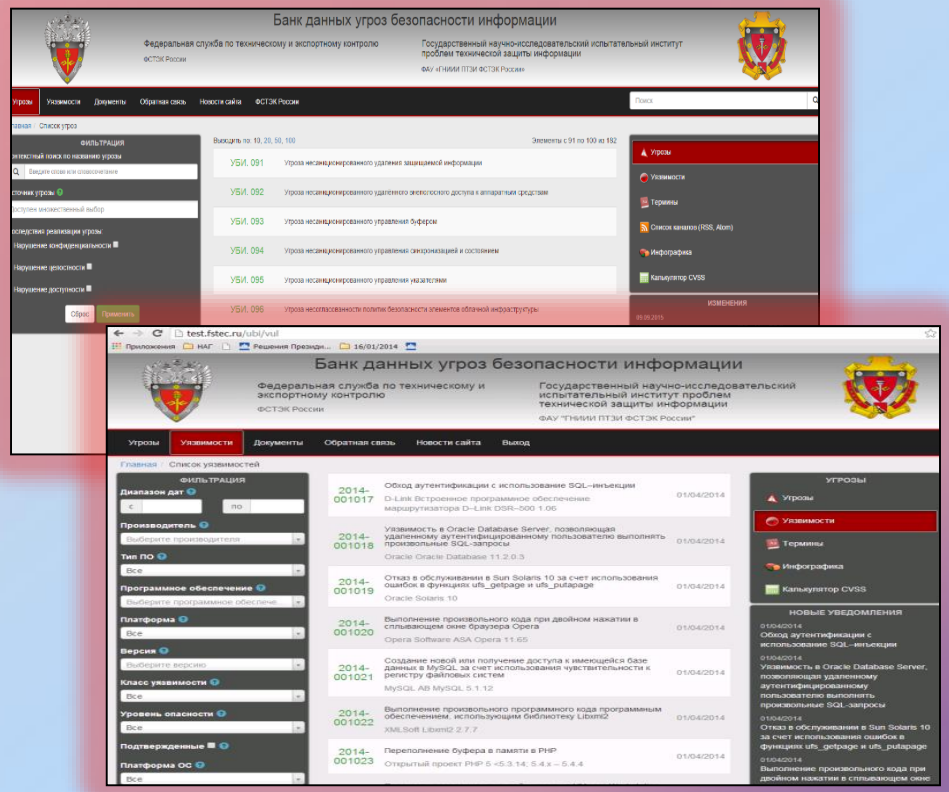
ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Разработанные, планируемые к утверждению в 2016, 2017 годах:

- Требования безопасности информации, предъявляемые к операционным системам (планируются к утверждению до 1 марта 2016 г.)
- Требования безопасности информации, предъявляемые к системам управления базами данных (планируются к утверждению до 1 марта 2016 г.)
- Требования к базовым системам ввода-вывода (BIOS)
- Требования к средствам управления потоками информации
- Требования к средствам защиты от несанкционированного вывода (ввода) информации (DLP – системам)
- Требования к средствам контроля и анализа защищенности
- Требования к средствам идентификации и аутентификации
- Требования к средствам управления доступом
- Требования к средствам мониторинга событий безопасности (SIEM)
- Требования к средствам защиты среды виртуализации

СОВЕРШЕНСТВОВАНИЕ БАНКА ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Банк данных угроз безопасности информации



Расширение функциональных возможностей:

Подписка на обновления;
Модуль статистики;
Раздел по небезопасным конструкциям кода

Развитие базы данных угроз:

Классификация угроз;
Добавление атрибутов угроз

Развитие базы данных уязвимостей:

Изменение атрибутов уязвимостей;
Исследование уязвимостей

ПРОБЛЕМНЫЕ ВОПРОСЫ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ. ПОДХОДЫ ПО СОВЕРШЕНСТВОВАНИЮ КАЧЕСТВА СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ СЕРТИФИКАЦИИ

I ЭТАП

Проверка устранения известных уязвимостей объекта и среды его функционирования

- Анализ общедоступных источников информации об уязвимостях
- Устранение уязвимостей заявителем на сертификацию в случае их выявления

II ЭТАП

Подтверждение отсутствия возможности эксплуатации потенциальных уязвимостей

- Идентификация потенциальных уязвимостей
- Разработка тестов для тестирования проникновения
- Тестирование проникновения объекта в среде функционирования

ТРЕБОВАНИЯ К ДОКУМЕНТАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЧАСТИ ИХ ПОДДЕРЖКИ

1 Конструкторская, производственная документация (технические условия, задание по безопасности) на СЗИ должны включать:

- Требования по порядку обновления сертифицируемых средств защиты
- Требования к порядку информирования потребителей об обновлении и каналу доведения обновления

2 Эксплуатационная документация (формуляр, руководства) на СЗИ должны включать:

- Источник обновления СЗИ
- Информацию о способе информирования об обновлении
- Порядок верификации и применения обновлений
- Описание способа обновления СЗИ

МЕТОДИКА АНАЛИЗА УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНОГО И МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ВОПРОСОВ ЗАЩИТЫ ИНФОРМАЦИИ

Начальник 2 управления ФСТЭК России
Лютиков Виталий Сергеевич