СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОБЛЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, НАПРАВЛЕНИЯ ПО ИХ РЕШЕНИЮ

Заместитель начальника Управления ФСТЭК России
Шевцов Дмитрий Николаевич

ИЗМЕНЕНИЯ В ФЕДЕРАЛЬНЫЙ ЗАКОН № 149-ФЗ

Проект Федерального закона
«О внесении изменений
в статью 16 Федерального закона
«Об информации, информационных технологиях
и о защите информации»

1. Установление требований о защите информации в информационных системах, в которых обрабатывается информация, обладателями которой являются государственные органы.

2. Установление обязанности операторов информационных систем:

- по созданию систем защиты информации;
- по информированию ФСТЭК России и ФСБ России о компьютерных инцидентах

Проект приказа ФСТЭК России «О внесении изменений
в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
(I квартал 2017 г.)

Методика определения угроз безопасности информации в информационных системах
(I квартал 2017 г.)

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 информации на стадии формирования требований защиты информации	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 защиты информации

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

- Идентификация и аутентификация 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
- Защита среды виртуализации
- Защита технических средств
- Защита информационной системы, ее средств, систем связи и передачи данных

- **Управление потоками информации**
- **Защита информации при использовании мобильных технических средств**
- **Безопасная разработка специального 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**

РАЗРАБОТКА МЕР ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ТП

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»

Методические документы ФСТЭК России (2017…2018 годы)

Меры 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 (2017 г.)

Методика определения угроз безопасности информации в автоматизированных системах управления технологическими процессами на критически важных объектах

Типовая модель угроз безопасности информации в автоматизированных системах управления технологическими процессами на критически важных объектах

НАЦИОНАЛЬНЫЕ СТАНДАРТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

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»

ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологии виртуализации. Общие положения»

ГОСТ Р 56939-2016 «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 20004-1-201X «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

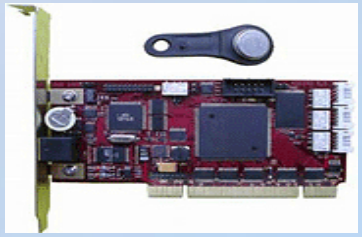
ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к системам обнаружения вторжений,
утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638

12 методических документов, содержащих профили защиты к системам обнаружения вторжений

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

24 методических документа, содержащих профили защиты к средствам антивирусной защиты



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

10 методических документов, содержащих профили защиты к средствам доверенной загрузки

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

10 методических документов, содержащих профили защиты к средствам контроля съемных машинных носителей информации

ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

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

24 методических документа, содержащих профили защиты к межсетевым экранам

Требования безопасности информации
к операционным системам,
утверждены приказом ФСТЭК России
от 19 августа 2016 г. № 119

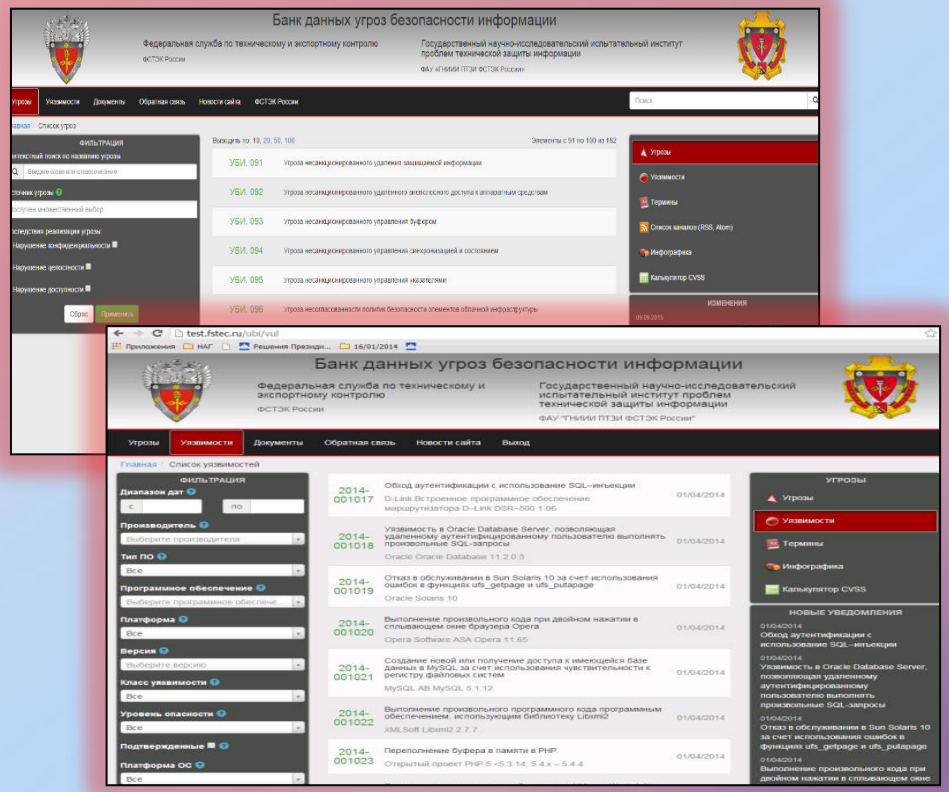
ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Разработанные, планируемые к утверждению:

- Требования безопасности информации к системам управления базами данных (готовятся к утверждению)
- Требования безопасности информации к средствам управления потоками информации (готовятся к утверждению)
- Требования к базовым системам ввода-вывода (BIOS)
- Требования к средствам защиты от несанкционированного вывода (ввода) информации (DLP – системам)
- Требования к средствам контроля и анализа защищенности
- Требования к средствам контроля целостности
- Требования к средствам ограничения программной среды
- Требования к средствам идентификации и аутентификации
- Требования к средствам управления доступом
- Требования к средствам разграничения доступа
- Требования к средствам регистрации событий
- Требования к средствам защиты среды виртуализации

СОВЕРШЕНСТВОВАНИЕ БАНКА ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Банк данных угроз безопасности информации



По состоянию на сентябрь 2016 г.

Сведения о 186 угрозах безопасности информации;

Более 14800 паспортов уязвимостей ПО

Расширение функциональных возможностей:

Пользовательские настройки;

Подписка на обновления;

Модуль статистики;

Раздел по небезопасным конструкциям кода

Развитие базы данных угроз:

Классификация угроз;

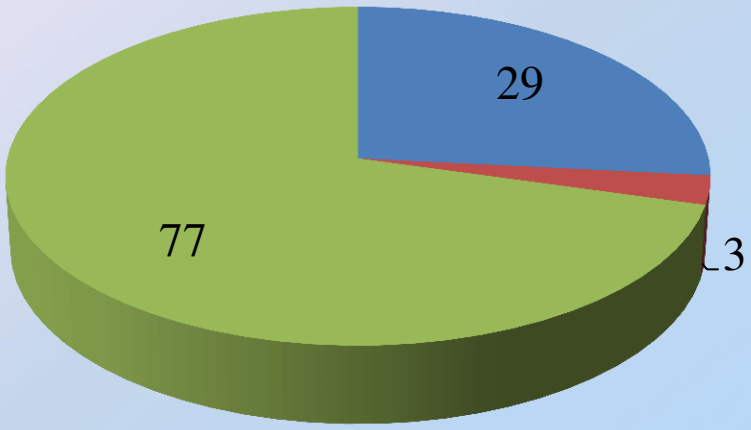
Пополнение перечня угроз

Развитие базы данных уязвимостей:

Внесение дополнительных сведений в паспорта уязвимостей;

Исследование уязвимостей

УСТРАНЕННИЕ УЯЗВИМОСТЕЙ В СЕРТИФИЦИРОВАННЫХ СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ



1. • Выявление уязвимости
2. • Информирование заявителя на сертификацию
3. • Проведение совещания с заявителем на сертификацию
4. • Разработка мер по нейтрализации уязвимости
5. • Информирование потребителей о необходимости применения разработанных мер
6. • Проведение инспекционного контроля
7. • Информирование потребителей о результатах инспекционного контроля

ПРОБЛЕМЫ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

Недостаточность требований и методических подходов по выявлению и устранению уязвимостей ПО

Отсутствие процедур безопасной разработки и поддержки ПО у отечественных разработчиков

Отсутствие процедур поддержки ПО у производителей импортного ПО

Недостаточное качество проведения работ по выявлению уязвимостей испытательными лабораториями

Отсутствие процедур по выявлению и устранению уязвимостей в информационных системах

МЕТОДИКА АНАЛИЗА УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Информационные системы создаются без учета требований по защите информации

Разработка отечественного прикладного ПО на базе импортного общесистемного ПО

Разработка общесистемного и прикладного ПО без учета имеющихся отечественных разработок

Проблема совместимости отечественного ПО

Проблема, связанная с завершением поддержки средств защиты информации

СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОБЛЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НАПРАВЛЕНИЯ ПО ИХ РЕШЕНИЮ

Заместитель начальника Управления ФСТЭК России
Шевцов Дмитрий Николаевич