Совершенствование системы сертификации средств защиты информации

Начальник управления ФСТЭК России

Шевцов Дмитрий Николаевич

Системе сертификации средств защиты информации ФСТЭК России 30 лет

Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом 27 октября 1995 г. № 199

Положение о системе сертификации средств защиты информации, утвержденное приказом ФСТЭК России от 3 апреля 2018 г. № 55

Выдано 4911 сертификатов соответствия

9 органов по сертификации

43 испытательные лаборатории

205 изготовителей средств защиты информации

1789 органов по аттестации объектов информатизации

В деятельности системы сертификации задействовано более 30 000 специалистов

В настоящее время производится **508** типов сертифицированных средств защиты информации

Ежегодно производится **2 500 000** экземпляров сертифицированных средств защиты информации

Направление совершенствования системы сертификации

Совершенствование порядка сертификации средств защиты информации

Разработка требований по безопасности информации к средствам защиты информации

Разработка методик проведения сертификационных испытаний средств защиты информации

Внедрение процессов разработки безопасного программного обеспечения средств защиты информации

Повышение уровня квалификации специалистов испытательных лабораторий и органов по сертификации, привлекаемых к сертификации средств защиты информации

Сертификация процессов разработки безопасного программного обеспечения средств защиты информации

Порядок сертификации процессов разработки безопасного программного обеспечения средств защиты информации

утвержден приказом ФСТЭК России от 1 декабря 2023 г. № 240

Количество заявок на сертификацию: 10

Количество решений: 7

Количество сертификатов: 3

Национальный стандарт ГОСТ Р 56939-2020 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

Проблемные вопросы

- **Недостаточное внимание уделяется вопросам проведения статического анализа заимствованных компонентов**
- **Недостаточное внимание уделяется вопросам обучения разработчиков СЗИ вопросам разработки безопасного ПО**
- **Формальный подход к моделированию угроз и описанию поверхности атаки**
- **Недостаточное внимание уделяется вопросам разработки документации в области разработки безопасного ПО и ее применения на практике**

Особенности сертификации средств защиты информации в системе сертификации ФСТЭК России

Упрощенный порядок реализации отдельных процедур сертификации средств защиты информации отечественного производства

от 22 января 2025 г. № 240/24/347
от 29 января 2025 г. № 240/24/421

самостоятельное проведение сертификационных испытаний в части внесения изменений в сертифицированное СЗИ продлено **до 1 июля 2025 г.**

разработчику допускается не предоставлять испытательной лаборатории (органу по сертификации) **до 1 января 2026 г.:**

- результаты идентификации и анализа скрытых каналов (пункт 20.2 Требований доверия)
- модель безопасности при сертификации средств защиты информации по 4 или 3 уровню доверия (пункт 8 Требований доверия)

Сведения об аппаратной платформе СЗИ должны быть включены в единый реестр российской радиоэлектронной продукции с **1 января 2025 г.**

Особенности сертификации СЗИ, в состав которых входят заимствованные программные компоненты с открытым исходным кодом

Порядок испытаний и поддержки безопасности средств защиты информации, в состав которых входят заимствованные программные компоненты с открытым исходным кодом

от 26 сентября 2024 г. № 240/24/4436

Выдано 4 плана испытаний на средства защиты информации

Сведения о SBOM представили: 95 организаций (47%)

Типовые недостатки выявленные при рассмотрении SBOM

Неверно определены заимствованные программные компоненты, относящиеся к поверхности атаки

Неправильно представлено описание полей объектов в части источников получения и внешних ссылок

В перечень включаются **только** заимствованные компоненты, относящиеся к поверхности атаки и реализующие функции безопасности информации

Недостатки содержались в 96% направленных перечней

Повышение безопасности СЗИ, в состав которых включены средства контейнеризации или образы контейнеров

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
о повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров

от 13 января 2025 г. № 240/24/38

- инвентаризация образов контейнеров, а также программного обеспечения из состава образов контейнеров
- обеспечение целостности образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства
- обеспечение совместимости программного обеспечения, входящего в состав образов контейнеров, с хостовыми операционными системами
- обеспечение запуска контейнеров с минимально необходимыми полномочиями
- обеспечение доступа между компонентами средства (контейнерами, микросервисами, иными ресурсами), компонентами среды функционирования, внешними по отношению к средству компонентами

Повышение безопасности СЗИ, в состав которых включены интерпретаторы, веб-сервера и сервера приложений

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
о повышении безопасности средств защиты информации, в состав которых разработчики включают интерпретаторы (компоненты среды функционирования интерпретируемых языков или языков, компилируемых в промежуточное представление), веб-сервера и сервера приложений или задействуют для реализации функциональных возможностей средств данные программные компоненты из состава среды функционирования

от 10 января 2025 г. № 240/24/39

сертификация интерпретаторов, веб-серверов и серверов приложений по требованиям безопасности информации, а также включение в технические условия несертифицированных интерпретаторов, веб-серверов и серверов приложений. Испытания по выявлению уязвимостей и недекларированных возможностей

прохождение сертификационных испытаний в составе средств в части задействования данных компонентов при реализации ФБ средств или в поверхности атаки, а также минимизация поверхности атаки

наделение компонентов интерпретаторов, веб-серверов и серверов приложений минимальными полномочиями необходимыми для функционирования, допуск к выполнению кода, а также включение в эксплуатационную документацию сведений о функциональных возможностях

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

МЕТОДИКА ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

(новая редакция)

проект

- при проведении исследований учитываются результаты реализации у разработчиков процессов разработки безопасного программного обеспечения в соответствии ГОСТ Р 56939
- определен порядок использования результатов работы Центра исследований безопасности системного программного обеспечения для сертификации объекта оценки
- введено требование о предоставлении исходного кода объекта оценки с 6 уровня контроля
- уточнена методология определения поверхности атаки объекта оценки
- введено требование о представлении информации о сторонних программных компонентах объекта оценки и проведении в их отношении композиционного анализа
- уточнены требования к проведению анализа архитектуры, статического, динамического анализа и оформлению результатов

Меры по повышению защищенности инфраструктуры разработки программного обеспечения

Письмо ФСТЭК России о мерах по повышению защищенности инфраструктуры разработки средств защиты информации

от 13 января 2025 г. № 240/24/56

- реализовать строгую идентификацию и аутентификацию работников организации в соответствии с положениями национального стандарта ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения».
- провести инвентаризацию учетных записей пользователей, внешних интерфейсов инфраструктуры организации
- реализовать сегментирование инфраструктуры организации, выделив при этом отдельно сегменты разработки, сборки, тестирования программного обеспечения, а также сегменты для хранения проектной и эксплуатационной документации, исходных кодов программного обеспечения
- обеспечить резервное копирование документации и исходных кодов программного обеспечения средств защиты информации
- организовать регулярное сканирование инфраструктуры организации на предмет наличия уязвимостей в программном обеспечении
- использовать локальные репозитории компонентов программного обеспечения, входящих в состав средств защиты информации
- отслеживать сведения об уязвимостях в программном обеспечении с открытым исходным кодом

Совершенствование требований к средствам защиты информации

Требования по безопасности информации к средствам обнаружения и реагирования уровня узла (EDR)

Требования по безопасности информации к средствам антивирусной защиты (новая редакция)

Требования по безопасности информации к межсетевым экранам (новая редакция)

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам безопасности информационных технологий (новая редакция)

Требования по безопасности информации к средствам контроля за действиями привилегированных учетных записей

Требования по безопасности информации к средствам обнаружения и реагирования уровня узла

Требования по безопасности информации к средствам обнаружения и реагирования уровня узла

(проект)

Предъявляются требования по безопасности информации к:

- уровню доверия средства обнаружения и реагирования уровня узла
- управлению доступом в средстве обнаружения и реагирования уровня узла
- идентификации и аутентификации пользователей средства обнаружения и реагирования уровня узла
- получению данных мониторинга средством обнаружения и реагирования уровня узла
- обнаружению признаков вредоносного программного обеспечения и компьютерных атак средством обнаружения и реагирования уровня узла
- реагированию средства обнаружения и реагирования уровня узла
- тестированию средства обнаружения и реагирования уровня узла
- управлению установкой обновлений (актуализации) служебных баз данных средства обнаружения и реагирования уровня узла
- регистрации событий безопасности в средстве обнаружения и реагирования уровня узла
- взаимодействию с иными средствами защиты информации
- централизованному управлению средством обнаружения и реагирования уровня узла

Разработка требований → Обсуждение с экспертами → Регистрация в Минюсте России → Вступление в силу

Реализация Требований по безопасности информации к многофункциональным межсетевым экранам уровня сети

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

утверждены приказом ФСТЭК России
от 7 марта 2023 г. № 44

Зарегистрирован Минюстом России
14 июня 2023 г. № 73832

Выдан 1 сертификат соответствия от 19 ноября 2024 г. № 4877 на программно-аппаратный комплекс «Positive Technologies Next Generation Firewall». Заявитель – АО «Позитив Текнолоджиз»

Подано 3 заявки на сертификацию

ООО «С-Терра СиЭсПи»

ООО «Русплатформа»

ООО «СИС Групп»

Проводятся работы 5 организациями - разработчиками по оценке соответствия сертифицированных средств защиты информации Требованиям

АО «ИнфоТеКС»

ООО «Код Безопасности»

ООО «СОЛАР СЕКЬЮРИТИ»

ООО «Юзергейт»

ООО «Айдеко»

Рабочая группа по решению проблемных вопросов, возникающих при проведении сертификации средств сетевой безопасности

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

утверждены приказом ФСТЭК России
от 7 марта 2023 г. № 44

Зарегистрирован Минюстом России
14 июня 2023 г. № 73832

Рабочая группа по проблемным вопросам сертификации средств сетевой безопасности

ООО «ТСС»	ООО «Фактор-ТС»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России»	
ООО «БИЗон»	АО «ИнфоТеКС»	ООО «ЦБИ»	ООО «СОЛАР СЕКЬЮРИТИ»
АО «Лаборатория Касперского»	АО «Позитив Текнолоджиз»	ООО «Юзергейт»	
ООО «Код Безопасности»	ООО «С-Терра СиЭсПи»	ООО НТЦ «Фобос-НТ»	
ООО «Айдеко»	ООО «Амикон»		

В состав рабочей группы входит 15 организаций

Проблемные вопросы при реализации Требований

- Тестирование производительности многофункциональных межсетевых экранов уровня сети
- Реализация многофункциональными межсетевыми экранами уровня сети на аппаратном уровне пакетной фильтрации сетевого трафика
- Ограничение доступа через сетевые интерфейсы к оперативной памяти аппаратных платформ
- Отсутствие взаимодействия между разработчиками типов средств защиты информации, входящих в состав многофункциональных межсетевых экранов уровня сети
- Создание единой базы тестов, содержащих описания признаков вредносного программного обеспечения и реализации компьютерных атак

Аттестация работников органов по сертификации и испытательных лабораторий

Порядок аттестации работников органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа

утвержден приказом ФСТЭК России от 27 июля 2023 г. № 147

Количество заявок на аттестацию работников - 104

Допущены к аттестации - 71 работник

Аттестовано 14 работников

Не прошли аттестацию 10 работников

Запланирована аттестация 47 работников

Аттестация работников осуществляется на материально-технической базе МГТУ им. Н.Э.Баумана

Причины отказа в аттестации работников

Несоответствие работников критериям, установленным в Порядке аккредитации ОС и ИЛ

Недостаточный уровень знаний:
Средний балл сдачи тестов менее 70%

Недостаточные практические навыки проведения:

- Динамического анализа
- Статического анализа
- Реверс-инжиниринга
- Веб-пентеста

Совершенствование системы сертификации средств защиты информации

Начальник управления ФСТЭК России

Шевцов Дмитрий Николаевич