Направления совершенствования сертификации средств защиты информации

Начальник
2 управления ФСТЭК России

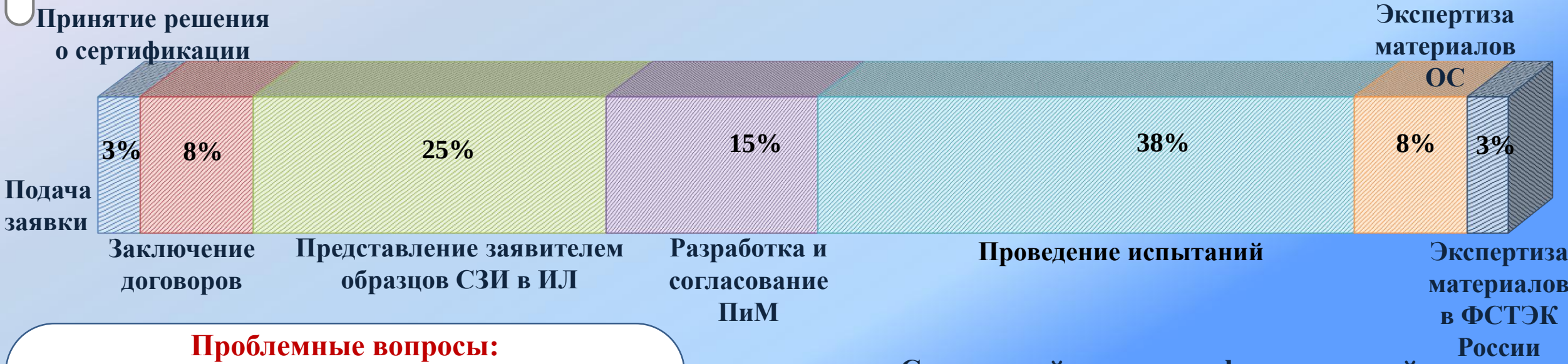
Шевцов Дмитрий Николаевич

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ СЕРТИФИКАЦИИ ФСТЭК РОССИИ

1. Совершенствование порядка сертификации (сокращение сроков сертификации)
2. Совершенствование требований по безопасности информации к средствам защиты информации
3. Аттестация экспертов органов по сертификации и испытательных лабораторий
4. Повышение безопасности системного программного обеспечения
5. Внедрение процессов безопасной разработки системного программного обеспечения средств защиты информации

СОВЕРШЕНСТВОВАНИЕ ПОРЯДКА СЕРТИФИКАЦИИ ФСТЭК РОССИИ

Приказ ФСТЭК России от 19 сентября 2022 г. № 172
«О внесении изменений в Положение о системе сертификации»
Сокращение сроков рассмотрения документов и проведения отдельных видов работ (суммарно на 105 календарных дней)



Проблемные вопросы:

- Неготовность СЗИ к сертификации.
- Использование услуг организаций-посредников.
- Отсутствие у изготовителя процедур безопасной разработки, поддержки безопасности СЗИ.

СОВЕРШЕНСТВОВАНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования по безопасности информации к средствам контейнеризации
приказ ФСТЭК России от 4 июля 2022 г. № 118
зарегистрирован Минюстом России 29 сентября 2022 г., регистрационный № 70275

Требования по безопасности информации к средствам виртуализации
приказ ФСТЭК России от 27 октября 2022 г. № 187
зарегистрирован Минюстом России 22 декабря 2022 г., регистрационный № 71774

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети
приказ ФСТЭК России от 7 марта 2023 г. № 44
зарегистрирован Минюстом России 14 июня 2023 г., регистрационный № 73832

Требования по безопасности информации к системам управления базами данных
приказ ФСТЭК России от 14 апреля 2023 г. № 64
зарегистрирован Минюстом России 15 июня 2023 г., регистрационный № 73865

Разрабатываемые документы:

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

СОВЕРШЕНСТВОВАНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

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

Требования предъявляются к:

- управлению доступом;
- идентификации и аутентификации пользователей;
- фильтрации сетевого трафика;
- обнаружению и блокированию компьютерных атак;
- обнаружению и блокированию вредоносного программного обеспечения;
- доверенной загрузке;
- тестированию и контролю целостности;
- производительности;
- аппаратной платформе;
- режимам работы;
- регистрации событий безопасности;
- обеспечению бесперебойного функционирования;
- взаимодействию с другими СЗИ;
- централизованному и удаленному управлению.

Информационная система страновой принадлежности IP-адресов

Методика тестирования производительности многофункционального межсетевого экрана уровня сети (проект)

Центр компетенций по тестированию производительности, устойчивости функционирования и функциональных возможностей межсетевых экранов и иных сетевых устройств, реализующих функции безопасности информации (Национальная программа «Национальная экономика данных»)

Необходимо привести в соответствие Требованиям в срок до 1 января 2025 г.

СОВЕРШЕНСТВОВАНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования по безопасности информации к системам управления базами данных

утверждены приказом ФСТЭК России от 14 апреля 2023 г. № 64

Требования предъявляются к:

- управлению доступом;
- идентификации и аутентификации пользователей;
- контролю целостности;
- регистрации событий безопасности;
- резервному копированию и восстановлению;
- обеспечению доступности;
- очистке памяти;
- производительности;
- ограничению программной среды.

Система управления базами данных – программное средство, реализующее функциональные возможности по созданию баз данных, манипулированию данными (вставке, обновлению, удалению, выборке), обеспечению безопасности, надежности хранения и целостности данных, администрированию баз данных, а также обеспечивающее управление доступом субъектов доступа к объектам доступа баз данных, предназначенных для хранения информации, подлежащей защите в информационной (автоматизированной) системе

В настоящее время в системе сертификации ФСТЭК России сертифицировано 15 СУБД, из них Требованиям соответствуют 4 СУБД.

АТТЕСТАЦИЯ ЭКСПЕРТОВ ОРГАНОВ ПО СЕРТИФИКАЦИИ И ИСПЫТАТЕЛЬНЫХ ЛАБОРАТОРИЙ

Изменения в Правила выполнения отдельных работ по аккредитации 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, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности, утверждённые приказом ФСТЭК России от 10 апреля 2015 г. № 33

Утверждены приказом ФСТЭК России от 27 июля 2023 г. № 148

Наличие в штате ИЛ и ОС аттестованных экспертов ОС и работников ИЛ
(вступает в силу с 1 марта 2025 г.)

Расширение областей аккредитации

- Средства противодействия иностранным техническим разведкам, включая средства в которых они реализованы, а также средства контроля эффективности
- Средства защиты информации от утечки по техническим каналам, включая средства в которых они реализованы, а также средства контроля эффективности
- Средства защиты информации от несанкционированного доступа, включая средства в которых они реализованы, а также средства контроля эффективности
- Средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации
- Процессы безопасной разработки программного обеспечения средств защиты информации

ПОВЫШЕНИЕ КАЧЕСТВА ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

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, вступает в силу с 1 сентября 2024 г.

ПОРЯДОК СЕРТИФИКАЦИИ ПРОЦЕССОВ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Порядок сертификации процессов безопасной разработки программного обеспечения средств защиты информации

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

вступает в силу с 1 июня 2024 г.

Пункт 71.1 Положения о системе сертификации СЗИ (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55)

Предоставляет право разработчику самостоятельно проводить испытания СЗИ в случае внесения в сертифицированное СЗИ изменений, в том числе изменений, связанных с добавлением новых функций безопасности информации, или изменений в имеющиеся функции безопасности информации, с обновлением версий ПО, включая совершенствование функций его безопасности или добавления новых функций безопасности, а также с добавлением новых или изменением существующих аппаратных платформ.

Национальный стандарт ГОСТ Р 56939-2016
«Защита информации. Разработка безопасного программного обеспечения. Общие требования»

ПОРЯДОК СЕРТИФИКАЦИИ ПРОЦЕССОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Представление изготовителем СЗИ заявки на сертификацию в ФСТЭК России

Рассмотрение заявки и оформление (отказ в оформлении) решения на сертификацию

Направление изготовителем в орган по сертификации руководства по безопасной разработке программного обеспечения

Проведение сертификации органом по сертификации

Оценка соответствия руководства требованиям по безопасной разработке

Проверка наличия у изготовителя средств разработки программного обеспечения и средств проведения композиционного, статического и динамического анализа программного обеспечения

Проверка выполнения требований к обучению специалистов изготовителя

Оценка соответствия руководства требованиям по безопасной разработке

Проверка реализации изготовителем процессов безопасной разработки, приведенных в руководстве и в документации

Проверка реализации изготовителем процедур поддержки безопасности программного обеспечения

Оформление органом по сертификации протоколов и экспертного заключения

Рассмотрение материалов сертификации в ФСТЭК России и принятие решения о выдаче сертификата соответствия

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

проект

Информационное сообщение «О проведении сертификации СЗИ с учетом результатов деятельности Центра исследования безопасности системного программного обеспечения»

Центр исследования безопасности системного программного обеспечения

Результаты деятельности:

- Исходный код программных компонентов;
- Методики проведения статического и динамического анализа компонентов;
- Результаты статического анализа программных компонентов.

ФСТЭК России

ИСП РАН

Подача заявки на проведение сертификации СЗИ

К заявке прилагается перечень заимствованных программных компонентов с открытым исходным кодом

Оформление решения

Представление в Центр разработчиком перечня заимствованных программных компонент с открытым исходным кодом

Рассмотрение перечня Центром

Направление разработчику Центром плана проведения испытаний заимствованных программных компонентов

Проведение оценки корректности перечня испытательной лабораторией

Проведение сертификационных испытаний в объеме, предусмотренном планом

Представление испытательной лабораторией в Центр результатов испытаний

Проведение органом по сертификации экспертизы материалов

Осуществление разработчиком выполнения плана в течение срока действия сертификата соответствия

Направления совершенствования безопасности системного программного обеспечения

Начальник
2 управления ФСТЭК России

Шевцов Дмитрий Николаевич