FBK | CS cybersecurity

АБИСС

Доверие к результатам оценки соответствия

Андрей Петрович Курило
Советник по вопросам информационной безопасности FBK CyberSecurity

ABISS conf | Москва | 2023

УЗКОЕ МЕСТО В МЕТОДИКЕ ОЦЕНКИ СООТВЕТСТВИЯ

Доверие к результатам оценки соответствия

- Отсутствуют единые методики контроля и оценки уровня защищенности ИС
- Нестыковки результатов оценок по методикам разных регуляторов
- Принятие сопутствующих остаточных рисков нарушения безопасности системы

Возникает вопрос к точности измерений, доверия к результатам оценки и, как следствие, **к профессионализму компании, проводящей оценку**

*«Результаты оценки соответствия защиты информации с привлечением проверяющей организации не всегда отражают реальное состояние процесса обеспечения информационной безопасности в организациях кредитно-финансовой сферы. **В итоге уровень доверия к результатам аудита, проведенного проверяющей организацией, снижается**»*

Центральный Банк России Концепция «Совершенствование системы внешнего аудита информационной безопасности»

ПРОФЕССИОНАЛИЗМ – В ГЛАЗАХ ЗАКАЗЧИКА

Решение одной из внутриотраслевых ассоциаций

*Присвоение **«знака качества»** организациям, прошедшим проверку в виде внешнего аудита и самооценки.*

- Не было внедрено по причине сохранения **проблемы объективности и точности оценки**

Решение на уровне государства

*Введение **ФЗ N 223-ФЗ** «О закупках товаров, работ, услуг отдельными видами юридических лиц" и **ФЗ N 44-ФЗ** от "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».*

- В тендерах решающим остается **стоимость предложения, а не профессионализм**
- Нет принципиального решения **вопроса демпинга**
- Официальное признание **зарубежных квалификационных сертификатов** и отсутствие их полноценных российских аналогов

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ К РЕЗУЛЬТАТАМ ОЦЕНКИ

7 базовых принципов обеспечения доверия к результатам оценки

Из опыта финансового аудита (ИСО/МЭК 17021-1:2015 и ГОСТ Р ИСО/МЭК 27006-2020)

1. Компетентность
2. Беспристрастность
3. Ответственность
4. Открытость
5. Конфиденциальность
6. Реагирование на жалобы
7. Подход на основе рисков

Кто определит соответствие данным принципам и как проверяемой организации легче всего будет считать эту информацию?

ЧТО ПОЗВОЛЯЕТ ОБЕСПЕЧИТЬ ДОВЕРИЕ К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИС

(А) Концептуально

- Адекватность используемой методики оценки, точностью выбора критериев защищенности
- Точность аппарата расчета уровня защиты, положенного в основу методики оценки
- Ответственность
- Открытость
- Конфиденциальность
- Реагирование на жалобы
- Подход на основе рисков

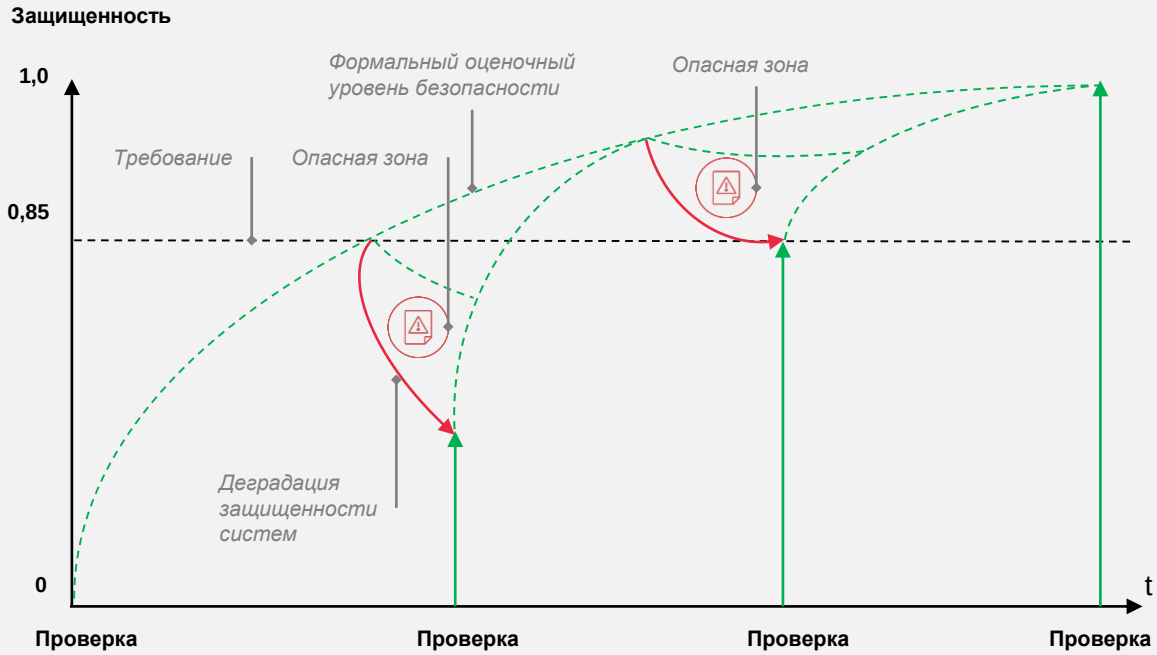
(Б) В ходе оценки защищенности

- Квалификация и опыт проектной команды

(В) в ходе практического обеспечения ИБ внутри организации

- Полнота покрытия «поверхности» защищаемой ИС требованиями по безопасности и защитными мерами
- Полнота и своевременностью выполнения требований по безопасности и защитных мер самой организацией
- Способностью системы защиты организации сохранять достигнутый уровень безопасности и противостоять неминуемой деградации

КОНТРОЛЬ СНИЖЕНИЯ РЕАЛЬНОГО УРОВНЯ ЗАЩИЩЕННОСТИ



Ключевые вопросы:

- Когда это отклонение станет критичным и когда его нужно измерять.
- Как предотвратить дальнейшее ухудшение ситуации и как организовать эту процедуру.
- **Какие индикаторы, характеризующие ухудшение, необходимо контролировать.**

ИНДИАКТОРЫ ЗАЩИЩЕННОСТИ

Индикаторы улучшения уровня защищенности

- Качественное управление процессами СМИБ;
- Наличие сервисов SOC и SIEM;
- Высокий уровень организации аналитической деятельности;
- Качество планирования;
- Использование в практике работы средств автоматизированного управления безопасностью класса SRGC;
- Налаженный процесс повышения квалификации;
- Наличие планов и свидетельств проведения тренингов,
- Наличие планов и свидетельств проведения киберучений;
- Наличие процедур прогнозирования и свидетельств улучшений на их основе;
- Своевременность и достаточный уровень финансирования,
- Кадровая и организационная стабильность,
- Оперативное управление уязвимостями.

Индикаторы снижения уровня защищенности

- Слабая аналитическая деятельность,
- Неструктурированное управление,
- Недостаточное финансирование,
- Кадровый голод,
- Организационная нестабильность,
- Смена собственников.

ПРЕДЛАГАЕМЫЕ РЕШЕНИЯ

1. Совершенствование методического аппарата
2. Создания СДС как способа улучшения качества работ, выполняемых ее членами
3. Создание механизма подтверждения квалификации проверяющей организации (обучение, сертификация, прозрачная система проверки данных об оценщике и его квалификации для заказчика)
4. Разработка и внедрение механизма постконтроля с проверкой отдельных параметров и процессов, существенно негативно влияющих на уровень безопасности

FBK | CS
cybersecurity

Благодарим за внимание!

+7 (495) 970-41-32

Sales@fbkcs.ru

Info@fbkcs.ru