
A 3
B 3
A 4
B 4
ЭЛВИС-ПЛЮС

Типовые решения по защите промышленных объектов КИИ

Оптимизация подходов к выбору мер по защите промышленных объектов КИИ от угроз безопасности информации на основе БДУ ФСТЭК России

Акименко Владимир

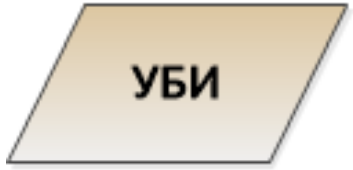
Руководитель Центра кибербезопасности критических инфраструктур АО «ЭЛВИС-ПЛЮС»

7 простых шагов по приведению в соответствие 187-ФЗ

1. Принятие решения о необходимости обеспечения безопасности (ОБ) объектов КИИ (ОКИИ)
2. Инвентаризация и категорирование ОКИИ
3. Оценка текущего состояния и определение требований по ОБ значимых ОКИИ (ЗО КИИ)
4. Определение (разработка) комплекса мер по ОБ ЗО КИИ
5. Создание и организация работы подразделения/ специалистов по безопасности
6. Реализация (внедрение) комплекса мер по ОБ ЗО КИИ
7. ОБ ЗО КИИ в ходе их эксплуатации, развития и вывода из эксплуатации

Определение требований по обеспечению безопасности ЗОКИИ

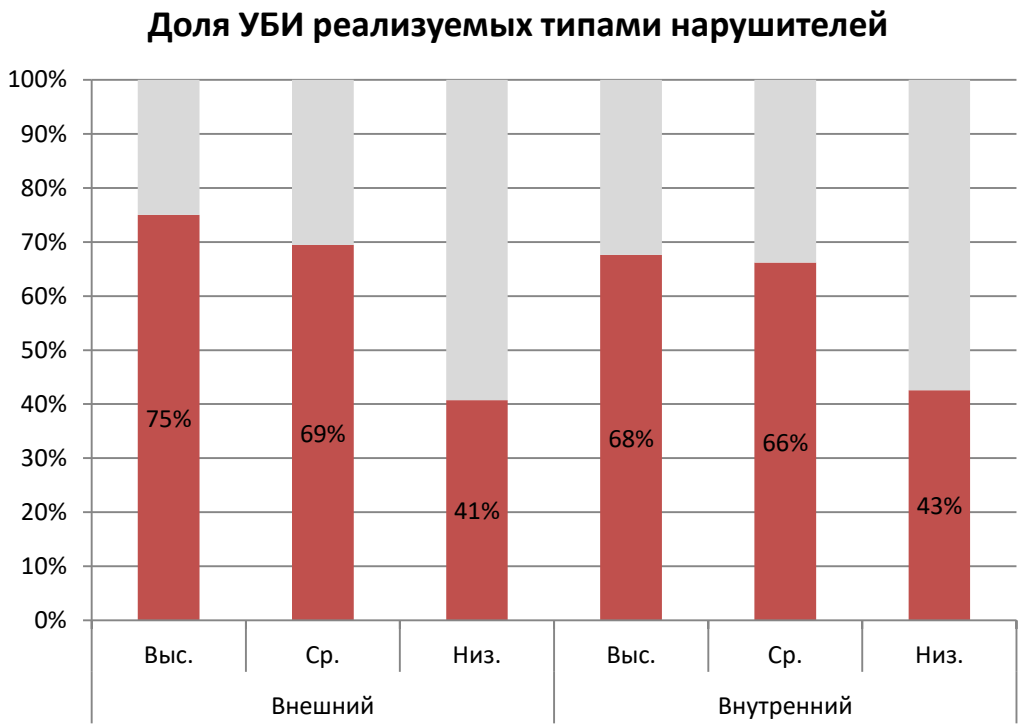
Угроза безопасности информации (УБИ) - совокупность условий и факторов, создающих опасность нарушения безопасности информации (КДЦ)



Источник угрозы
Объект воздействия
Уязвимость
Способ реализации
Последствия (КДЦ)

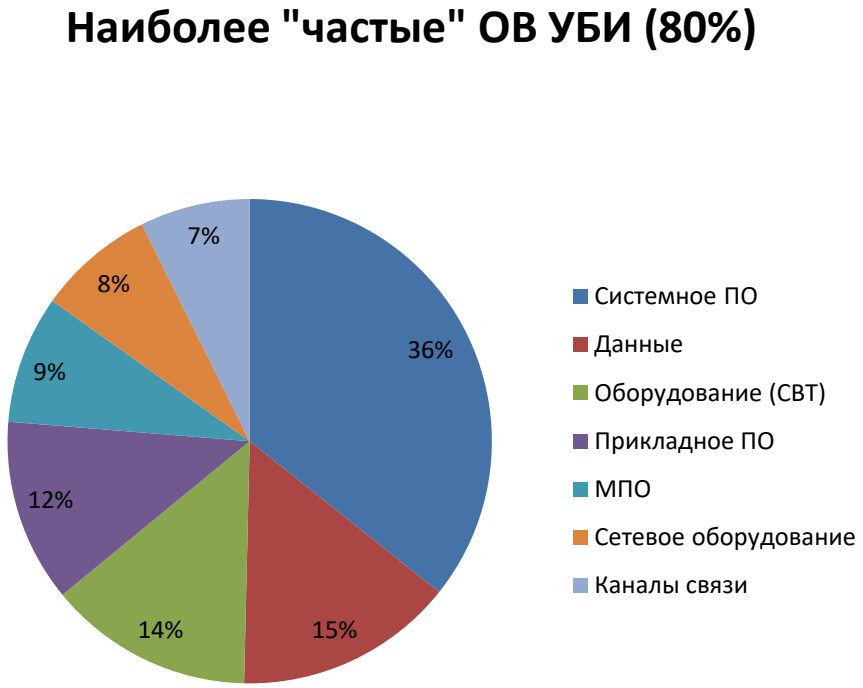
*Приказ 239-П (пункт 11.1) «…в качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз….» (БДУ)

БДУ ФСТЭК России (источники угроз - нарушители)



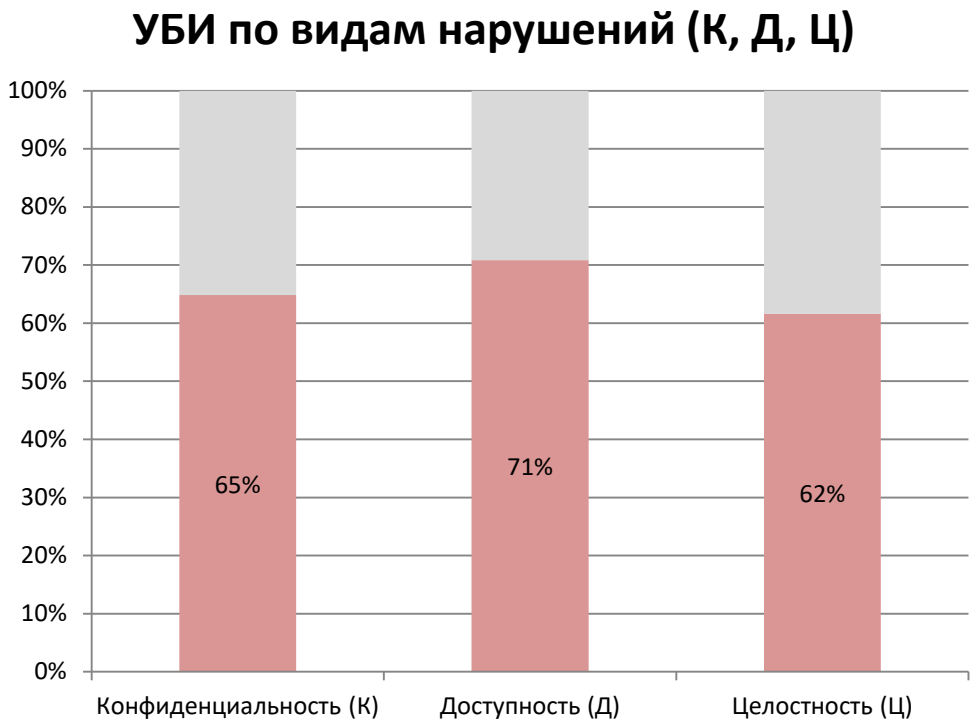
* Количество угроз, реализуемых нарушителем с высоким потенциалом – 5%

БДУ ФСТЭК России (объекты воздействия)



*Всего в БДУ разных (по формулировкам) ОВ – 55 типов

БДУ ФСТЭК России (виды нарушений БИ)



*УБИ, нарушающие только Ц и/или Д, составляют 81%

БДУ ФСТЭК России (уязвимости, сценарии)

*Количество УБИ, обусловленных уязвимостями/«слабостями» ПО – 37%

БДУ ФСТЭК России (меры противодействия)

#	Группы угроз	Мера, механизм защиты
1	Использование "слабостей" приложений	Анализ программного кода, безопасная разработка, сертификация по требованиям безопасности, техническая поддержка и сопровождение
2	Нарушение установленных процедур (правил, настроек, контроля)	Регламентация и установление ответственности, организация и контроль выполнения процессов обеспечения ИБ, функциональное тестирование, нагрузочные испытания, проведение тестов на проникновение, аудит ИБ
3	Воздействие вредоносного кода	Антивирусная защита
4	Преднамеренное деструктивное использование санкционированных возможностей	Управление идентификацией и доступом, регламентация и установление ответственности, регистрация и анализ событий ИБ
5	Обход механизмов идентификации и аутентификации	Аудит ИБ, проведение тестов на проникновение, анализ кода, сертификация по требованиям безопасности
6	Обход механизмов управления доступом	Аудит ИБ, проведение тестов на проникновение, анализ кода, сертификация по требованиям безопасности
7	Использование слабостей технологий сетевого обмена	Межсетевое экранирование, защита периметра и каналов связи, применение протоколов с функциями безопасности
8	Исследование инфраструктуры	Применение межсетевого экранирования, настройка сетевых служб, использование систем обнаружения вторжений, анализ событий
9	Необоснованно завышенный уровень доверия к разработчику	Внедрение стандартов, требований к разработке и внедрению
10	Технический сбой	Кластеризация, резервирование, резервное копирование и восстановление, техническая поддержка и сопровождение
11	Социальная инженерия	Обучение, инструкции, правила, проведение семинаров, проверка знаний
12	Нарушение целостности инфраструктуры	Инвентаризация, контроль и фиксация изменений, управление изменениями (конфигураций, политик, правил)

БДУ ФСТЭК России («эффективность» мер противодействия)

*Меры, направленные на снижение уязвимостей/«слабостей» ПО – 20%

СБ ЗОКИИ (организационные меры)

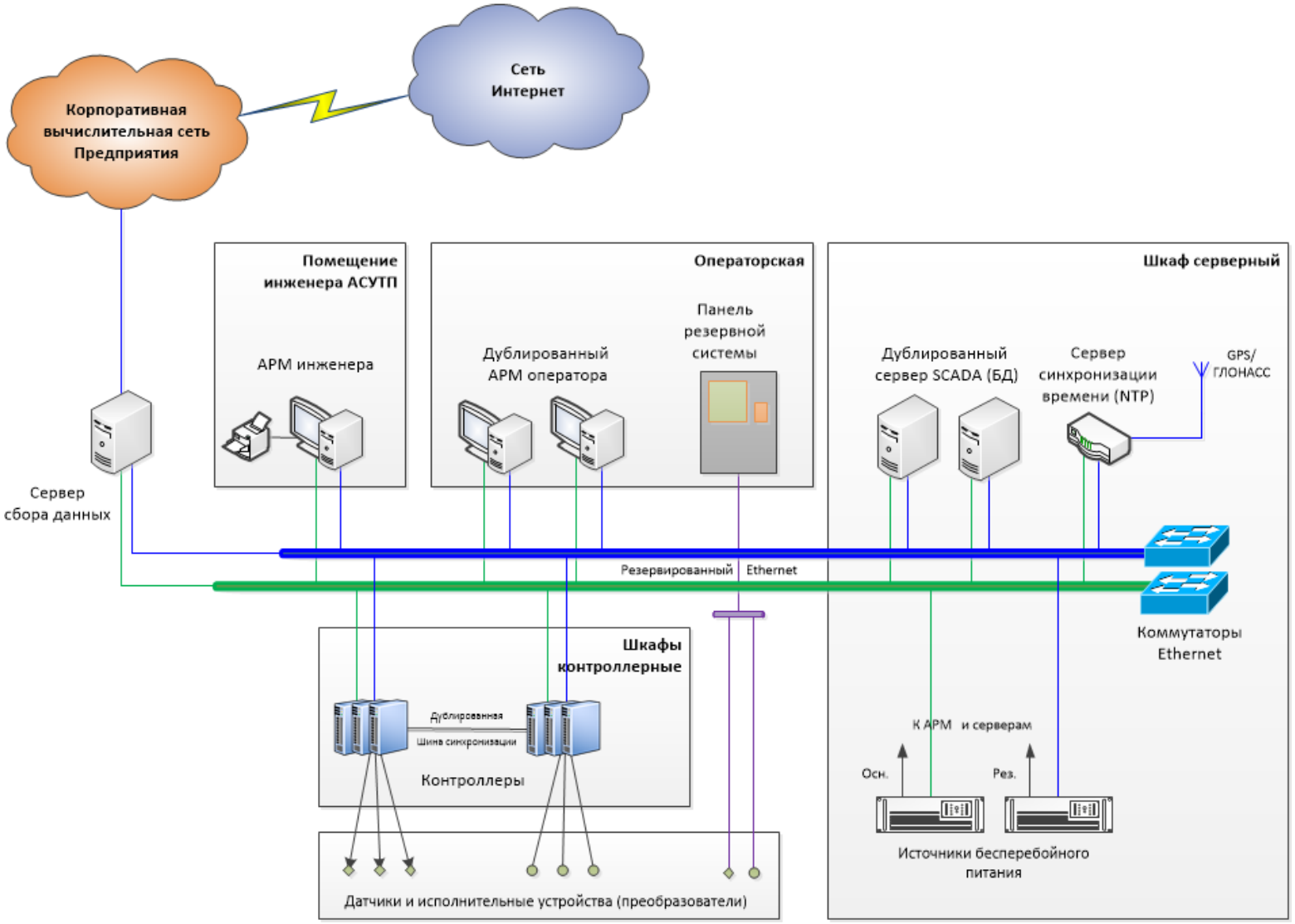
Мероприятия (меры)	Документ (тип документа)
Регламентация требований	Стандарты, политики
Регламентация процессов (обеспечение, контроль)	Регламенты, инструкции
Установление ответственности	Приказы, положения, ДИ
Проведение тестов на проникновение	Программы, методики
Анализ программного кода, сертификация по требованиям безопасности	Программы, методики, сертификаты, аттестаты
Функциональное, нагрузочное тестирование, техническая поддержка и сопровождение	Договоры, соглашения (треб-я к услугам, сервису)
Внедрение стандартов безопасной разработки	Стандарты, требования
Инвентаризация, управление и контроль изменений (конфигураций, политик, правил)	Политики, ведомости, реестры, инструкции
Повышение квалификации	План обучения, журналы проверки знаний
*Физическая защита ТС и периметра	Положение, регламент, инструкции
*Выявление и реагирование на инциденты	План реагирования
*Восстановление работоспособности	План восстановления

СБ ЗОКИИ (технические меры)

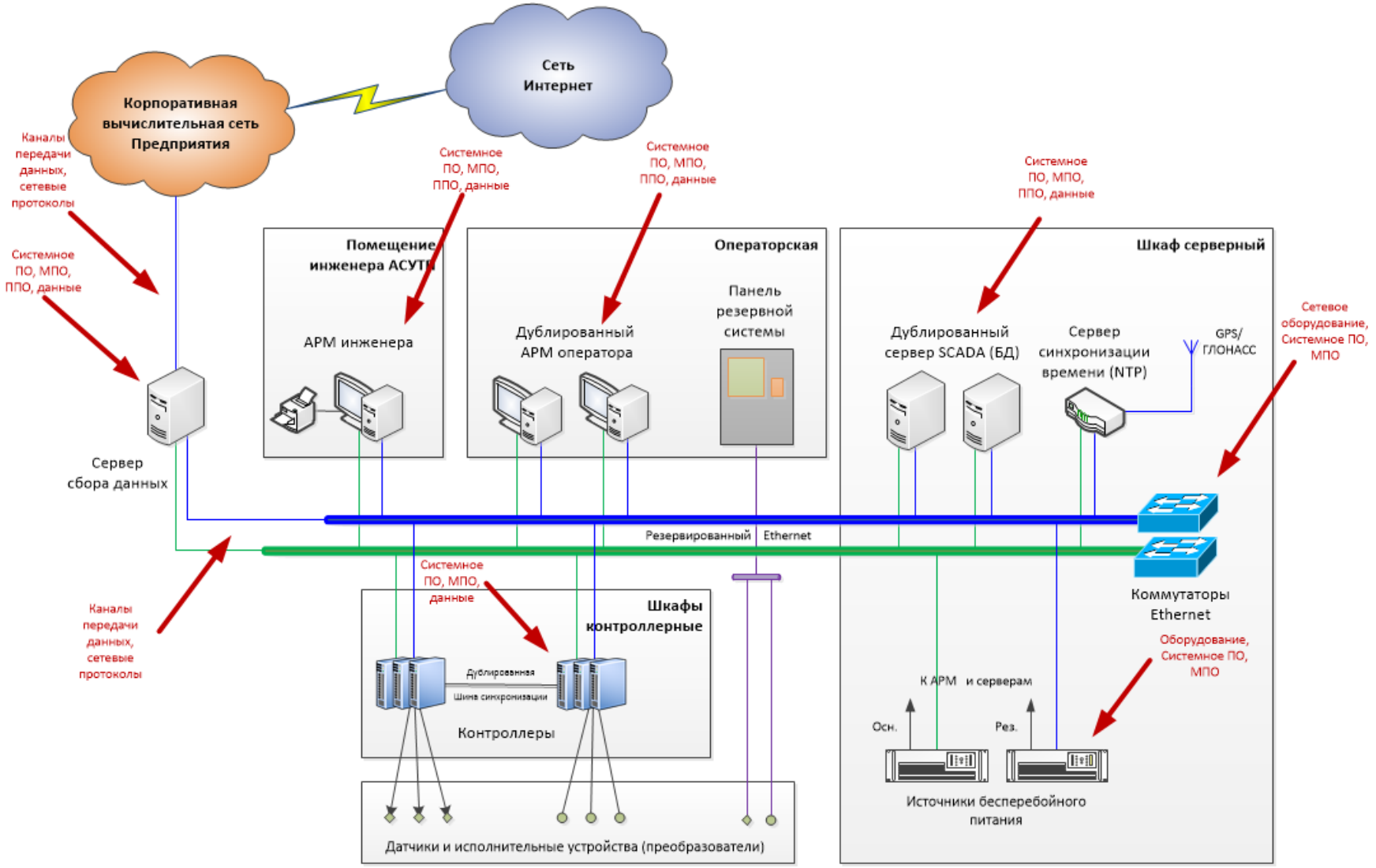
Технические (меры)	Реализация
Межсетевое экранирование, защита периметра и каналов связи	Средства межсетевого экранирования (+VPN)
Антивирусная защита	Средства антивирусной защиты
Управление идентификацией и доступом	Встроенные функции в МПО, СПО, ППО (идент., доступ)
Настройка сетевых служб, применение систем (средств) обнаружения вторжений	Встроенные функции в МПО, СПО, ППО (доп. функции), Встроенные в средства МЭ функции IDS/IPS
Регистрация и анализ* событий ИБ	Встроенные функции в МПО, СПО, ППО (регистрация событий)
Кластеризация, резервирование, резервное копирование и восстановление	СВТ, съемные носители, специализированные средства

*Средства анализа событий используются в рамках процесса выявления и реагирования на инциденты ИБ (за скобками).

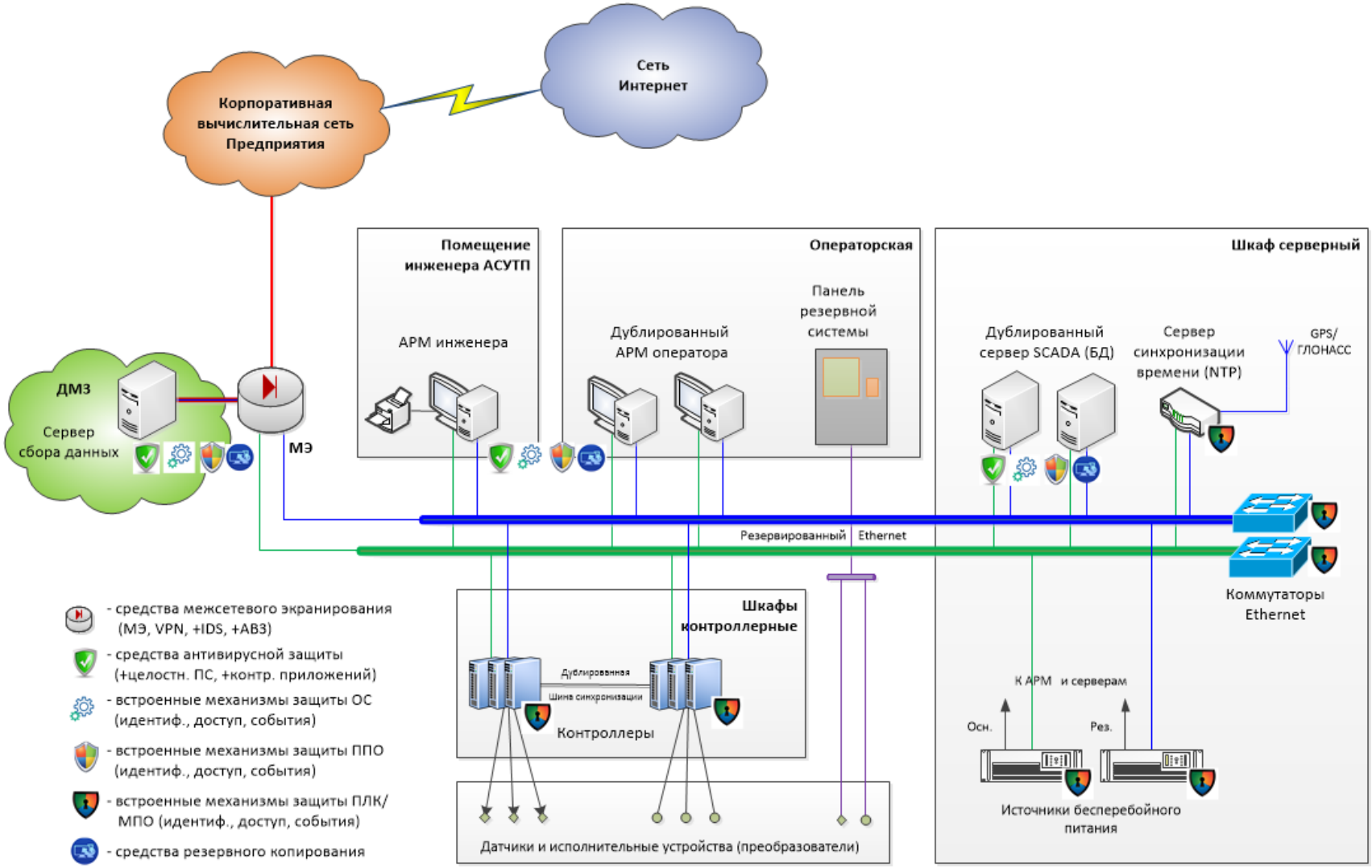
ОКИИ (типовая структура АСУТП)



Основные виды УБИ (векторы воздействия угроз)



СБ ЗОКИИ (реализация технических мер)



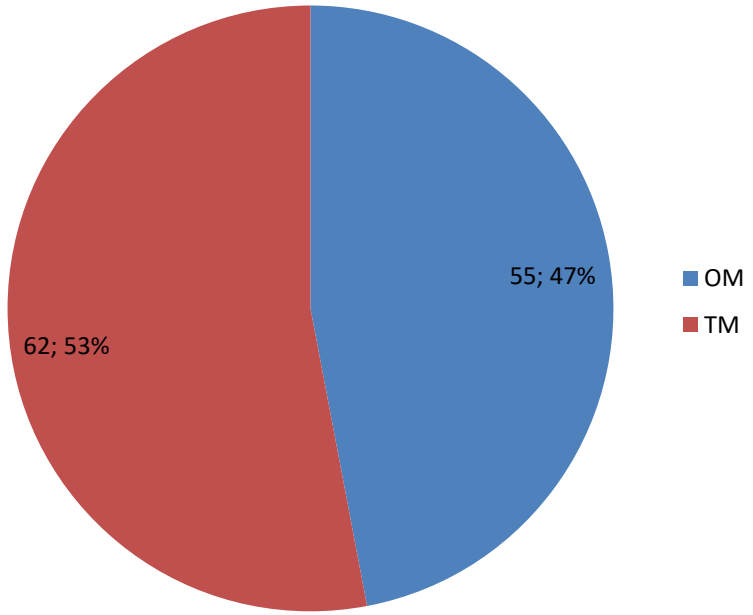
Нормативные требования по обеспечению безопасности ЗОКИИ

Приказ 239-П «Об утверждении требований по обеспечению безопасности…»

17 групп мер (ИАФ, УПД, ОПС, ЗНИ, АУД, АВЗ, СОВ, ОЦЛ, ОДТ, ЗТС, ЗИС, ПЛН, УКФ, ОПО, ИНЦ, ДНС, ИПО)

Всего 134 меры (без учета категории)
117 обязательных мер для 1 категории
98 обязательных мер для 3 категории

Структура мер (ОМ/ТМ) 239-П (1 кат.)



*Не учитываются требования Приказов ФСБ, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак

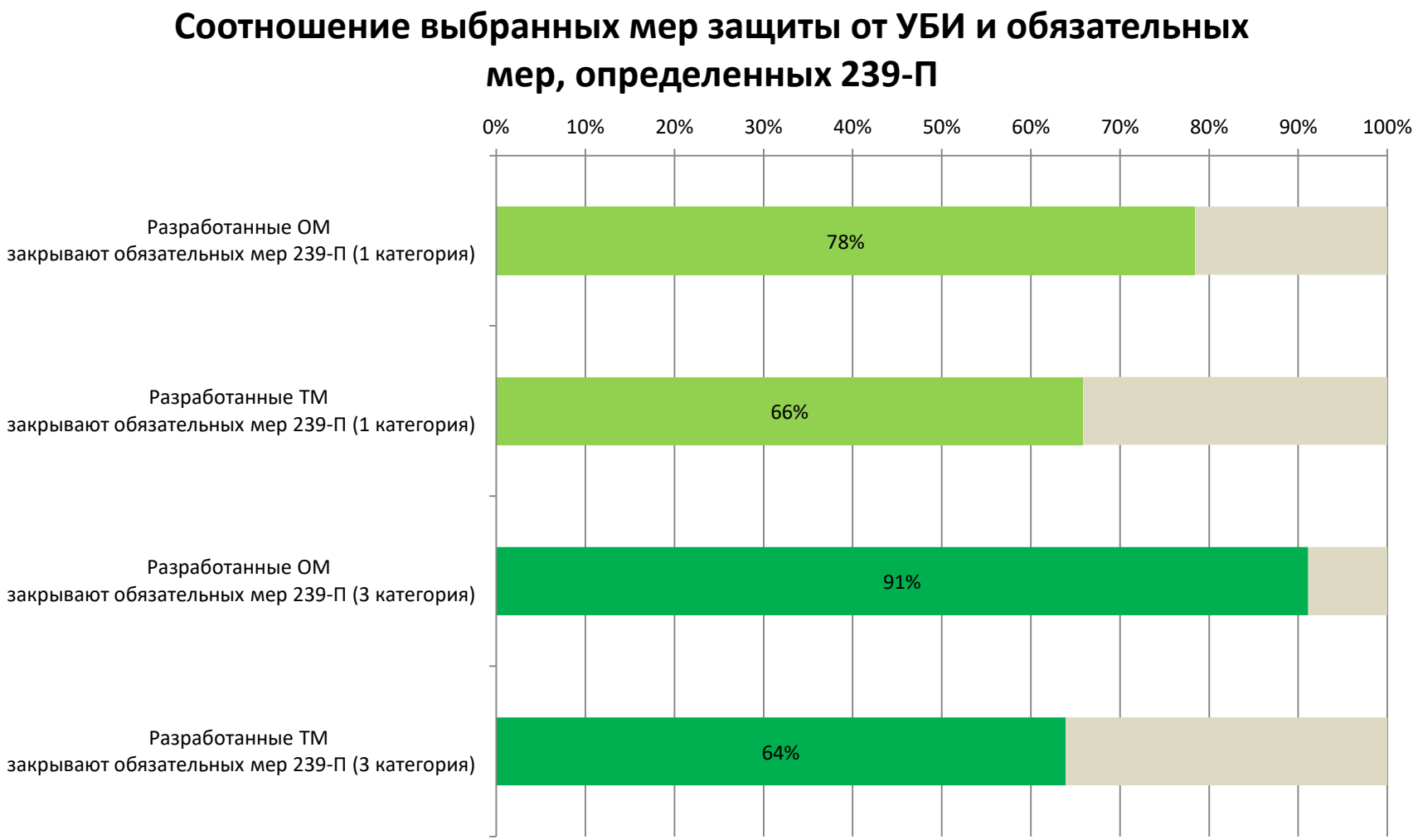
СБ ЗОКИИ (организационные меры по УБИ vs меры по 239-П)

Мероприятия (меры) по УБИ	Мероприятия (меры) по 239-П
Регламентация и установление ответственности	«Нулевые» меры + ОПС.3, ОДТ.1, ОДТ.2, ОДТ.3, ПЛН.1, ПЛН.2, ДНС.4
Проведение тестов на проникновение	АУД.2
Анализ программного кода, сертификация по требованиям безопасности	АУД.2
Функциональное, нагрузочное тестир-е, техническая поддержка и сопровождение	239-П (п.31 в части технической поддержки производителя)
Внедрение стандартов безопасной разраб.	239-П (п.11.2 в части разработки ПО)
Инвентаризация, управление и контроль изменений (конфиг., политик, правил)	ЗНИ.1, АУД.1, УКФ.2, УКФ.3, ОПО.1, ОПО.2, ОПО.3, ОПО.4
Повышение квалификации	ИПО.1, ИПО.2, ИПО.3, ИПО.4
*Физическая защита ТС и периметра	ЗНИ.2, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5, ДНС.3
*Реагирование на инциденты	ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.5, ИНЦ.6
*Восстановление работоспособности	ИНЦ.4, ДНС.2, ДНС.5, ДНС.6

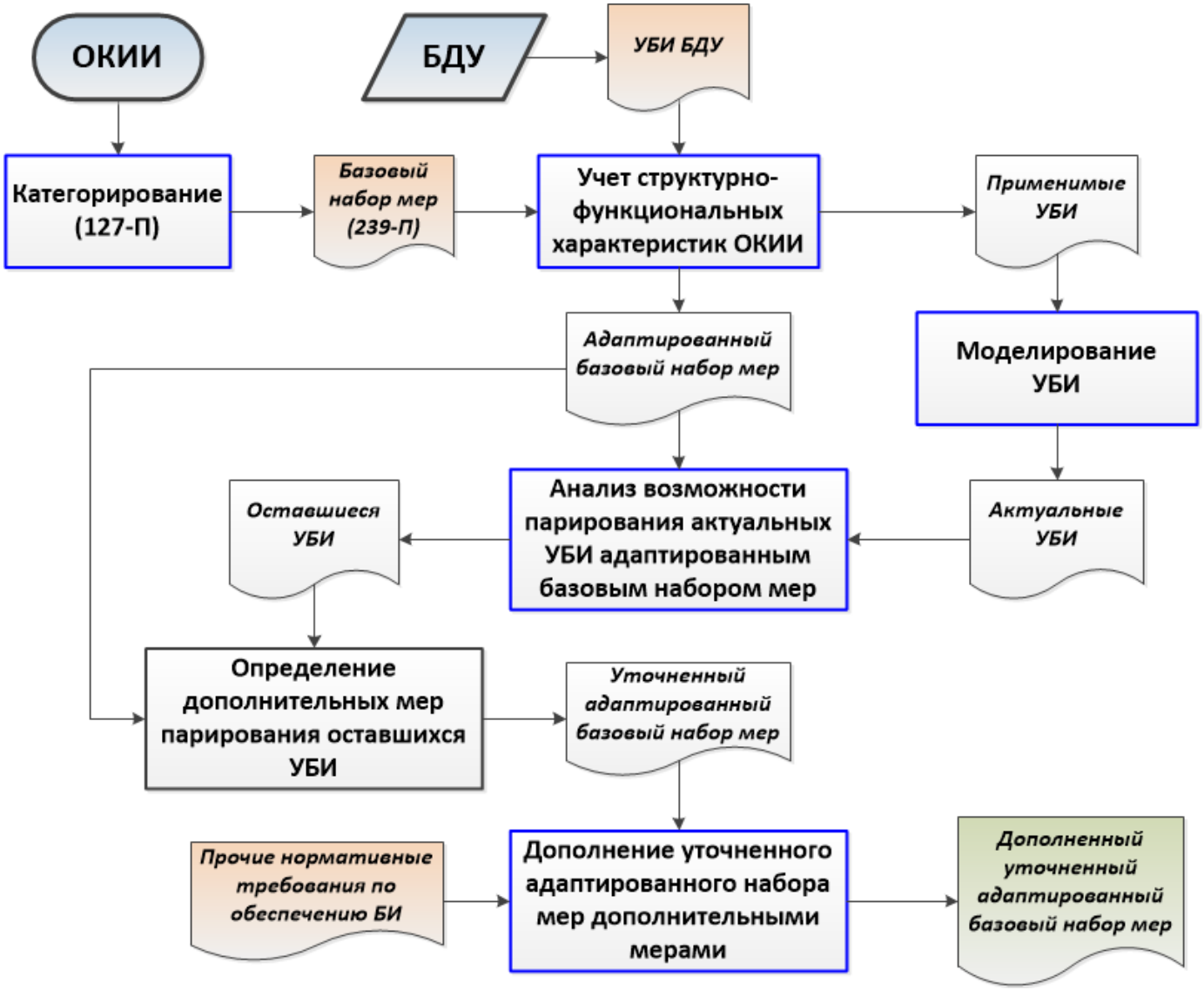
СБ ЗОКИИ (технические меры по УБИ vs меры по 239-П)

Мероприятия (меры) по УБИ	Мероприятия (меры) по 239-П
Межсетевое экранирование, защита периметра, защита каналов связи	АУД.5, ЗИС.2, ЗИС.3, ЗИС.4, ЗИС.5, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.27, ЗИС.33, ЗИС.34, ЗИС.35
Антивирусная защита	АВЗ.1, АВЗ.2, АВЗ.4, ОЦЛ.1, ЗИС.16
Управление идентификацией и доступом (встроенные механизмы)	ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, ЗИС.1
Настройка сетевых служб, примен. средств обнаружения вторжений	АУД.5, СОВ.1, СОВ.2
Регистрация и анализ* событий ИБ (встроенные механизмы)	АУД.4, АУД.6
Резервное копирование и восстановление	ОДТ.4, ОДТ.5, ОДТ.6

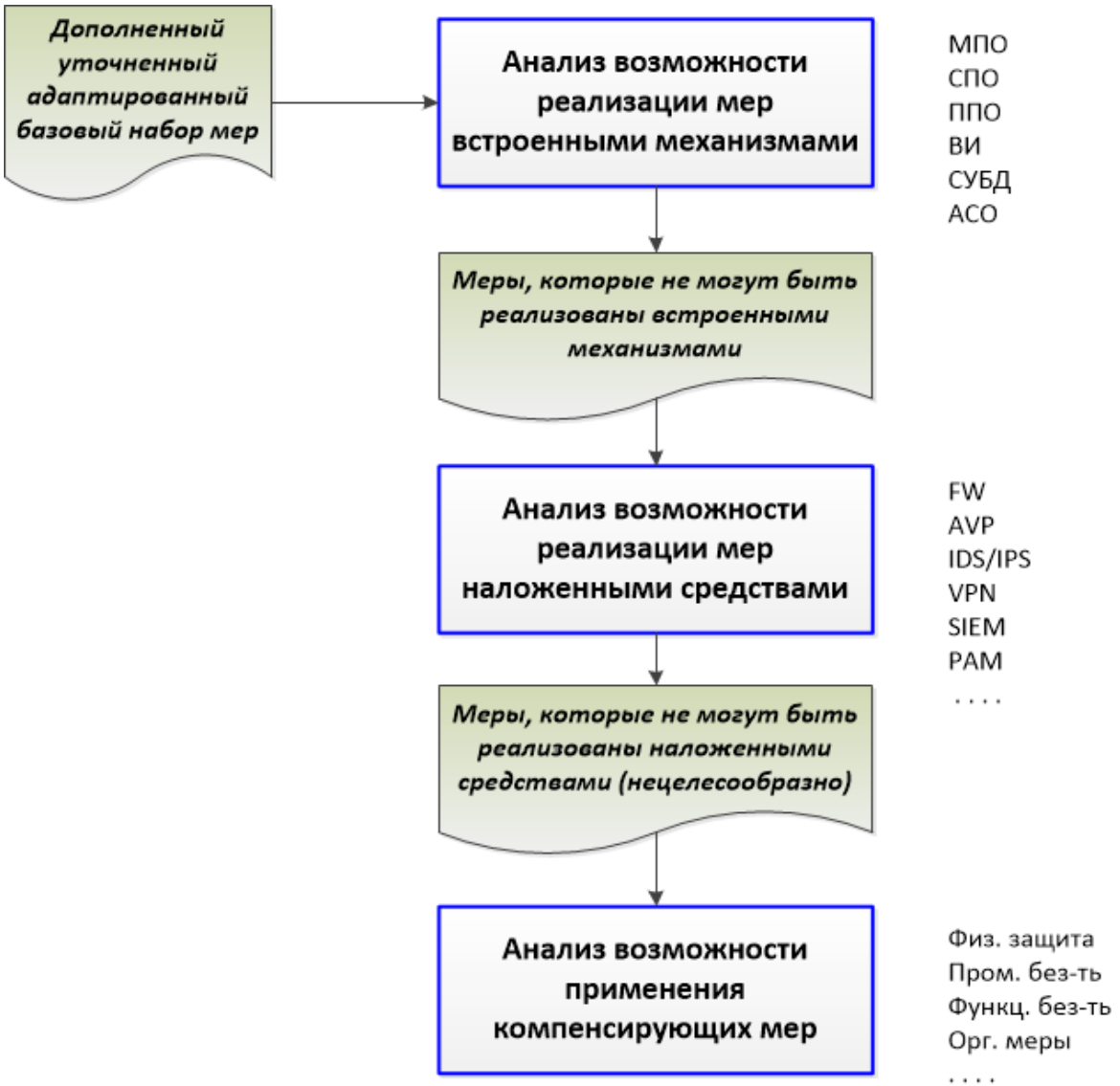
СБ ЗОКИИ (степень выполнения обязательных мер 239-П)



СБ ЗОКИИ (выбор состава мер)



СБ ЗОКИИ (выбор средств реализации мер)



СПАСИБО ЗА ВНИМАНИЕ!

Акименко Владимир

Руководитель Центра кибербезопасности критических инфраструктур АО «ЭЛВИС-ПЛЮС»
avv@elvis.ru
8(495)276-0211
8(985) 766-4636 моб.