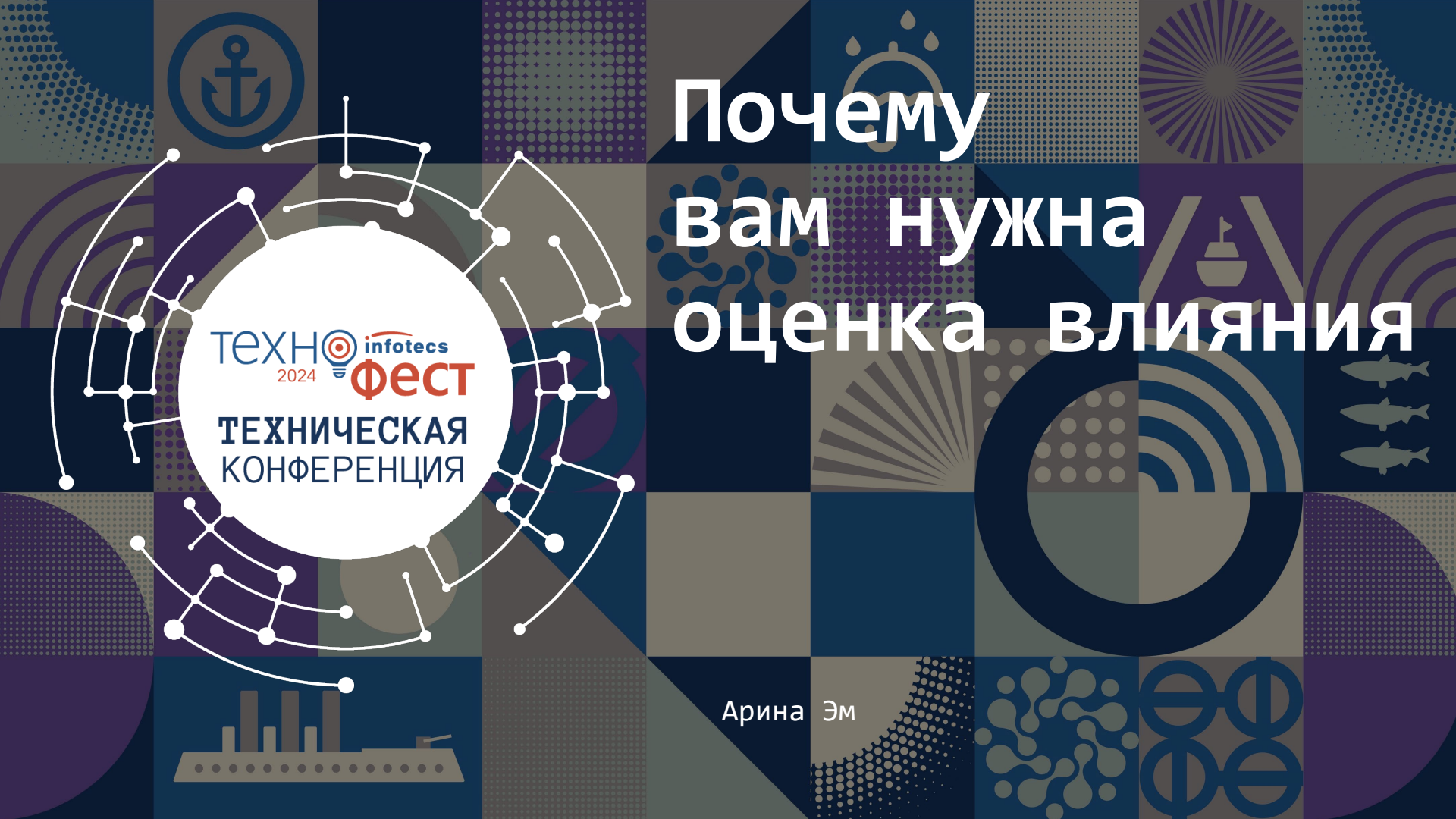

Почему вам нужна оценка влияния

Арина Эм

План

1. Почему нам всем важно знать об оценке влияния
2. Что такое оценка влияния
3. При каких условиях она должна проводиться
4. Кто участвует в этом процессе и что для этого нужно

История вопроса

Мы разделяем СКЗИ на два типа

Коробочные СКЗИ

- Готовы к работе из коробки
- Не требуют дополнительного программирования

Встраиваемые СКЗИ

- Возможно интегрировать в любое решение
- Прозрачны для конечных пользователей
- Могут быть использованы на имеющихся мощностях

Встраиваемые СКЗИ

ТехноФест 2024 infotecs

Аппаратные

- ViPNet SIES Core
- ViPNet SIES Core Nano
- ViPNet SIES Unit

Программные

- ViPNet OSSL
- ViPNet JCrypto SDK
- ViPNet CSP

Нормативка

ТЕХНО 2024 infotecs ФЕСТ

- ПКЗ-2005
- Положение о лицензировании
- 152 приказ ФАПСИ
- Информационное сообщение ФСБ Росси

Положение ПКЗ-2005

Приказ ФСБ России от 9 февраля 2005 г. №66 об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации

35 **Оценка влияния** аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований **осуществляется разработчиком СКЗИ совместно со специализированной организацией.**

36 **Результаты тематических исследований и оценки влияния** аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований, а также опытные образцы СКЗИ и аппаратные, программно-аппаратные и программные средства, необходимые для штатного функционирования СКЗИ, **передаются в ФСБ России для проведения экспертизы.**

Положение ПКЗ-2005

Приказ ФСБ России от 9 февраля 2005 г. №66 об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации

46 СКЗИ эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

Формуляр на СКЗИ

На примере формуляра ViPNet CSP 4.4

При встраивании ViPNet CSP в прикладное ПО необходимо проводить (по согласованному с ФСБ России техническому заданию) оценку влияния прикладного ПО на встроенное ViPNet CSP (исполнения 1, 2, 4, 5) в следующих случаях:…

Для ViPNet CSP (исполнения 3 и 6) указанная оценка влияния проводится в обязательном порядке.

Правила пользования на СКЗИ

На примере правил пользования ViPNet CSP 4.4

Разработка прикладного ПО на основе ViPNet CSP может производиться без создания нового СКЗИ **в случае использования вызовов функций из перечня**, приведенного в Приложении А.

В случае **использования прочих вызовов необходимо производить разработку отдельного СКЗИ** в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

ТЕХНО 2024 infotecs ФЕСТ

Вы создаете отдельное СКЗИ или все-таки нет?

Что есть что?

Оценка влияния*

Вызываются функции, описанные в правилах пользования

И

само встраиваемое СКЗИ сертифицировано

Какая лицензия нужна разработчику

Лицензия на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем

Создание нового СКЗИ*

Вызываются функции, **не** описанные в правилах пользования,

или

встраиваемое СКЗИ не сертифицировано

Какая лицензия нужна разработчику

Лицензия на разработку шифровальных (криптографических) средств

* Постановление Правительства Российской Федерации от 16 апреля 2012 г. №313

Лицензия на разработку СКЗИ имеет свои требования

Для лицензии **на разработку СКЗИ необходимо наличие** у соискателя лицензии **допуска к выполнению работ и оказанию услуг**, связанных с использованием **сведений, составляющих государственную тайну**.

Разные требования к наличию персонала (как к руководителям работ, так и к инженерно-техническим работникам).

* Постановление Правительства Российской Федерации от 16 апреля 2012 г. №313

Когда нужно проводить оценку влияния

Возвращаемся к ПКЗ-2005

3 Настоящим Положением необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее - государственные органы);
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее - организации, выполняющие государственные заказы);
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Информационное сообщение ФСБ России

«О неукоснительном соблюдении операторами персональных данных требований формуляров на СКЗИ»

Обращаем внимание на обязательность неукоснительного соблюдения операторами персональных данных требований формуляров на средства криптографической защиты информации (далее – СКЗИ), в частности, **на требование, касающееся проведения оценки влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований**.

Проведение работ по оценке влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований является обязательным условием действия сертификата на СКЗИ, в соответствии с которым СКЗИ обеспечивает заданный уровень информационной безопасности при выполнении требований эксплуатационной документации согласно формуляру на СКЗИ.

<…>

Применение операторами СКЗИ, не имеющего положительного заключения ФСБ России по результатам оценки влияния аппаратных, программно-аппаратных и программных средств, если такое требование установлено в формуляре на это СКЗИ, **приводит к нарушению п. 46 Положения ПКЗ-2005 и влечет за собой административную ответственность** операторов персональных данных, предусмотренную ч. 6 ст. 13.12. Кодекса Российской Федерации об административных правонарушениях.

ТЕХНО 2024 infotecs ФЕСТ

Участники процесса

Главные участники процесса

Испытательная лаборатория

- Проводит испытания
- Подготавливает отчет
- Взаимодействует с регулятором

Орган по сертификации

- Анализирует отчет от ИЛ
- Верифицирует результаты
- Выдает заключение об оценке влияния или сертификат

Сколько времени занимает весь процесс

Специализированная организация
проводит исследования по оценке влияния одной ИС на функционирование одного СКЗИ (общий случай)

~3 месяца

Работа завершается отправкой отчетных материалов в экспертную организацию

Экспертная организация
проводит экспертизу отчетных материалов по оценке влияния одной ИС на функционирование одного СКЗИ (типовая задача)

~3 месяца

По результатам экспертизы выдается заключение о соответствии требованиям

Для оценки влияния потребуется пакет материалов

Согласовывается с 8 Центром ФСБ России

- ТЗ на проведение оценки влияния
- Дистрибутивы ПО (СПО)
- Тест-план

Комплект документации на ПО (СПО)

- общие сведения (назначение, целевые и дополнительные функции и т.п.)
- структурная схема
- перечень собственных и сторонних библиотек и компонентов
- состав дистрибутива
- инструкция по сборке дистрибутива
- описание используемых функций СКЗИ
- перечень кодов и ошибок, получаемых при взаимодействии с СКЗИ

Все это не так страшно, как кажется

- У Инфотекс есть экспертиза и опыт
- Мы регулярно сами проводим оценку влияния для наших продуктов
- Исследовательская лаборатория СФБ Лаб в ГК Инфотекс

ТЕХНО 2024 infotecs Фест

Арина Эм
Ведущий менеджер продуктов

Подписывайтесь на наши соцсети