AKTIV.
CONSULTING

Внедрение процесса безопасной разработки прикладного ПО в соответствии с требованиями 239 приказа ФСТЭК России

Александр Моисеев

Ведущий консультант по информационной безопасности
AKTIV.CONSULTING

Вебинар, октябрь 2022

Организационный слайд

Всем участникам будет выслана презентация и запись видео

Задавайте вопросы на вкладке «Вопросы»

Автор самого лучшего вопроса получит подарок от AKTIV.CONSULTING

О чем сегодня пойдет речь

01

Актуальность внедрения безопасной разработки

02

Подходы к безопасной разработки

03

Примеры реализации процессов безопасной разработки по 239 приказу ФСТЭК России

04

Проект внедрения безопасной разработки

01

Актуальность внедрения безопасной разработки

Предпосылки внедрения БРПО

01

Требования регулятора

Приказ ФСТЭК России
от 25 декабря 2017 г. N 239

*п.29.3 «...Прикладное ПО должно соответствовать требованиям **безопасной разработки**...»*

02

Политика активного импортозамещения на ЗО КИИ

Указ Президента
от 30.03.2022 № 166

*«...с 01.01.2025 г. запрещается использовать **иностранное программное обеспечение** на ЗО КИИ...»*

03

Бизнес-потребность

Помощь в достижении целей бизнеса за счет:

- снижения стоимости разработки
- управления рисками ИБ

Примеры требования безопасности ПО в отраслях

01

Финансовая отрасль

ГОСТ 57580.1 Безопасность финансовых (банковских) операций

*п.9.5 (ЖЦ.8) «…Применение прикладного ПО, соответствующего требования по **ВУ и НДВ**, или **ОУД4** по ГОСТ Р ИСО/МЭК 15408-3…»*

02

Атомная энергетика

ГОСТ Р 60880 Атомные электростанции

*п.5.7.4.2 «...Должны быть предусмотрены меры против **скрытых функций** в прикладном ПО...»*

МЭК 62859 Атомные электростанции

п.6.3.5a

*«…проверка кода учитывает уязвимости, связанные с **небезопасными методами написания кода**… »*

Примеры требований функциональной безопасности

01

Приказ ФСТЭК России от 25 декабря 2017 г. N 239

*п.21. «...Принимаемые меры безопасности ЗО КИИ должны соотноситься с мерами **функциональной безопасности**...»*

02

Приказ ФСТЭК России от 14 марта 2014 г. N 31

п.8 «...Принимаемые меры защиты информации:

***не должны оказывать отрицательного влияния** на штатный режим функционирования АСУ...»*

03

МЭК 62859 Электростанции атомные. Системы контроля и управления.

*п.6.2 b «...б) Функции кибербезопасности **не должны негативно влиять** на реализацию функций, важных для безопасности, (производительность, время отклика)...»*

Выводы по блоку

01

Требования безопасности ПО вступают в силу в ближайшее время

02

Безопасная разработка ПО – это уже тенденция, а не просто комплаенс

03

У отраслей могут быть свои требования (в т.ч. функциональной безопасности)

02

Подходы к безопасной разработке

Существующие подходы к безопасной разработке ПО

01

Национальные стандарты и НПА

- 239 приказ ФСТЭК России
- ГОСТ Р 56939 (+проекты новых стандартов)

- 76 приказ ФСТЭК России (выписка)
- *Методика ВУ и НДВ (2020)

**ограниченного распространения*

02

Гармонизированные стандарты

- ГОСТ Р ИСО/МЭК 27034xx «Безопасность приложений»
- ГОСТ Р ИСО/МЭК 15408xx «Общие критерии»

03

Международные практики

- Microsoft SDL
- Cisco SDL
- и др.

Меры по ГОСТ Р 56939

Этап 1 «Анализ требований»:	1. Определение требований по безопасности	
Этап 2 «Проектирование архитектуры ПО»:	2. Моделирование угроз* 3. Уточнение проекта архитектуры ПО	
Этап 3 «Конструирование и комплексирование ПО»:	4. Использование идентифицированных инструментальных средств разработки 5. Создание ПО на основе уточненного проекта архитектуры 6. Порядок оформления исходного кода 7. Статический анализ 8. Экспертиза исходного кода	Основные процессы
Этап 4 «Квалификационное тестирование ПО»:	9. Функциональное тестирование 10. Тестирование на проникновение 11. Динамический анализ 12. Фаззинг	
Этап 5 «Инсталляция и приемка ПО»:	13. Обеспечение целостности ПО в процессе передачи пользователю 14. Поставка пользователю эксплуатационных документов	
Этап 6 «Поддержка в процессе эксплуатации»:	15. Процедуры отслеживания и исправления ошибок и уязвимостей ПО в ходе ЖЦ 16. Систематический поиск уязвимости	
Этап 7 «Менеджмент конфигурации»:	17. Процедуры уникальной маркировки версий ПО 18. Использование системы управления конфигурацией ПО	Обеспечивающие процессы
Этап 8 «Менеджмент среды разработки»:	19. Защита от НСД к элементам конфигурации 20. Резервное копирование 21. Регистрация событий, связанных изменения элементов конфигурации	
Этап 9 «Менеджмент персонала»:	22. Периодическое обучение сотрудников и анализ программы обучения	

*меры соответствуют требованиям 239 приказа

Выводы по блоку

01

Для внедрения безопасности ПО есть стандарты и фреймворки

02

Процессы БРПО по 239 приказу ФСТЭК России соответствуют процессам ГОСТ Р 56939

03

Примеры реализации процессов безопасной разработки по 239 приказу ФСТЭК России

239 приказ ФСТЭК России

01 Руководство по безопасной разработке программного обеспечения

02 Анализ угроз

03 Обеспечение прослеживаемости (только для 1 КЗ)

04 Статический анализ

05 Динамический анализ (только для 1 КЗ)

06 Фаззинг

07 Отслеживание и исправление ошибок и уязвимостей в ходе ЖЦ

08 Информирование разработчиком информации до конечных пользователей

09 Оповещение об окончании поддержки ПО в ходе ЖЦ (только для 1 КЗ)

01. Руководство по безопасной разработке ПО

- Описание области действия руководства
- Цели организации в области БРПО
- Распределение ролей и обязанностей
- Перечень документации
- Правила и требования к планированию и проведению проверок реализации мер БРПО
- Описание действий по улучшению процесса

02. Анализ угроз

- Перечень угроз ПО в соответствии с ГОСТ Р 58412
- Методика моделирования угроз ФСТЭК (от 2021)

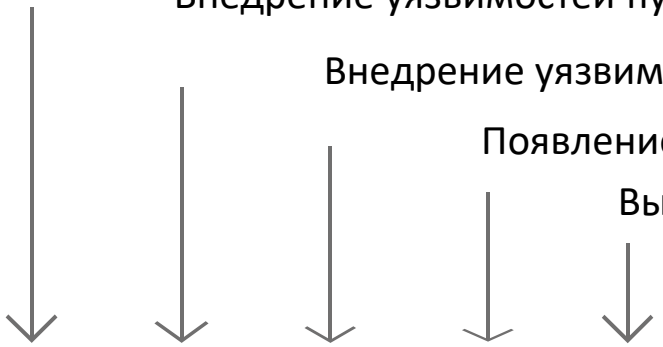
Внедрение уязвимостей в ходе разработки

Внедрение уязвимостей путем использования заимствованных компонент

Внедрение уязвимостей из-за неверного использования инструментальных средств разработки

Появление уязвимостей из-за ошибок в эксплуатационных документах

Выявление уязвимостей из-за раскрытия исходного кода



Этап 3 «Конструирование и комплексирование ПО»

03. Обеспечение прослеживаемости
(для ЗО КИИ 1 категории)

- Описания структуры ПО на уровне подсистем
- Сопоставления функций и интерфейсов ПО с подсистемами ПО

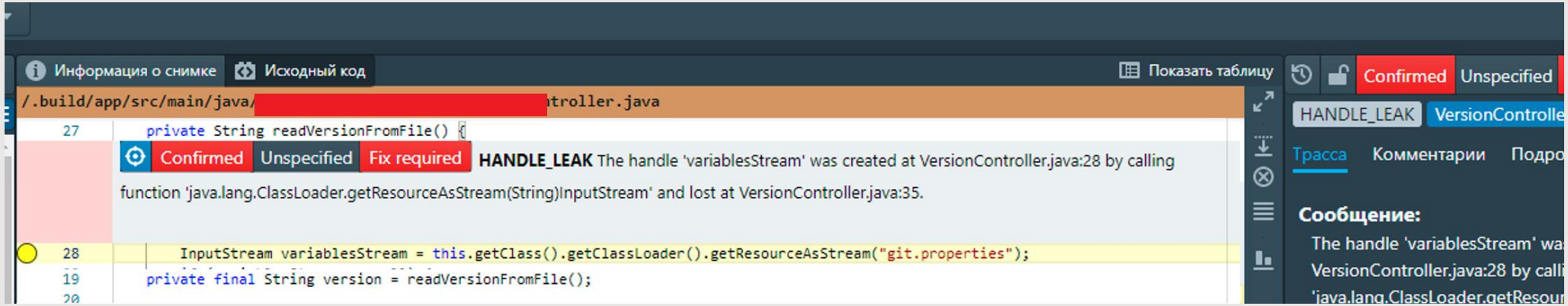
Пример обеспечения прослеживаемости:

Подсистемы ОО	Блоки функций ОО	Взаимодействует с функциями	Категория функции
Подсистема «Файлового менеджмента»	Блок функций для работы с файлами: service.admin.user.UserService#getUser domain.services.shares.SharesService#doResolveNode domain.services.nodes.FoldersService#deleteNode	БФУП	Поддерживает выполнение ФТБ

04. Статический анализ кода

- Выбор инструментов SAST
- Классификация ошибок
- Классификация применяемых методов
- Сопоставление типов предупреждений анализатора списку критических ошибок

Пример выявленной анализатором проблемы утечки из-за незакрытого потока:



05. Динамический анализ кода
(для ЗО КИИ 1 категории)

- Определение функций, принимающих на вход внешние данные
- Инструментирование кода санитайзерами / отладочными аллокаторами
- Проведение модульного и регрессионного тестирования
- Сбор покрытия
- Анализ результатов
- ГОСТы по тестированию:

56920, 56921, 56922

Пример фрагмента отчета о покрытии модульных тестов с нулевым покрытием:
:

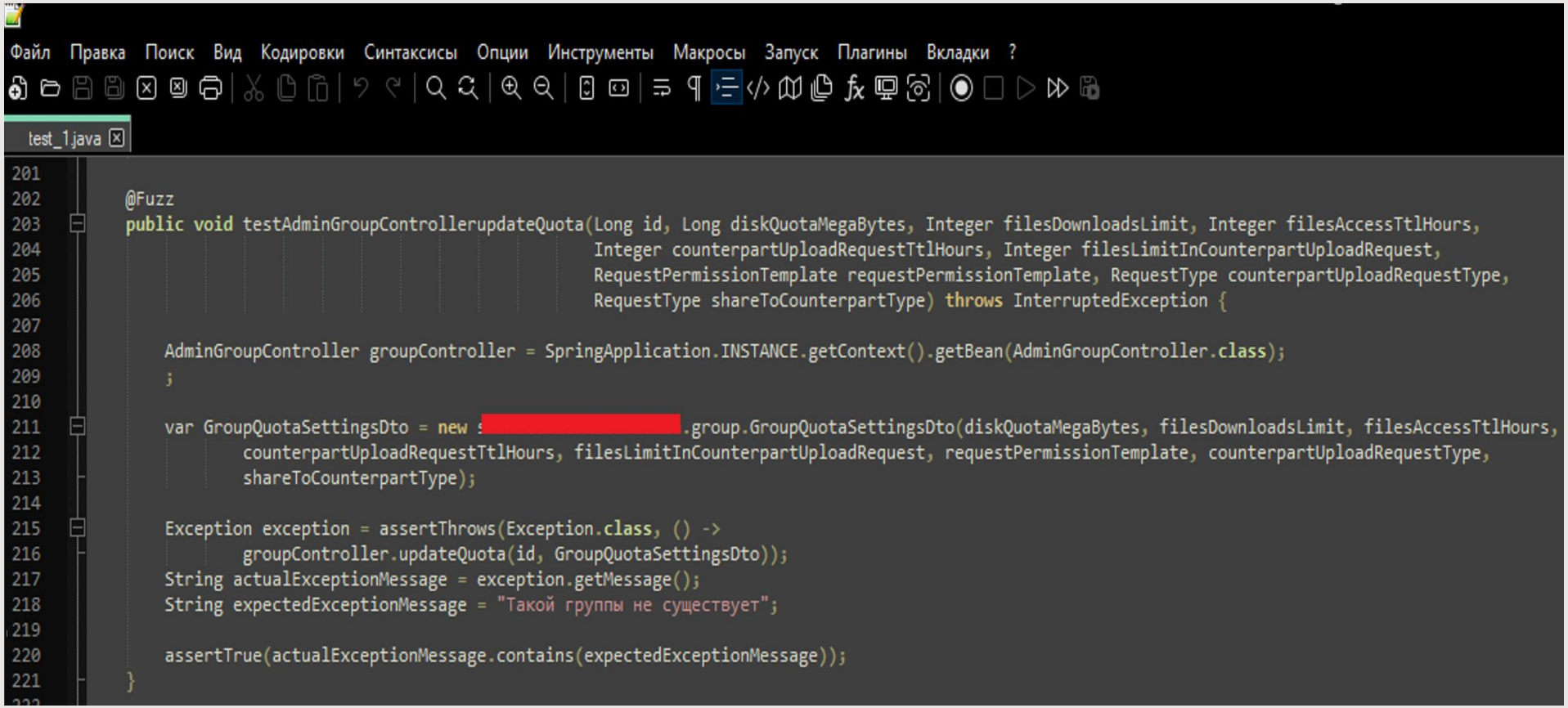
webapp

Element	Missed Instructions	Cov.	Missed Branches	Cov.
[redacted]		0 %		n/a
[redacted]ice.admin.settings.counterpart		0 %		n/a
[redacted]ice.common.logging.event.mq		0 %		0 %
[redacted]		0 %		n/a
[redacted]		0 %		n/a
[redacted]ice.admin.role.authority		0 %		n/a
[redacted]iguration.websocket		0 %		0 %
[redacted]ice.verifier.check.scenario.instance.counterpart		0 %		n/a
[redacted]ain.services.publisher.mq		0 %		0 %
[redacted]ice.admin		0 %		0 %
[redacted]		0 %		n/a
[redacted]ice.common.settings.mq.ldap		0 %		0 %
[redacted]ice.common.settings.mq.general		0 %		0 %
[redacted]ice.verifier.check.scenario.instance.transfer		0 %		0 %
[redacted]ice.verifier.check.routine		0 %		0 %
[redacted]ice.verifier.check.stage.instance		0 %		0 %
[redacted]		0 %		n/a
[redacted]		0 %		0 %
[redacted]		0 %		0 %
[redacted]ice.verifier.check.report		0 %		0 %
[redacted]iguration.db		0 %		n/a
[redacted]		0 %		0 %

06. Фаззинг

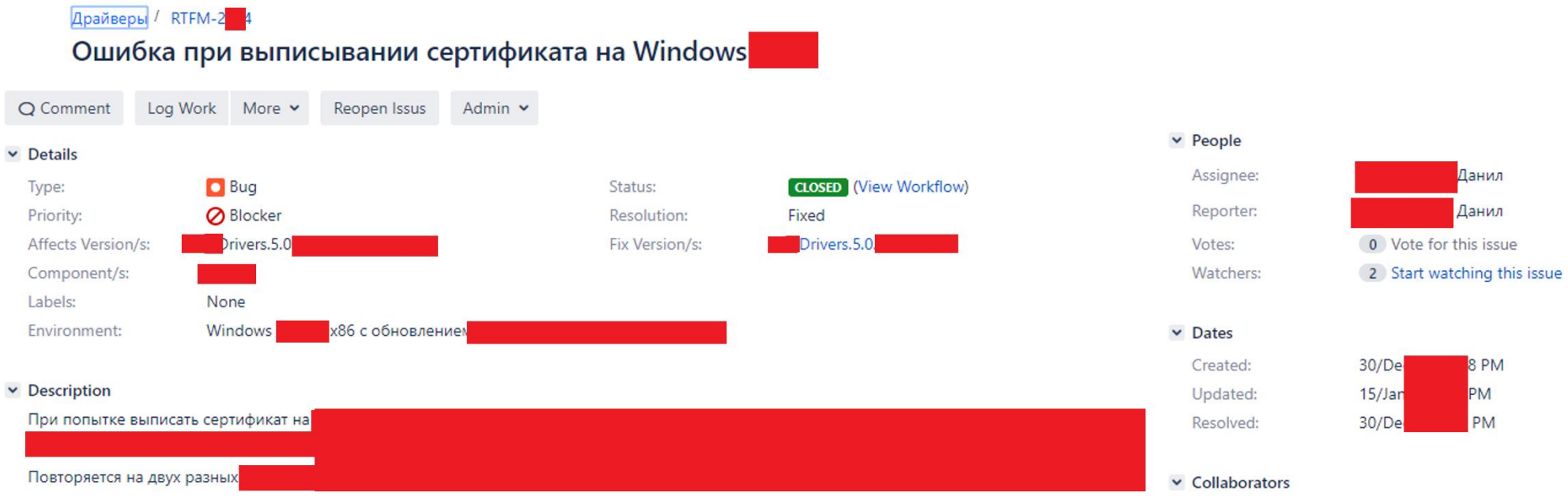
- Разработка функций для фаззинга
- Проведение тестирования
- Сбор покрытия
- Анализ результатов

Пример написания тестового кода для фаззинг-тестирования:



07. Отслеживания и исправления ошибок и уязвимостей в ходе ЖЦ

Пример регистрации проблемы в информационной системе JIRA:



08. Информирование разработчиком информации до конечных пользователей

Примеры доведения информации до конечных пользователей:

НОВОСТИ КОМПАНИИ

УСТРАНЕНА УЯЗВИМОСТЬ В СЗИ НСД [redacted]

27.12.2021

Опубликованная в базе уязвимостей ФСТЭК России 07.12.2021 г. (https://bdu.fstec.ru/vul/2021-06035) уязвимость BDU:2021-06035 устранена.

Компания «[redacted]» сообщает, что опубликованная в базе уязвимостей ФСТЭК России 07.12.2021 г. уязвимость BDU:2021-06035 Системы защиты информации от несанкционированного доступа [redacted], позволяющая нарушителю вызвать отказ в обслуживании рабочей станции с помощью внедрения в ОС специально созданного исполняемого скрипта, устранена.

Компенсирующей мерой по устранению уязвимости является установка программного изделия [redacted] версии 4550, содержащей исправление данной уязвимости.

В связи с подтверждением испытательной лабораторией АО «[redacted]» отсутствия уязвимости BDU:2021-06035 в изделии [redacted] (версии 4550), проведением испытаний и получением обновленных листов утверждения ФСТЭК России ответственный за эксплуатацию обязан:

1. Скачать обновление: https:/[redacted]Full/DLL/DLL_4550.zip.
2. Выполнить обновление изделия и внести изменения в эксплуатационную документацию на объектах в соответствии с Инструкцией по обновлению и внесению изменений в эксплуатационную документацию и Руководством администратора по обновлению изделия [redacted]

Также обращаем внимание на то, что повторная аттестация информационных систем не требуется, так как работы по обновлению средств защиты информации проводятся в рамках действующих аттестатов соответствия.

Вкладыш в формуляр [redacted]

В [redacted] исправлена критическая уязвимость

Главная / Новости

25 марта 2016

Обновление | Защита от НСД Продукт: [redacted]

Компания «[redacted]» объявляет о выпуске новой версии средства защиты информации [redacted] где исправлена критическая уязвимость.

Ранее в продукте была обнаружена уязвимость, позволяющая пользователю повысить свои привилегии до административных путем запуска вредоносного программного обеспечения. Уязвимость зарегистрирована в банке данных угроз безопасности ФСТЭК под номером 2016-00436.

В связи с этим компания «[redacted]» выпустила обновление СЗИ [redacted] (пакет обновления 6). В нем исправлены ошибки, позволяющие злоумышленникам эксплуатировать уязвимость, а также сделан ряд доработок, повысивших общий уровень защищенности продукта. Дистрибутив и порядок обновления доступны по ссылке.

Обновление обязательно к установке для всех пользователей СЗИ [redacted] Его нужно устанавливать сразу после выпуска без ожидания окончания процедуры инспекционного контроля. В случае проведения обновления в аттестованной системе заказчику требуется направить письмо-уведомление в орган по аттестации. При этом переаттестации системы не требуется. Подробно порядок обновления СЗИ [redacted] зафиксирован в обновленном разделе 6 Формуляра RU.88338853.501410.015 30.

09. Оповещение об окончании поддержки ПО в ходе ЖЦ

(для ЗО КИИ 1 категории)

Пример оповещения конечных пользователей об окончании поддержки:

Windows 10 IoT Корпоративная 2021 с долгосрочным обслуживанием

Windows 10 IoT Корпоративная 2021 с долгосрочным обслуживанием следует Фиксированной политике жизненного цикла.

Даты поддержки показаны в тихоокеанском часовом поясе (PT) — Redmond, WA, USA.

Даты предоставления поддержки

Список	Дата начала	Дата окончания основной фазы	Перенесенная дата окончания
Windows 10 IoT Корпоративная 2021 с долгосрочным обслуживанием	16 нояб. 2021 г.	12 янв. 2027 г.	13 янв. 2032 г.

Выводы по блоку

01

Процессы безопасности учитывают индивидуальные особенности организации

02

Все необходимые свидетельства и записи по процессам безопасности могут иметь различный вид и представление

04

Проект внедрения процесса БРПО

Зависимость параметров проекта от типа разработки

Основные процессы БРПО

Тип 1 «внутренняя»	Управление БРПО	Создание ПО	Поддержка ПО в ходе ЖЦ	Обучение персонала	Управление конфигу-рацией	Управление инфраструктурой среды разработки	Правовое регулирова-ние
Тип 2 «заказная»	Управление БРПО	Получение свидетельств по процессам (в максимально полном объеме)					Правовое регулирова-ние
Тип 3 «вендорская»	Управление БРПО	Получение свидетельств по процессам (в достаточном объеме)					Правовое регулирова-ние

Препятствия для внедрения БРПО

- Отсутствие обоснования для руководства
- «Сопротивление» разработчиков
- Трактовка требований регулятора
- Неопределенность влияния на существующие бизнес процессы
- Постановка кроссфункционального взаимодействия

Пример проекта по внедрению БРПО

1 этап
Обоснование

- Определение целей проекта
- Определение задач проекта
- Определение выгод от реализации проекта

Результат этапа:

ТЭО и принятое на его основе решение руководства

2 этап
Аудит

- Обследование текущих бизнес процессов разработки
- Формирование целевого состояния процессо (в соответствии с требованиям регулятора)
- GAP-анализ
- Разработка рекомендаций

Результат этапа:

подготовка «Рекомендаций...», содержащих орг. и тех. меры

Пример проекта по внедрению БРПО

3 этап
Разработка дорожной карты

- Ранжирование орг. и тех. мер (на основе рекомендаций)
- Разработка «Плана перехода...»
- Разработка «Пояснительной записки…»

Результат этапа:
подготовка «Дорожной карты...»

4 этап
Внедрение процессов

- Внедрение орг. мер (ОРД, ЛНА, обучение)
- Внедрение тех. мер (SAST, DAST, Fuzzing)

Результат этапа:
функционирующие процессы БРПО

5 этап
Контроль

Проверка полноты и достаточности внедренных мероприятий

Результат этапа:
свидетельства функционирования БРПО

Выводы по блоку

Проектный подход позволяет устранить озвученные ранее препятствия за счет:

01 единой точки ответственности (т.е. руководителя проекта)

02 команды проекта: ИБ, ИТ, разработки, эксплуатирующих и обеспечивающих подразделений (с техническим лидерством разработчиков)

03 определения этапов проекта внедрения БРПО и промежуточных результатов

04 оценки и планирования ресурсов (время, специалисты, финансы)

05 подготовки ТЭО

В качестве резюме

01 Внедрение БРПО в минимальном объеме требований ФСТЭК для субъектов КИИ — это подъемная задача

02 Приступать к внедрению нужно уже вчера

03 Необходимо разобраться в требованиях 239 приказа ФСТЭК*

04 Адаптировать БРПО к бизнес-процессам вашей организации

05 Сформировать команду проекта и назначить руководителя проекта

*И заранее заложить развитие процессов под систему стандартов ГОСТ Р 56939

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting