FBK | CS
cybersecurity

Об интерпретации результатов оценок ИБ

Курило АП,
ктн. Доцент РГУ им.Губкина,
Советник по ИБ ООО
«Финансовые и бизнес консультанты»
(ФБК)
Советник по ИБ ООО ФБК CS

Москва | 2024

«Теория без практики - мертва, практика без теории слепа».

Генералиссимус А.В. Суворов

А кто мы сейчас: мертвые или слепые?

- Скорее слепые, чем мертвые

А в чем это выражается?

FBK | CS cybersecurity

Немного теории

- Защищенность информации - это специфическое состояние (свойство объекта), относящееся к категории качества и возникающее в результате выполнения защитных мер на среде ее обработки.
- ИБ возникает как «оружие» собственника информационного актива и злоумышленника в борьбе за обладание этим активом.
- Защищенность имеет неприятное свойство незаметно улетучиваться.
- В качестве среды обработки информации рассматривается автоматизированная система (АС). Все защитные меры применяются к ней.
- Каждое защитное действие имеет свой процесс СОИБ.
- Каждый процесс СОИБ может быть измерян по шкале зрелости.
- Состояние защищенности системы бывает разное.

Состояние защищенности объекта бывает:

- **статическое**
- **динамическое.**

Статическое

Динамическое

На объект в состоянии покоя или интенсивной эксплуатации действуют разные факторы, контролировать и оценивать их нужно по - разному.

Сравнительные характеристики статического и динамического описания состояния безопасности объекта

Контроль статического состояния защищенности объекта проводится периодическими проверками, начиная с испытаний ИС, управлением рисками и аттестацией

Достоинства:

- Официально принятый подход
- Подробное описание объекта и его СОИБ
- Рекомендации по стратегическому улучшению

Недостатки:

- Не позволяет противодействовать атакам и осуществлять менеджмент инцидентов
- Высокий уровень обобщения наряду с низкой точностью
- Высокая зависимость от субъективного фактора
- Невозможно экстраполировать результаты оценки на весь межпроверочный период.
- Критическое отношение регуляторов к некоторым видам проверок

Контроль динамического состояния защищенности объекта проводится только по некоторым процессам, но непрерывно (постоянный мониторинг настроек системы защиты, состояния системы, целостности активов, уязвимостей, инцидентов)

Достоинства:

- Позволяет непрерывно контролировать и корректировать настройки СИБ
- Позволяет бороться с атаками и инцидентами
- Собирает аудит для проведения расследований и анализа деятельности

Недостатки:

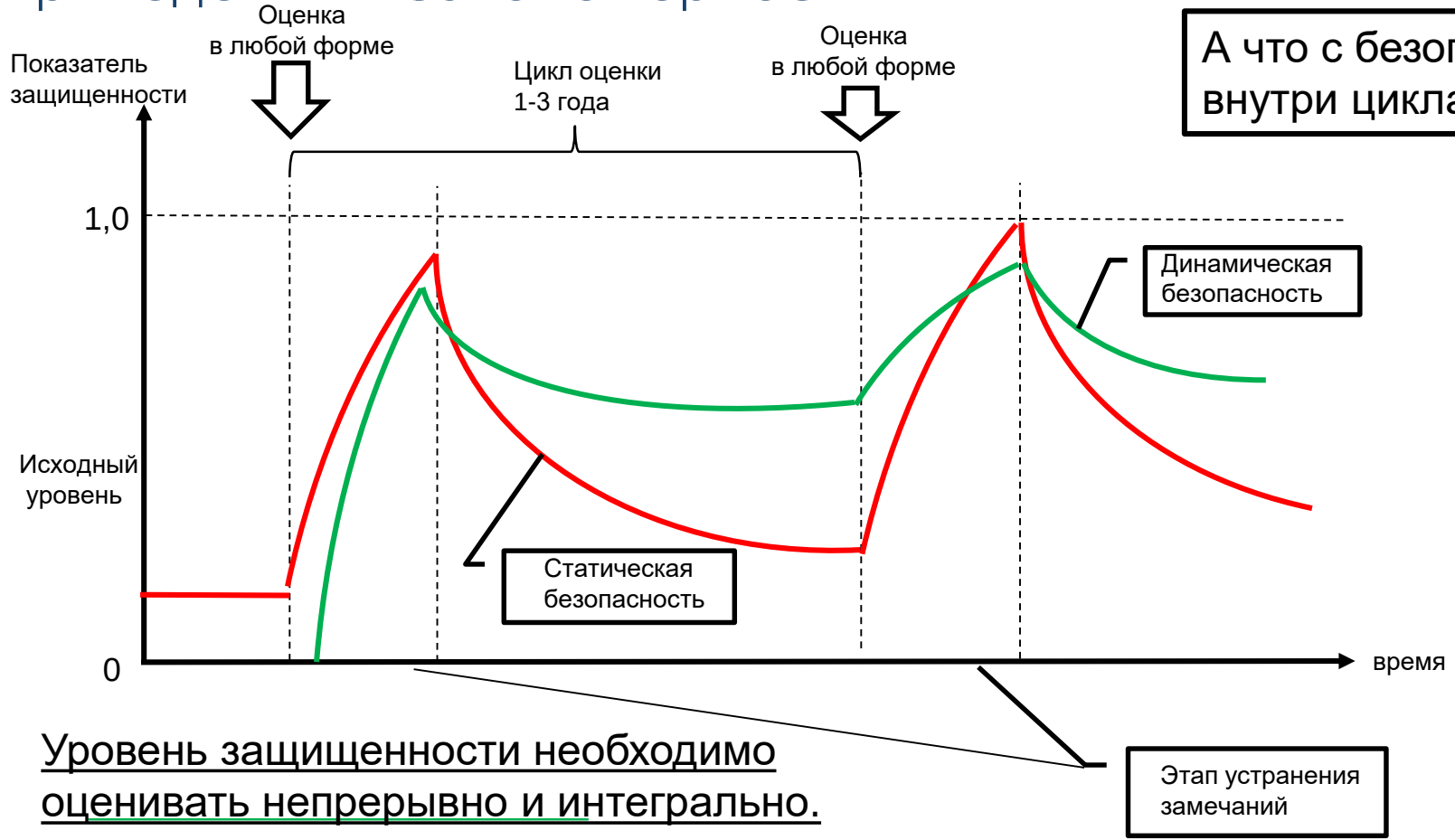
- Позволяет мониторить только некоторые группы защитных мер, хотя их можно отнести к категории наиболее важных (Закон Парето 20/80);
- Большой объем «сырых» данных, недостаточная автоматизация обработки, большой объем рутинных операций, возлагаемых на операторов

Общий недостаток- отсутствие системы единого централизованного учета результатов контроля (на основе процессного подхода и шкал зрелости)

Нужно использовать технологии ИИ

Нужно сводить результаты к интегральному показателю зрелости процессов обеспечения СОИБ и контролировать их доступными средствами!

Реальное поведение защищенности объекта подчиняется приведенным закономерностям



Уровень защищенности необходимо оценивать непрерывно и интегрально.

Сколько уже сейчас контролей на практике?

- 14, не считая выполнения Указа Президента №250 в части импротозамещения.

- Плюс проверки отраслевых регуляторов

№ п/п	Вид контроля	Что преимущественно оценивается	Форма измерения, состояние СОИБ	Результативность
1	**Аттестация**	Выполнение требований ФСТЭК	Дискретная, статическое	Не высокая
2	**Аудит ИБ**	Общее состояние системы защиты, организация работ, выполнение требований по защите	Дискретная, статическое	Средняя Не закрывает проблему реальной защищенности
3	**Оценка соответствия требованиям по безопасности**	Соответствие заданным требованиям по безопасности	Дискретная, статическое	Выше средней Не закрывает проблему реальной защищенности
4	**Оценка безопасности КИИ**	Анализ деятельности по отражению кибератак	Дискретная, статическое. Анализ логов состояния на момент атаки	?
5	**Госконтроль**	Выполнение требований ФЗ и ФСТЭК	Дискретная, статическое	Аналог аудита
6	**Экспресс-оценка защищенности**	Требования по безопасности для отдельных элементов СОИБ,	Дискретная, статическое	Противоречит сложившейся идеологии
7	**Инструментальное тестирование**	Наличие уязвимостей в системе	Дискретная, статическое	Высокая
8	**Белый хакинг**	Наличие уязвимостей в системе	Статическое, в течение длительного времени	Возможны серьезные негативные последствия
9	**Мониторинг СОИБ. Мониторинг настроек СИБ**	Текущее состояние защищенности и состояния системы	Непрерывная, динамическое	высокая
10	**Мониторинг СОИБ. Мониторинг инцидентов**	Наличие результативных атак	Непрерывная, динамическое	высокая
11	**Контрольная проверка**	Подготовленность и работоспособность коллектива	Дискретная, статическое	Низкая в части оценки требований ИБ. Высокая в части оценки деятельности коллектива
12	**Анализ рисков**	Уязвимости и ошибки в системе защиты, создающие риски ИБ	Дискретная, статическое	Высоко ресурсозатратная превентивная мера с неясной эффективностью
13	**Проверки по 152 ФЗ**	Готовность к обработке инцидентов	Дискретная, статическое	Практически не влияют
14	**Киберучения**	Реальная готовность коллектива АИС (объекта) к отражению атак	Дискретная, динамическое	Весьма высокая

Критерии оценки защищенности, методики оценки и виды контролей

практика

ФСТЭК – 100% выполнения требований по защите, соответствие требованиям законодательства

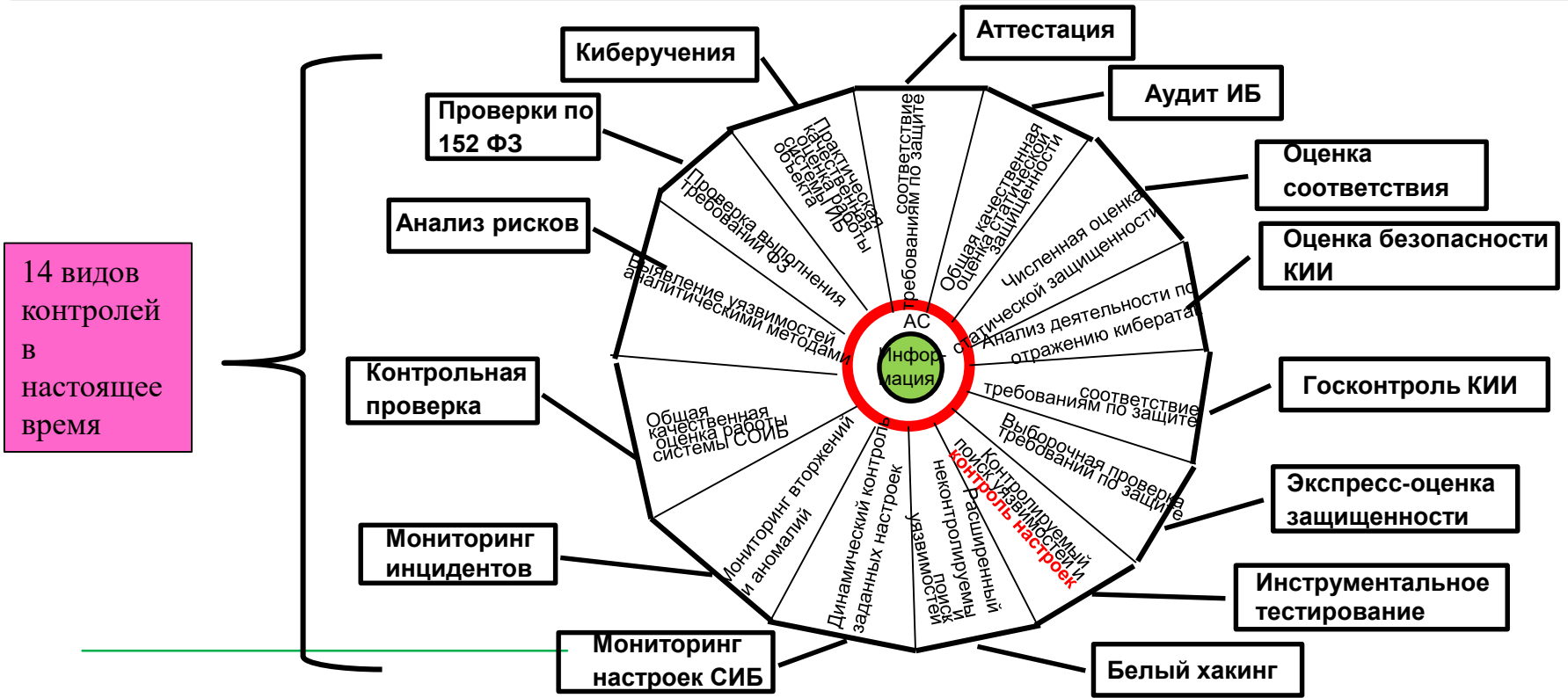
Минцифры – наличие (выборочное) процедур и регламентов

ФСБ - ?, соответствие требованиям законодательства

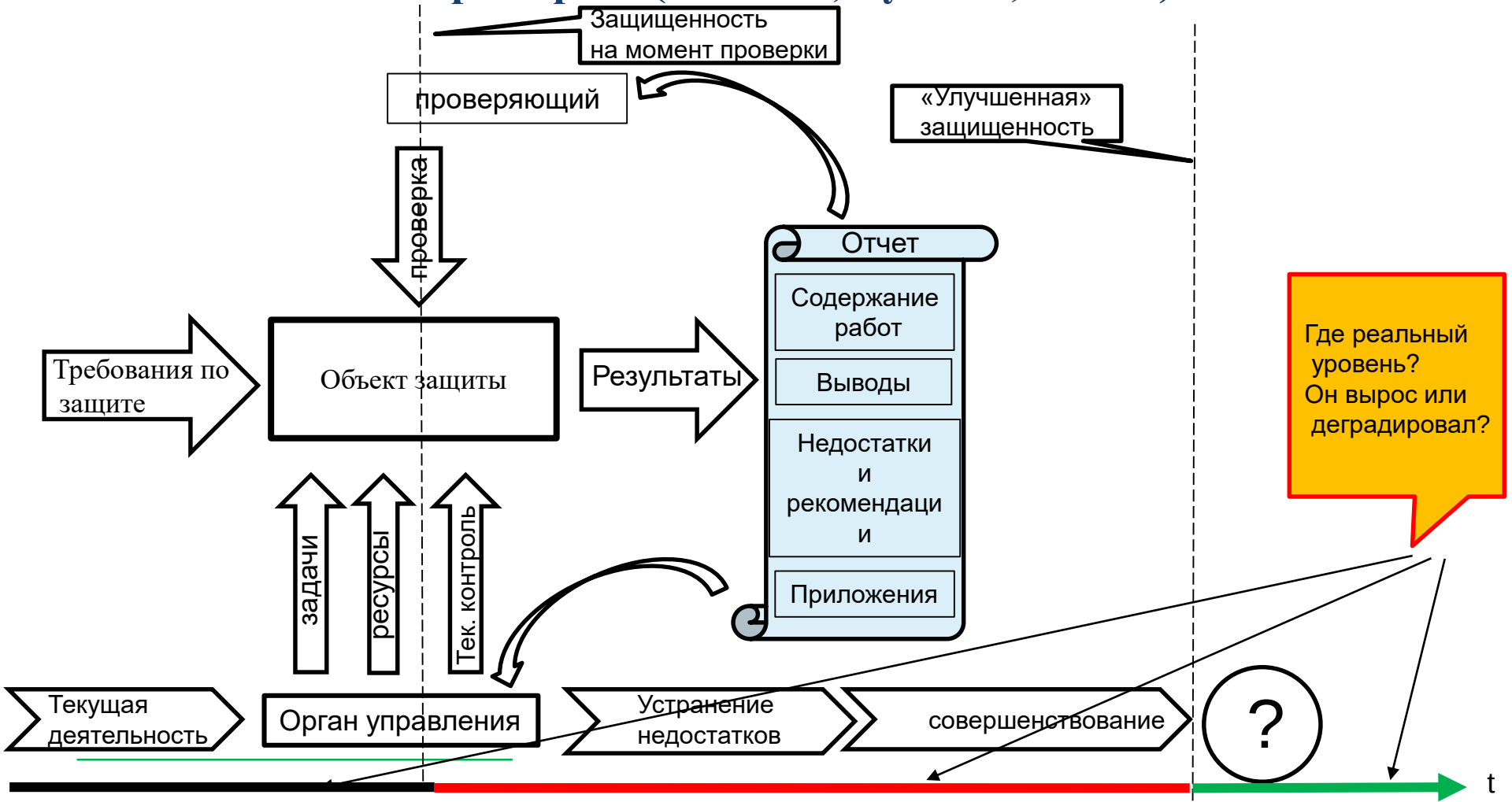
ЦБ РФ (на основе стандартов ISO) – шкала оценки с установленным регулятором критерием защищенности.

?

14 видов контролей в настоящее время



Жизненный цикл проверки (оценки, аудита, теста)



Причины:

Анархия в проверках и оформлении их результатов
Неоптимальная методология проверок

Итог:

Сложно.
Не контролируемо.
Не дает реальной картины.
Высокие трудозатраты.
Дальнейшее усложнение картины и перегрузка служб ИБ.
Риски суровых административных и дисциплинарных санкций для персонала ИБ.
Дальнейшая децентрализация в регулировании.

Следствие:

В стране 500 000 объектов КИИ из них 35 тыс ЗО КИИ из них 10% в реестре
В ходе проверок ФСТЭК выявляет по 800 нарушений в год
Составлено более 160 протоколов об административных правонарушениях

FBK | CS cybersecurity

Что делать и что можно сделать (быстро, на первом этапе).

1. Привести результаты всех имеющихся контролей к стандартному унифицированному виду, позволяющему централизованно обобщить их, хранить и анализировать имеющиеся данные, делать более точные выводы о состоянии уровня защищенности «внутри цикла оценки» и применять адресные воздействия.
2. Применить как унифицированный подход методологию оценки зрелости процессов.
3. Ввести реестры процессов обеспечения защиты для каждого объекта как основу (классификатор) методик проверки, анализа и экспертизы.
4. Обеспечить:
   - регулярный централизованный сбор (представление) отчетности от всех контролируемых объектов защиты;
   - регулярный сбор отчетности об устранении выявленных недостатков и контроле (самооценке) показателей зрелости процессов обеспечения СОИБ
5. Организовать на объектах по возможности частый и регулярный контроль
   Использовать технологии ИИ для анализа больших массивов данных технического аудита.

Немного определений

- **Процесс:** Обычно – набор практик, находящихся под влиянием политик и процедур предприятия, который получает на вход ресурсы (включая результаты других процессов), преобразует их и создает результат (выходы, то есть продукты и услуги).

  Замечание по охвату: для существования процессу необходимо иметь ясную бизнес-причину, подотчетного владельца, четкое закрепление ролей и обязанностей за исполнение процесса и средства измерения производительности.

- **Метрика:** Поддающаяся количественному исчислению сущность, которая позволяет измерить степень достижения целей процесса. Метрика должна соответствовать принципам SMART (то есть быть конкретной, измеримой, достижимой, актуальной и привязанной к промежутку времени). Подход к определению метрик должен включать единицы измерения, частоту измерения, эталонное значение (если таковое применимо), а также процедуру измерения и процедуру интерпретации результатов измерения.

- **Атрибут:** (возможностей) процесса Согласно стандарту ISO/IEC 15504: измеримая характеристика возможностей процесса, применимая к любому процессу.

Возможный общеметодологический подход

1. Следует рассматривать описание защищенности объекта защиты в форме многомерного информационного куба (OLAP), каждая ячейка которого содержит информацию о проведенном контроле (реализуемом процессе) и их результатах. Результаты представляются по шкале оценки зрелости на основе методологии построения модели зрелости процессов.
2. Использование системы интегральных оценок результатов контролей на основе методологии построения модели зрелости процессов СОИБ.

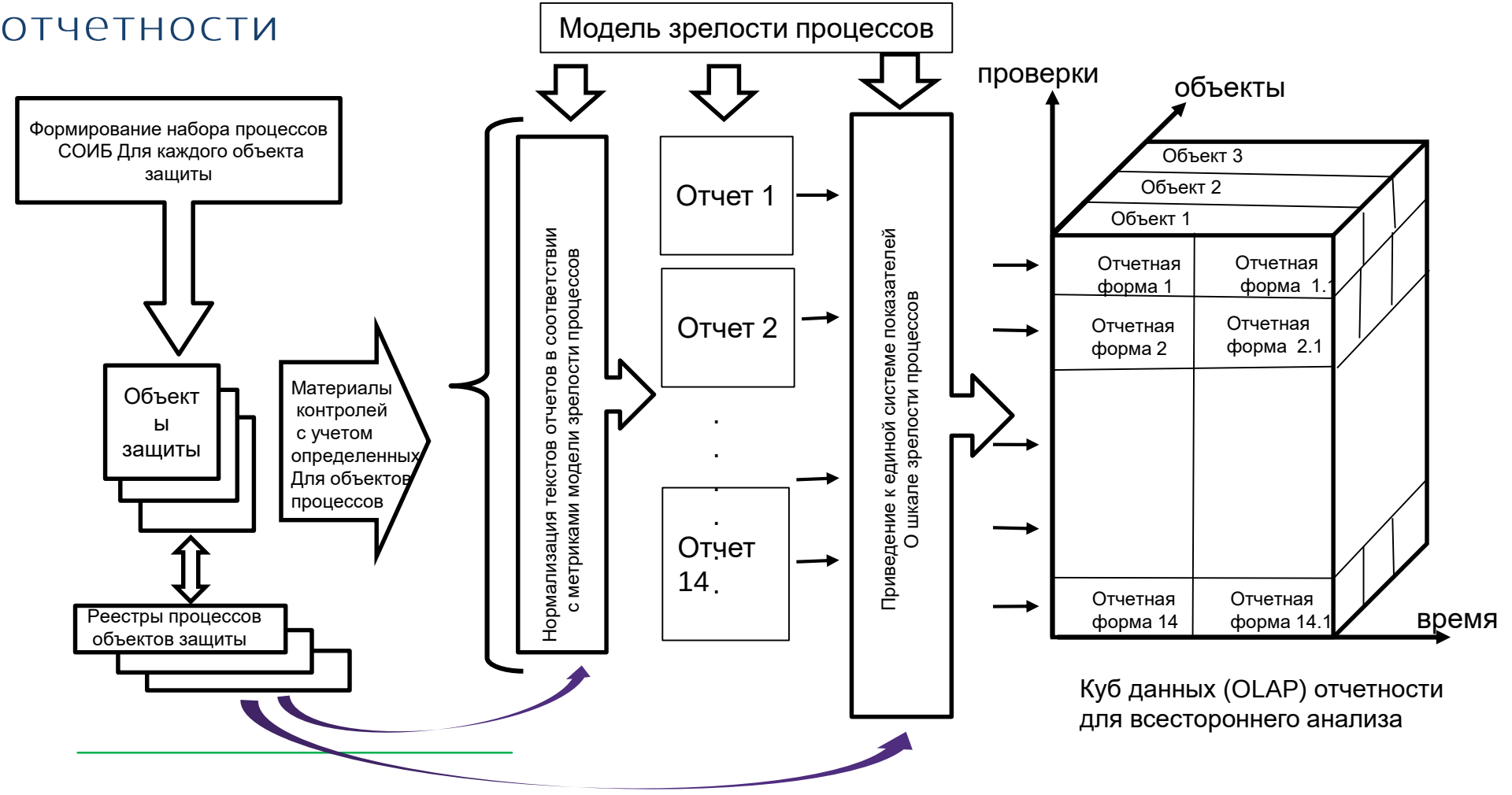
   Модель зрелости процессов СОИБ строится на базе группы стандартов ГОСТ Р 15504 и стандарта COBIT 4.1
3. Идентификация процессов СОИБ для каждого объекта, разработка реестра процессов и контролей и включение его в паспорт объекта.

   В реестр включаются:

   Все идентифицированные процессы (по документам ФСТЭК) обеспечения СОИБ с указанием их зрелости по шкале модели зрелости.

   Все результаты проверок и аудитов, с указанием оснований для их проведения, с указанием даты, исполнителя и способа проверки с указанием их зрелости по шкале модели зрелости.
4. Организация системы сбора отчетности по результатам деятельности защищаемых объектов.
5. Отчетные формы разрабатываются на основе и с учетом реестров процессов и контролей.
6. Центральная часть системы сбора отчетности включает систему сбора и хранения информации, а также информационно- аналитическую систему.

Общая схема формирования интегрированной отчетности



Куб данных (OLAP) отчетности для всестороннего анализа

Пример подхода к преобразованию результатов проверок

Методика инструментального тестирования

Цели проверки:

получение независимой/инструментальной оценки текущего состояния настроек системы информационной безопасности и связанной инфраструктуры

Содержание работ:

Внешнее тестирование
Внутренне тестирование
Исследование мобильных приложений
Анализ уязвимостей

} Форма заключения – текстовая, произвольная + приложения

Переход от изложения результатов проверки в произвольной форме к формализованной оценке по шкале зрелости

1. Определяются процессы(процессы), в том числе:
   - Внешнее тестирование
   - Внутренне тестирование
   - Исследование мобильных приложений
   - Анализ уязвимостей
   - Устранение замечаний

2. Устанавливаются метрики для каждого процесса (Максимальное значение метрики - полное отсутствие уязвимостей и слабостей по каждому направлению).

3. Устанавливается уровень зрелости каждого процесса в соответствии с метриками.

4. Составляется формализованный отчет содержащий показатели каждого процесса, представленные в форме матрицы зрелости процессов.

Устанавливается регламент сбора отчетности по установленным формам.

5. ~~Составляется база данных в форме OLAP к~~уба, позволяющего проводить всесторонний анализ данных по всей совокупности объектов защиты..

FBK | CS
cybersecurity

Контакты

Андрей Курило
Советник по вопросам информационной безопасности

+7 (495) 737 53 53 доб. 3037

+7 (495) 970-41-32
Sales@fbkcs.ru
Info@fbkcs.ru