информзащита

Безопасность дочерних зависимых обществ

Марат Цихмистров
Руководитель направления технической экспертизы,
«Информзащита»

кибербезопасность
в эпоху перемен

информзащита

Централизованный подход

кибербезопасность
в эпоху перемен

Безопасность дочерних зависимых обществ

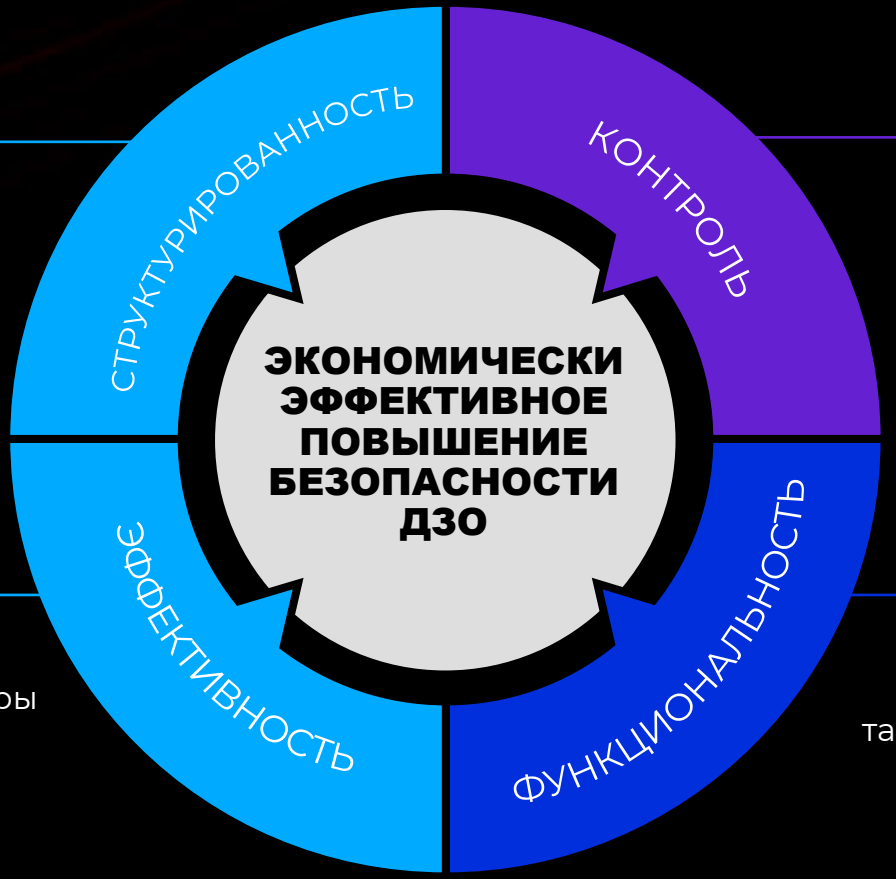
Принципы и цели централизованного подхода к защите ДЗО

ЦЕНТРАЛИЗАЦИЯ УПРАВЛЕНИЯ ИБ И СЗИ

Стандартизация, планирование и управление ИБ для ДЗО централизовано в ГО и реализовано в SLA / контрактах

АДЕКВАТНОСТЬ ПРИМЕНЯЕМЫХ МЕР

Организационные и технические меры ИБ отвечают профилю угроз для той или иной ДЗО



ОПЕРАЦИОННЫЙ КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ

Ведется постоянный контроль защищенности ДЗО, основанный на анализе применяемых СЗИ, процессов ИБ, метрик защищенности

ШЭРИНГ ФУНКЦИЙ ИБ

Функции ИБ выполняются персоналом на уровне ДЗО (оперативный и тактический уровни), ГО (стратегический уровень), налажена структура взаимодействия в случае ЧС

Компоненты защиты ДЗО

кибербезопасность
в эпоху перемен

информзащита

01 СТАНДАРТЫ И ТРЕБОВАНИЯ ИБ
В зависимости от вида деятельности, вырабатываются стандарты и требования ИБ, основанные на требованиях законодательства и бизнес-целях ГО и ДЗО. Стандарты и требования применяются с учетом типа ДЗО или вида деятельности контрагента

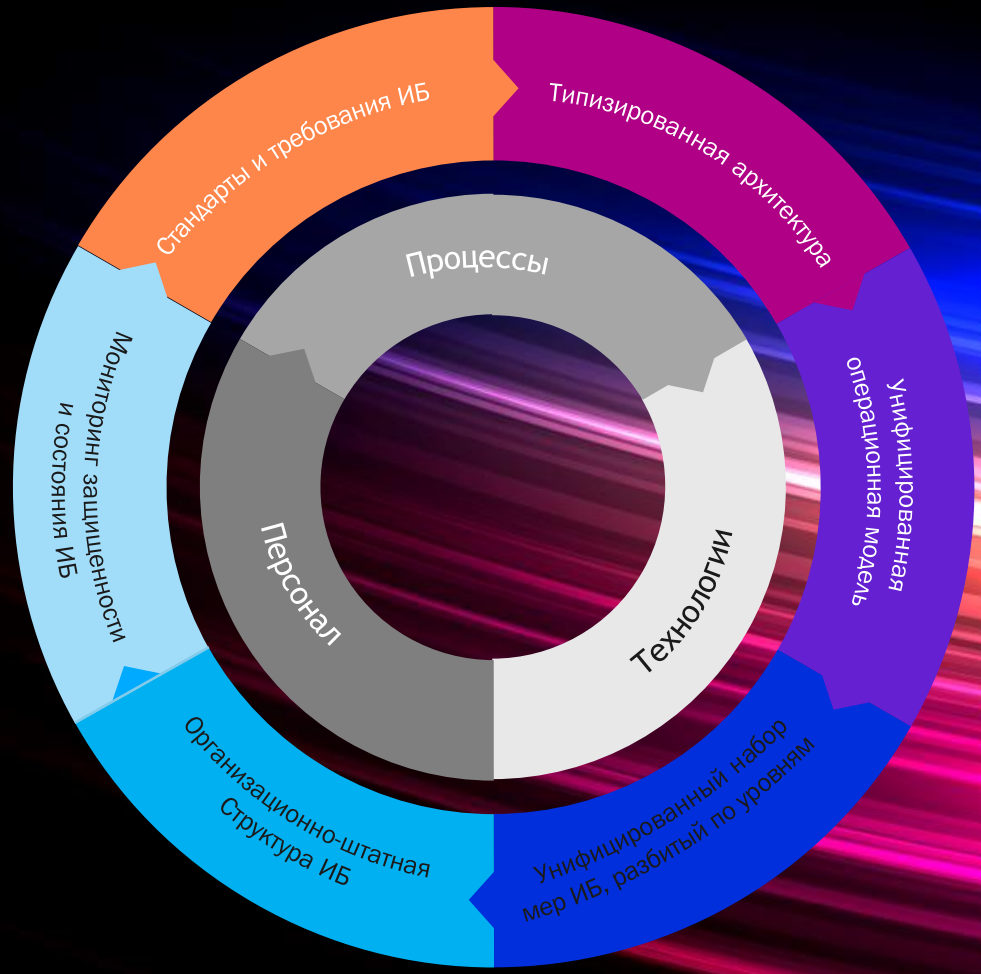
02 ТИПИЗИРОВАННАЯ АРХИТЕКТУРА
Определены шаблоны архитектуры ИБ для различных типов ДЗО (критерии типизации фиксируются в программе безопасности ДЗО), продиктованные требованиями ИБ. Для контрагентов применяется ограниченно, в части взаимодействия

03 УНИФИЦИРОВАННАЯ ОПЕРАЦИОННАЯ МОДЕЛЬ
Операционная модель ИБ ДЗО определяется на основании требований и стандартов ИБ, выделенного шаблона архитектуры ИБ.

04 УНИФИЦИРОВАННЫЙ НАБОР МЕР ИБ, РАЗБИТЫЙ ПО УРОВНЯМ
Технические и организационные меры ИБ, применяемые в ДЗО, распределяются по последовательно достигаемым уровням безопасности. Достижение уровней заложено в дорожную карту, отталкиваясь от изначального уровня безопасности ДЗО

05 ОРГАНИЗАЦИОННО-ШТАТНАЯ СТРУКТУРА ИБ
Организационно-штатная структура учитывает особенности бюджетирования ДЗО и включает в себя распределение функций по ГО, ДЗО и подрядчикам / аутсорсерам

06 МОНИТОРИНГ ЗАЩИЩЕННОСТИ И СОСТОЯНИЯ ИБ
Обязателен контроль исполнения дорожной карты, процессов ИБ и регулярные проверки защищенности (экспресс-аудит, пентест, багбаунти, киберучения)



Подход к защите ДЗО и результаты

кибербезопасность **в эпоху перемен**

информзащита

АНАЛИЗИРУЕМ И ПРОРАБАТЫВАЕМ КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ	МЕТОДЫ И РЕШЕНИЯ	КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ
Управление ИБ-архитектурой, существующие и планируемые технические решения	Типовые решения в технической и организационной части	На уровне Головного офиса: • Оптимизация финансовых и временных затрат на защиту ДЗО • Повышение защищенности ДЗО • Постоянный контроль защищенности ДЗО На уровне ДЗО: • Систематизированный подход к защите ДЗО • Повышение безопасности существующих ИС • Рост эффективности используемых СЗИ • Оптимизация кадровых ресурсов ДЗО
Функционал службы ИБ, оптимальная организационная структура, распределение ответственности между ГО и ДЗО	Перераспределение компетенций	
Целевая процессная карта ИБ, взаимодействие с ГО и подрядчиками	Масштабирование решений	
Оценка защищенности ДЗО, используемые инструменты, метрики и показатели	Отказ от дублирования функций / СЗИ	
Управление ИБ: на основании чего расставляются приоритеты и принимаются решения	Готовые наборы стандартов, методик и документации	

Задачи по направлениям (1/2)

кибербезопасность
в эпоху перемен

информзащита

СТАНДАРТЫ И ТРЕБОВАНИЯ ИБ

- Типизация ДЗО по признакам (вид деятельности, категории обрабатываемой информации, ИТ-ландшафт, применимая модель угроз)
- Создание требований ИБ к ИТ- и ИБ-системам
- Создание вариантов архитектуры / реализации распространенных ИТ- и ИБ-систем
- Разработка и приведение в соответствие ВНД для управляющих и операционных процессов ИБ
- Разработка стандартов безопасной настройки и эффективной эксплуатации СЗИ
- Создание шаблонов ОРД для соответствия требований законодательства, применимых для того или иного типа ДЗО

ТИПИЗИРОВАННАЯ АРХИТЕКТУРА

- Централизация управления отдельными СЗИ, применяемыми в ДЗО
- Создание функциональных требований к СЗИ
- Разработка шаблонов архитектуры для различных типов ДЗО с учетом возможности централизации / локализации СЗИ
- Анализ вариантов реализации СЗИ в централизованном / локальном вариантах с точки зрения эффективности и стоимости
- Анализ необходимости миграции отдельных СЗИ в централизованный ЦОД

УНИФИЦИРОВАННАЯ ОПЕРАЦИОННАЯ МОДЕЛЬ

- Определение необходимого уровня защищенности ДЗО
- Определение минимального и оптимального перечня процессов ИБ для ДЗО
- Создание операционной модели ИБ для различных типов ДЗО
- Разработка модели взаимодействия управляющего центра ИБ в ГО с ДЗО
- Разработка модели аутсорсинга функций ИБ для операционных моделей
- Разработка метрик эффективности выполнения процесса
- Разработка каталога услуг и SLA / OLA для контроля уровня сервиса
- Разработка шаблонов ВНД и ОРД для регламентации операционных процессов ИБ и эксплуатации СЗИ

Задачи по направлениям (2/2)

кибербезопасность
в эпоху перемен

информзащита

ОРГАНИЗАЦИОННО-ШТАТНАЯ СТРУКТУРА ИБ

- Разработка организационно-штатной структуры ИБ для различных вариантов операционных моделей ИБ в ДЗО
- Определение требуемого штата сотрудников ИБ для каждого варианта ОШС и матрицы компетенций
- Разработка шаблонов ОРД для штата сотрудников ИБ
- Создание хабов ИБ

УНИФИЦИРОВАННЫЙ НАБОР МЕР ИБ, РАЗБИТЫЙ ПО УРОВНЯМ

- Определение набора мер для различных уровней защищенности
- Определение критериев достижения уровня защищенности
- Разработка шаблонов дорожных карт по достижению целевых уровней защищенности
- Разработка и актуализация шаблонов безопасной настройки для распространенных ИТ-активов (ОС, СУБД, веб-сервер, сетевое оборудование, офисные приложения)
- Реализация технических и организационных мер ИБ в ДЗО
- Разработка шаблонов / пилотирование планов восстановления после инцидента (DRP)

МОНИТОРИНГ ЗАЩИЩЕННОСТИ И СОСТОЯНИЯ ИБ

- Разработка методологии экспресс-оценки уровня защищенности ДЗО и порядка аудита ИБ ДЗО
- Разработка показателей для мониторинга уровня защищенности и управления ИБ ДЗО
- Реализация системы мониторинга показателей уровня защищенности и управления ИБ
- Внедрение сценариев принятия управленческих решений на основе пограничных значений показателей
- Планирование и проведение необходимых мероприятий инструментальной и организационной проверки защищенности (аудит, пентест, багбаунти, киберучения)

информзащита

Сервисный подход

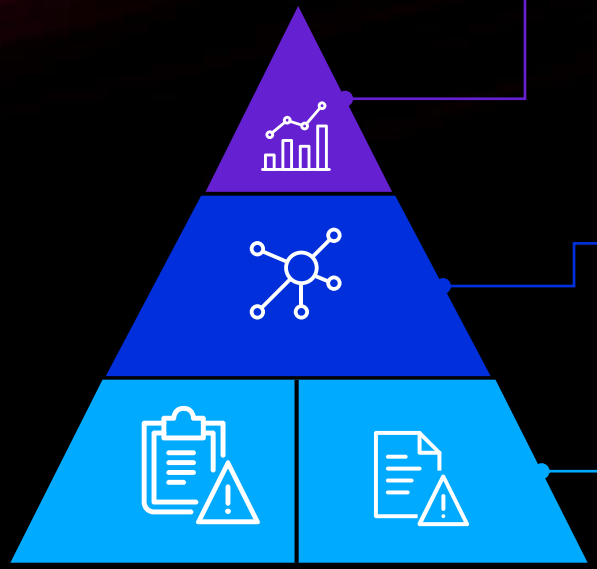
кибербезопасность
в эпоху перемен

Безопасность дочерних зависимых обществ

Сервисная модель ИБ для ДЗО

кибербезопасность **в эпоху перемен**

информзащита



Головной офис

- Головной офис (ГО) отвечает за стратегическое управление ИБ, аллокацию бюджета и высокоуровневое планирование задач / мер ИБ и развития каталога услуг
- Группа ответственных за ИБ-сервисы для ДЗО в Головном офисе состоит из руководства и экспертов, ответственных за функциональные области внутри компании
- Головной офис выполняет анализ регулярной отчетности по предоставляемым Сервисной группой услугам ИБ и принимает управленческие решения на их основе

Группа или компания, предоставляющая услуги ИБ

- Сервисная группа (СГ) ведет каталог услуг и отвечает за их предоставление ДЗО и уровень качества согласно заключенным SLA
- Сервисная группа отвечает за закупку, масштабирование и администрирование СЗИ, автоматизирующих тот или иной сервис ИБ, а также наличие компетентного персонала для управления ими
- Сервисная группа планирует и проводит аудит / обследование состояния ИБ в ДЗО, предоставляя результат Головному офису.
- При возникновении чрезвычайной ситуации (ЧС) отвечает за восстановление штатного уровня функционирования ДЗО

Дочерние и зависимые общества

- Дочерние и зависимые общества (ДЗО) являются объектом услуг ИБ
- ДЗО отвечают за своевременность и достаточность заказываемых услуг
- ДЗО принимает стандарты и требования ИБ, налагаемые Головным офисом
- При возникновении ЧС или инцидента ИБ ДЗО отвечают за своевременность и корректность оповещения и взаимодействие с Сервисной группой и Головным офисом

Подход к выстраиванию сервисной модели для ДЗО

кибербезопасность **в эпоху перемен**

информзащита

АНАЛИЗИРУЕМ И ПРОРАБАТЫВАЕМ КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ	МЕТОДЫ И РЕШЕНИЯ	КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ
Существующий и целевой каталог услуг, дорожная карта инициатив	Типы и уровни услуг ИБ для ДЗО	На уровне Головного офиса: • Оптимизация финансовых и временных затрат на защиту ДЗО • Повышение защищенности ДЗО • Постоянный контроль защищенности ДЗО На уровне ДЗО: • Систематизированный подход к защите ДЗО • Повышение безопасности существующих ИС • Рост эффективности используемых СЗИ • Оптимизация кадровых ресурсов ДЗО
Бизнес-модель предоставления услуг (ценообразование, центры затрат, расчет ROI)	Экономическая модель работы СГ	
Управление ИБ-архитектурой, существующие и планируемые технические решения в ДЗО	Архитектура и масштабирование СЗИ	
Функционал службы ИБ, оптимальная организационная структура, распределение ответственности между ГО, СГ и ДЗО	Отказ от дублирования функций / СЗИ	
Стандарты и требования ИБ, целевая процессная карта ИБ СГ, взаимодействие с ГО и ДЗО	Готовые наборы стандартов, методик и документации	
Используемые инструменты оценки защищенности ДЗО, SLA, метрики и показатели		

Задачи по направлениям (1/2)

кибербезопасность
в эпоху перемен

информзащита

УНИФИЦИРОВАННЫЙ НАБОР УСЛУГ ИБ

- Определение набора услуг ИБ для различных типов ДЗО и необходимых им уровней защищенности
- Определение направления развития каталога услуг в горизонте 2 лет
- Разработка дорожной карты создания СГ
- Определение критериев достижения уровня защищенности

БИЗНЕС-МОДЕЛЬ СГ

- Разработка бизнес-модели работы СГ
- Определение экономических показателей СГ и их требуемых значений на горизонте 2 лет
- Определение центров затрат
- Определение модели закупок и оплаты услуг, амортизации СЗИ и инфраструктуры
- Определение ROI и контрольных мер по его достижению

АРХИТЕКТУРА И РАЗМЕЩЕНИЕ СЗИ

- Централизация управления отдельными СЗИ, применяемыми для обеспечения услуг ИБ в ГО, СГ и ДЗО
- Создание функциональных требований к СЗИ и их масштабированию
- Анализ вариантов реализации СЗИ в централизованном / локальном вариантах с точки зрения эффективности и стоимости
- Анализ необходимости миграции отдельных СЗИ в централизованный ЦОД

Задачи по направлениям (2/2)

кибербезопасность
в эпоху перемен

информзащита

ОПЕРАЦИОННАЯ МОДЕЛЬ СГ

- Разработка организационно-штатной структуры, требуемого штата сотрудников и матрицы их компетенций для СГ и ДЗО
- Разработка модели взаимодействия управляющего центра ИБ в ГО с СГ и ДЗО
- Разработка основных и поддерживающих процессов ИБ для операционных моделей ГО, СГ и ДЗО
- Разработка ВНД и ОРД для регламентации операционных процессов ИБ и эксплуатации СЗИ

СТАНДАРТЫ И ТРЕБОВАНИЯ ИБ

- Типизация ДЗО по признакам (вид деятельности, категории обрабатываемой информации, ИТ-ландшафт, применимая модель угроз)
- Создание требований ИБ к ИТ- и ИБ-системам
- Создание вариантов реализации требований ИБ на основе услуг ИБ
- Разработка и приведение в соответствие ВНД для управляющих и операционных процессов ИБ
- Создание шаблонов ОРД для соответствия требований законодательства, применимых для того или иного типа ДЗО

SLA И KPI

- Разработка каталога услуг ИБ
- Разработка SLA / OLA услуг для контроля уровня сервиса
- Определение пороговых значений SLO / OLO сервиса
- Разработка метрик эффективности выполнения процесса

информзащита

Безопасность дочерних зависимых обществ

Марат Цихмистров
Руководитель направления технической экспертизы,
«Информзащита»

кибербезопасность
в эпоху перемен