Основные направления совершенствования деятельности по технической защите информации

Заместитель директора ФСТЭК России
Лютиков Виталий Сергеевич

Направления деятельности ФСТЭК России, в области технической защиты информации в 2020 году и основные проблемные вопросы, требующие решения

I. Определение угроз безопасности информации

II. Реализация требований по технической защите информации на объектах защиты

III. Сертификация средств защиты информации

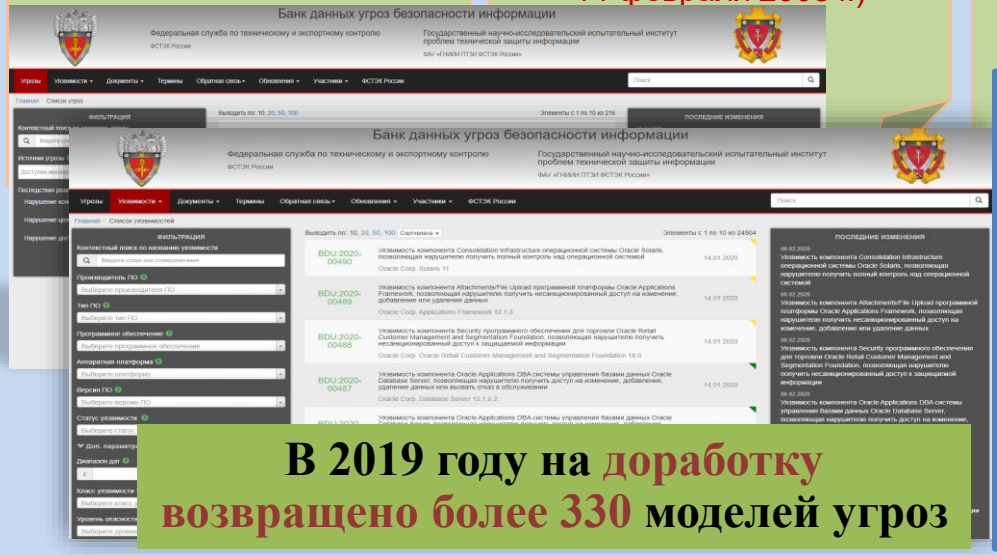
I. Определение угроз безопасности информации

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК России 14 февраля 2008 г.)

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК России 14 февраля 2008 г.)

Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена ФСТЭК России 18 мая 2007 г.)

Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена ФСТЭК России 18 мая 2007 г.)



В 2019 году на доработку возвращено более 330 моделей угроз

Количество рассмотренных моделей угроз

Количество рассмотренных документов в 2019 году увеличилось в 1,8 раза

I. Определение угроз безопасности информации

Основные недостатки

Модели угроз составляются для разработки документа, а не для проектирования системы защиты

При моделировании угроз не учитываются сценарии действий нарушителей

Система защиты информации строится без учета модели угроз

Не проводится оценка эффективности системы защиты информации относительно угроз

Задачи, требующие решения

Разработка методики моделирования угроз

Переработка перечня угроз в банке данных угроз

Повышение квалификации специалистов по защите информации по вопросам моделирования угроз

Разработка средства автоматизации моделирования угроз

Разработка механизмов оповещения об угрозах и уязвимостях информационных систем

II. Реализация требований по защите информации

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 11 февраля 2013 г. № 17

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

(в редакции приказа ФСТЭК России от 28 мая 2019 г. № 106)

Аттестация на весь срок эксплуатации системы

Усиление требований к эксплуатации системы защиты информации

Установление требования в части уровней доверия сертифицированных средств защиты информации

Установление требования по применению сертифицированных маршрутизаторов

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 21 декабря 2017 г. № 235

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

(в редакции приказа ФСТЭК России от 27 марта 2019 г. № 64)

Уточнение состава организационных и технических мер обеспечения

Уточнение порядка создания систем безопасности в филиалах (представительствах) и подчиненных организациях интегрированных структур

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 25 декабря 2017 г. № 239

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации

(в редакции приказа ФСТЭК России от 26 марта 2019 г. № 60)

Уточнение состава организационных и технических мер обеспечения

Установления требования в части уровней доверия сертифицированных средств защиты информации

Установление требования по применению сертифицированных маршрутизаторов

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 28 февраля 2017 г. № 31

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса

(в редакции приказа ФСТЭК России от 14 января 2019 г. № 5)

Запрет на обработку цифровой информации за пределами территории Российской Федерации

Изменения в нормативные правовые акты 2019 года направлены на:

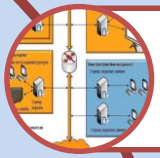
II. Реализация требований по технической защите информации

Количество рассмотренных технических заданий

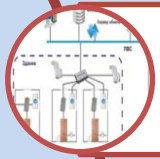
Количество рассмотренных документов в 2019 году увеличилось в 1,8 раза

В 2019 году на доработку возвращено более 127 технических задания

Основные недостатки



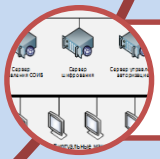
Неверно определены границы информационной системы



Не учитывается информационно-телекоммуникационная инфраструктура, на базе которой функционирует система

Низкое качество работ по аттестации (оценке эффективности) системы защиты информации

Не заданы требования к специалистам, эксплуатирующим систему защиты информации



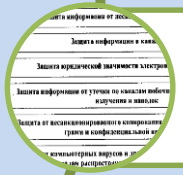
Не реализованы требования по управлению системой защиты информации

II. Реализация требований по технической защите информации

Задачи, требующие решения

Сопоставление угроз безопасности информации и мер защиты информации

Усиление мер по выявлению событий безопасности информации в информационной системе и реагированию на них



Дифференциация мер защиты информации в зависимости от архитектуры информационной системы (АРМ, ЛВС, ИТКС, ЦОД)

Разработка методического обеспечения, определяющего порядок аттестации системы

III. Сертификация средств защиты информации

Положение о системе сертификации средств защиты информации

утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55

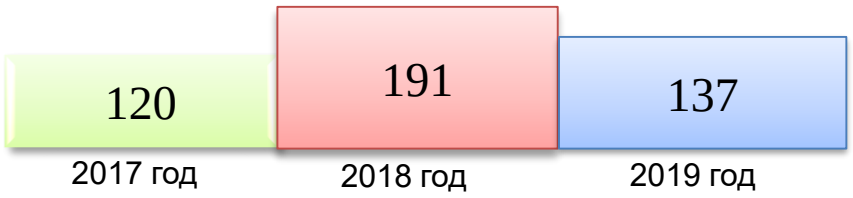
Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131

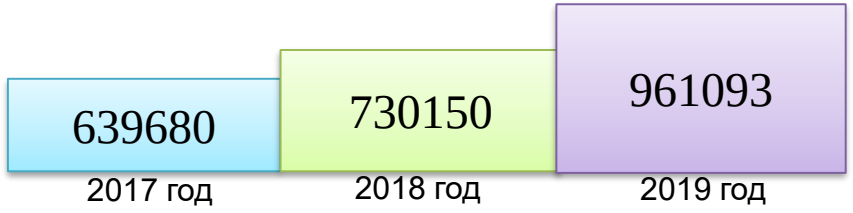
Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России 11 февраля 2019 г.

Количество сертифицированных средств защиты информации



Количество произведенных средств защиты информации



III. Сертификация средств защиты информации

Основные недостатки

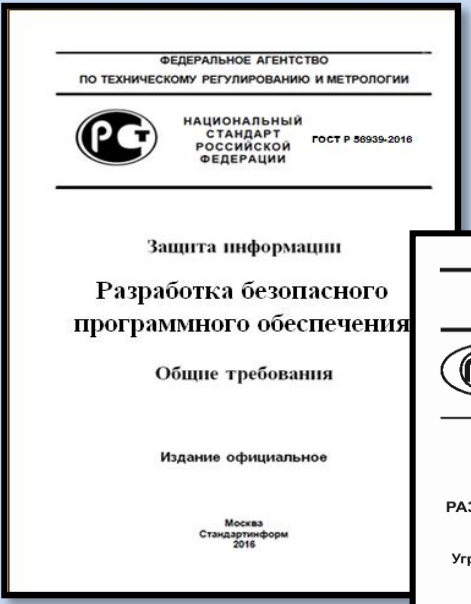
- Низкий уровень внедрения процессов разработки безопасного программного обеспечения
- Значительные сроки проведения сертификационных испытаний
- Необходимость повышения квалификации специалистов
- Отсутствие требований по безопасности информации к различным типам средств защиты информации
- Большие сроки устранения уязвимостей

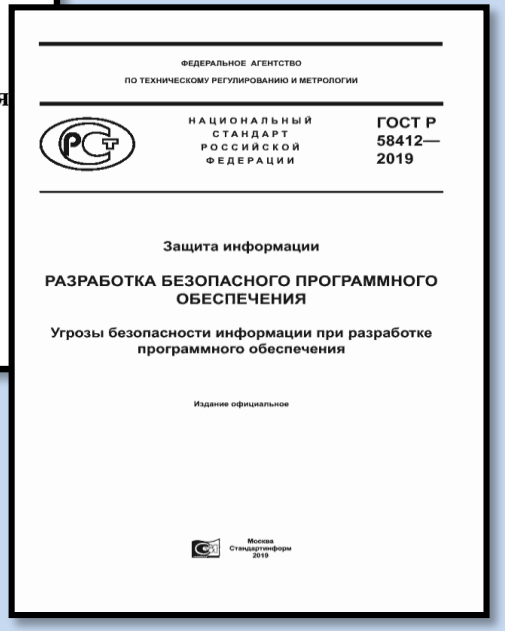
Задачи, требующие решения

- Совершенствование порядка сертификации средств защиты информации в части сроков их сертификации
- Повышение требований к специалистам испытательных лабораторий и организация работ по повышению уровня их квалификации
- Разработка и совершенствование требований к отдельным типам средств защиты информации
- Совершенствование методического обеспечения по сертификации средств защиты информации
- Внедрение стандартов по разработке безопасного программного обеспечения
- Совершенствование методики выявления уязвимостей в программном обеспечении

III. Сертификация средств защиты информации

Технический комитет 362
Подкомитет 4
Разработка безопасного программного обеспечения





ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по разработке безопасного программного обеспечения»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по оценке безопасности разработки программного обеспечения»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению статического анализа. Общие требования»
ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (пересмотр)
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Доверенный компилятор языков Си/Си++. Общие требования»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Управление безопасностью программного обеспечения при использовании заимствованных и привлекаемых компонентов»

Основные направления совершенствования деятельности по технической защите информации

Заместитель директора ФСТЭК России
Лютиков Виталий Сергеевич