Сертификация средств защиты информации

Основные аспекты и их роль в развитии научных исследований

СЕРТИФИКАЦИЯ / ИССЛЕДОВАНИЯ

М. Л. Радюкевич

Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»
Минск, Республика Беларусь

Сертификация и исследования усиливают друг друга

Научные исследования

Методы испытаний
Модели риска
Инструменты оценки

методы →

← задачи

Практика сертификации

Проверка требований
Экспертный опыт
Нормативные пробелы

> Результаты науки становятся требованиями,
> а опыт сертификации - новыми исследовательскими задачами.

Нормативная основа: от правовых оснований к требованиям

Правовые основания	**Закон № 455-З и Указ № 449** Использование средств защиты информации
Правила процедуры	**Постановление Госстандарта № 61** Правила подтверждения соответствия
Технические требования	**ТР 2013/027/BY** Требования информационной безопасности к СЗИ
Взаимосвязанные стандарты	**Приказ ОАЦ № 207** Перечень государственных стандартов в поддержку технического регламента

Для создания системы защиты информации используются средства технической и криптографической защиты информации, имеющие сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы.

Какие СЗИ подлежат обязательной сертификации

Области применения, перечисленные в техническом регламенте

а) **Техническая защита государственных секретов**

б) **Системы защиты информации ИС, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено**

в) **Системы информационной безопасности критически важных объектов информатизации**

г) **Целостность и подлинность электронных документов**

Требования и независимая оценка

Common Criteria / ISO/IEC 15408

Риск-ориентированный подход

Профили защиты

Задания по безопасности

Уровни гарантии оценки

НЕЗАВИСИМОЕ ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ

Аккредитованная испытательная лаборатория
Проводит сертификационные испытания

→

Аккредитованный орган по сертификации
Подтверждает соответствие требованиям

Два вида сертификационных испытаний

«ЧЕРНЫЙ ЯЩИК»

Функциональное тестирование

Проверка соответствия нормативным требованиям без анализа внутреннего устройства программы

«БЕЛЫЙ ЯЩИК»

Структурное тестирование

Анализ исходных текстов программ для контроля отсутствия недекларированных возможностей

Структурное тестирование применяется только к СКЗИ

От соответствия требованиям - к оценке снижения риска

НАПРАВЛЕНИЕ РАЗВИТИЯ

Показатели соответствия требованиям → **Снижение риска за период действия сертификата**

ЧТО ТРЕБУЕТ НАУЧНОГО ОБОСНОВАНИЯ

- **Математические модели рисков**
- **Количественная оценка защищенности**
- **Требования к обновлению ПО СЗИ**

Новые требования выявляют нормативные пробелы

01

Развитие требований

Обнаружение и реагирование на угрозы конечных узлов

Сбор и хранение сведений о DNS-запросах

02

Нормативный пробел

Для ряда новых средств технические требования в ТНПА не установлены

03

Субъективный подход

Опора на задания по безопасности, разрабатываемые производителями

Научная задача: выработать общие технические требования к новым средствам защиты информации.

Приказ ОАЦ № 259: примеры изменений

ТРЕБОВАНИЕ	КЛАССЫ СИСТЕМ
Обнаружение и реагирование на угрозы конечных узлов	**3-бг, 3-дсп**
Централизованный сбор и хранение сведений о DNS-запросах активов информационной системы и средств защиты информации	**3-ин, 3-спец, 3-бг, 3-юл, 3-дсп**

Также отмечены требования к защите виртуальной инфраструктуры и к оценке эффективности защищенности информационных систем.

НИР «Стандарт»: от научной задачи к требованиям

ГНТП

«Кибербезопасность-2»

2026

2030

Развитие национальной системы технического нормирования и стандартизации в области кибербезопасности

ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

Технические требования к СЗИ

Новые методы защиты информации

Методы оценки эффективности систем защиты

Что ограничивает систему сертификации ?

01 **Нормы отстают от технологий**

Требования не всегда отражают современные угрозы и векторы атак.

02 **Высокая стоимость и сроки**

Сложный комплекс процедур с опорой на экспертные методы.

03 **Субъективизм оценок**

Многоуровневые проверки требуют участия человека.

04 **Неполнота исходных материалов**

Трудности с доступом к исходному коду, особенно иностранной продукции.

05 **Устаревание сертификатов**

Сертификат относится к версии ПО; обновление меняет объект оценки.

06 **Изменчивость Open Source**

Динамика проектов, внешние репозитории и риск вредоносных изменений.

Автоматизация усиливает инструментальную основу испытаний

Автоматизация тестирования

Анализ исходного кода

Поиск уязвимостей

Меньше субъективизма

Более оперативная сертификация

Обновления требуют непрерывной оценки соответствия

ПРОБЛЕМА

Сертификат на конкретную версию

↓

Обновление ПО СЗИ

↓

Возможная пересертификация

ПЕРСПЕКТИВА: ОЦЕНКА В ЖИЗНЕННОМ ЦИКЛЕ

Безопасная разработка: проверять не только готовую продукцию, но и процесс ее создания.

Open Source: прозрачность кода и риски зависимостей

Возможности

Независимый аудит

Выявление уязвимостей

Прозрачность и доверие

Вызовы

Динамичность проектов

Зависимость от сторонних репозиториев

Риск вредоносных изменений

ИССЛЕДОВАТЕЛЬСКИЕ ЗАДАЧИ

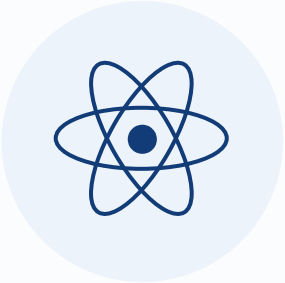
Верификация компонентов

Мониторинг уязвимостей в зависимостях

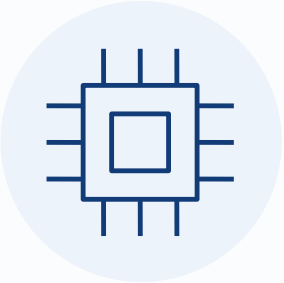
Целостность и аутентичность исходного кода

Оценка доверия к сообществам разработчиков

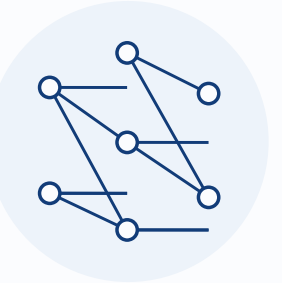
Спектр угроз расширяет исследовательскую повестку



Квантовые вычисления



Атаки по сторонним каналам



Искусственный интеллект в кибератаках

Новые методики сертификационных испытаний

Исследовательская повестка: шесть направлений

	НАПРАВЛЕНИЕ	ИССЛЕДОВАТЕЛЬСКИЙ РЕЗУЛЬТАТ
01	**Риск-ориентированная оценка**	Модели риска, угроз и уязвимостей
02	**Автоматизация испытаний**	Инструменты испытаний и анализа кода
03	**Непрерывная оценка**	Модели мониторинга защищенности
04	**Безопасная разработка**	Модели зрелости процессов разработки
05	**Новые классы угроз**	Методики сертификационных испытаний
06	**Open Source-компоненты**	Верификация и мониторинг компонентов

Сертификация опирается на науку. И формирует задачи для науки.

1. **Научно-технический процесс**
   Не только подтверждение соответствия, но и развитие методов оценки.
2. **Обратная связь с нормативной базой**
   Исследования формируют требования; практика - новые научные задачи.
3. **Совместное развитие**
   Риск-ориентированная оценка, автоматизация и непрерывный мониторинг.

Спасибо за внимание!

Радюкевич Марина Львовна
Научно-производственное
республиканское унитарное предприятие
«Научно-исследовательский институт
технической защиты информации»