

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 2

Структура бизнес-машины

Спикер: Ануфриев Иван



ЗАНЯТИЕ 2.2

Инциденты и процессы информационной безопасности



Условное разделение информации. «Метки» на слайдах *

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.		«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
			
Рабочий «экспертный» инструментарий «Expert tools»		Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»	Метки по используемым инструментам и практикам
 (EXPERT TOOLS)		(BEST PRACTICE)	
Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
(INSIGHTS)	(COMPLIANCE) 	(BUSINESS CONTINUITY)	



Основные рассматриваемые вопросы занятия

Вопрос 1

**Цель ИБ 1: Защита
технологического
сегмента
от угроз ИБ**

Вопрос 2

**Цель ИБ 2:
Эффективная система
оперативного
управления
инцидентами**

Вопрос 3

**Цель ИБ 3:
Противодействие
мошенническим
операциям**

Вопрос 4

**Цель ИБ 4:
Контроль утечек
коммерческой
тайны**

Вопрос 5

**Цель ИБ 5:
Формирование
киберкультуры
персонала**



Цель 1: Защита технологического сегмента от угроз ИБ



Создание системы контролей/процессов информационной безопасности технологического сегмента

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий



Управление доступом

Сегментация технологической сети, отделение от бизнес сегмента, выделение сегментов разработки и тестирования



Управление полномочиями

Минимизация и контроль действий привилегированных пользователей, непрерывный мониторинг изменений, контроль безопасности разработки, ИБ в управлении проектами



Управление удаленным доступом

Создание замкнутой среды для безопасной реализации удаленного доступа



Контроль состояния ИБ

Эффективный процесс управления уязвимостями, регулярная оценка защищенности, обучение административного и рядового персонала



Соответствие нормативным требованиям

Соответствие технологического сегмента требованиям законодательства в области КИИ (187-ФЗ РФ)



Управление инцидентами ИБ

Мониторинг инцидентов ИБ, Киберучения, запуск и поддержание Процессов BCM&DR



Цель 1: Защита технологического сегмента от угроз Информационной безопасности



Создание системы контролей/процессов информационной безопасности технологического сегмента

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий



Ограничение прав и контроль действий привилегированных пользователей



Создание замкнутой среды для безопасной реализации удаленного доступа



Сегментация технологической сети, отделение от бизнес-сегмента, выделение сегментов разработки и тестирования

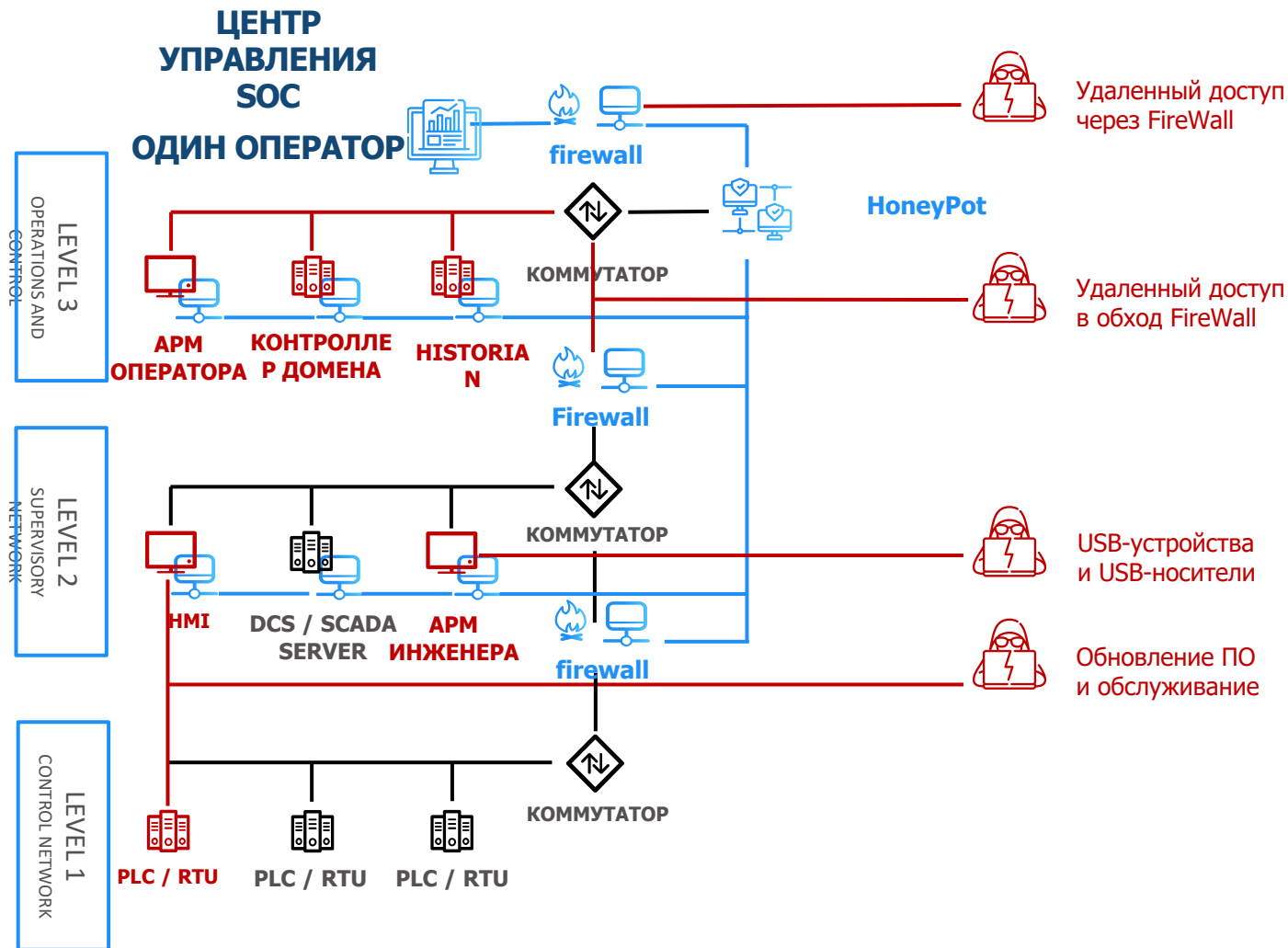


Цель 1: Защита технологического сегмента от угроз Информационной безопасности



Создание системы контролей/процессов информационной безопасности технологического сегмента

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий



Ограничение прав и контроль действий привилегированных пользователей



Создание замкнутой среды для безопасной реализации удаленного доступа



Сегментация технологической сети,
отделение от бизнес-сегмента, выделение
сегментов разработки и тестирования



Администраторы
АСУ ТП и
подрядчики

Защищенный далённый доступ

*Сайты
автоматизации
технологических
процессов*



**Защита внешнего
периметра
технологического
сегмента**

ФСБ России
НКЦКИ

SOC



**Система анализа и
выявление аномалий в
технологических
процессах**

Выявление инцидентов ИБ

Анализ копии

Передача
контролируемых
параметров и
команд
управления
технологическими
процессами

Защита от
вирусов



SCADA



HMI



PLC

Агрегаты



Мониторинг инцидентов ИБ,
киберучения, запуск и поддержание
процессов BCM&DR

Система безопасности значимых объектов КИИ

Бизнес-сегмент и
иные внешние
сети

Кибератака

Злоумышленник



Цель 1: Защита технологического сегмента от угроз Информационной безопасности



Создание системы контролей/процессов информационной безопасности технологического сегмента

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий



СИСТЕМА КРП

Запуск и исполнение целевых КРП по отражению атак в технологических сегментах



Инцидентов ИБ в АСУ ТП разрешены в рамках SLA



Запланированных киберучений проведено



Непрерывный мониторинг и реагирование на инциденты ИБ



Выявленных в АСУ ТП уязвимостей своевременно устранены



Цель 1: Защита технологического сегмента от угроз Информационной безопасности (BEST PRACTICE)



СОДЕРЖАНИЕ

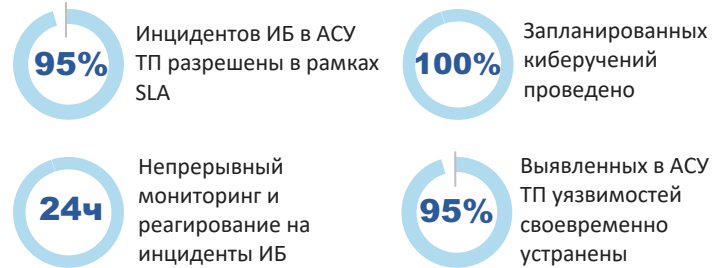
Создание системы контролей/процессов информационной безопасности технологического сегмента

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий



СИСТЕМА КРП

Запуск и исполнение целевых КРП по отражению атак в технологических сегментах



ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

Обеспечение защиты от угроз ИБ и постоянный контроль состояния ИБ

- Эффективный процесс управления уязвимостями и инцидентами ИБ
- Регулярная оценка защищенности и устранение уязвимостей
- Обучение привилегированных и рядовых пользователей

Соответствие нормативным требованиям

Соответствие технологического сегмента требованиям законодательства РФ в области КИИ (187-ФЗ)

Цель 2: Эффективная система оперативного управления инцидентами



Создание инфраструктуры и организационной модели центра ИБ

для обеспечения тотального контроля над процессами и информацией в инфраструктуре предприятия на всех уровнях

Обеспечение непрерывного мониторинга

в целях своевременного выявления и реагирования на инциденты ИБ



Экспертная команда мониторинга и
реагирования на инциденты ИБ



Цель 2: Эффективная система оперативного управления инцидентами

Создание инфраструктуры и организационной модели центра ИБ

для обеспечения тотального контроля над процессами и информацией в инфраструктуре предприятия на всех уровнях

Обеспечение непрерывного мониторинга

в целях своевременного выявления и реагирования на инциденты ИБ



Экспертная команда мониторинга и реагирования на инциденты ИБ



Централизованное управление ИБ



Цель 2: Эффективная система оперативного управления инцидентами

Создание инфраструктуры и организационной модели центра ИБ

для обеспечения тотального контроля над процессами и информацией в инфраструктуре предприятия на всех уровнях

Обеспечение непрерывного мониторинга

в целях своевременного выявления и реагирования на инциденты ИБ



Экспертная команда мониторинга и реагирования на инциденты ИБ



Централизованное управление ИБ



Система KPI



Цель 2: Эффективная система оперативного управления инцидентами

Создание инфраструктуры и организационной модели центра ИБ

для обеспечения тотального контроля над процессами и информацией в инфраструктуре предприятия на всех уровнях

Обеспечение непрерывного мониторинга

в целях своевременного выявления и реагирования на инциденты ИБ



Экспертная команда мониторинга и реагирования на инциденты ИБ



Совершенствование системы оперативного управления инцидентами



Централизованное управление ИБ



Система KPI



Цель 2: Эффективная система оперативного управления инцидентами

Создание инфраструктуры и организационной модели центра ИБ

для обеспечения тотального контроля над процессами и информацией в инфраструктуре предприятия на всех уровнях

Обеспечение непрерывного мониторинга

в целях своевременного выявления и реагирования на инциденты ИБ



Экспертная команда мониторинга и реагирования на инциденты ИБ



Совершенствование системы оперативного управления инцидентами



Централизованное управление ИБ



Взаимодействие с регуляторами



Система KPI



Цель 2: Эффективная система оперативного управления инцидентами

{ BEST PRACTICE }
{ BUSINESS
CONTINUITY }



Создание инфраструктуры и организационной модели SOC

для обеспечения тотального контроля над процессами и информацией в инфраструктуре компании на всех уровнях

Обеспечение непрерывного мониторинга

в целях своевременного выявления и реагирования на инциденты ИБ



Экспертная команда мониторинга и реагирования на инциденты ИБ

Формирование и поддержание экспертной зрелости команды SOC компании, ресурсное обеспечение подразделений мониторинга и реагирования



Централизованное управление ИБ

Развертывание и достижение целевой эффективности ядра системы управления ИБ



Система KPI

Запуск и исполнение целевых KPI по отражению атак на компанию



Совершенствование системы оперативного управления инцидентами

Постановка задач Команде SOC по непрерывному совершенствованию эффективности выявления инцидентов всех уровней инфраструктуры и информационных систем, технических каналов передачи информации, фрод-деятельности в рамках бизнес-процессов



Взаимодействие с регуляторами

Взаимодействие с ФСБ, ФСТЭК и национальными CERT в части информирования об инцидентах ИБ



Цель 2: Эффективная система оперативного управления инцидентами

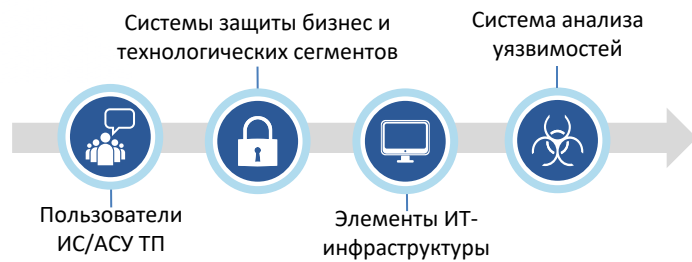
Создание инфраструктуры и организационной модели SOC
для обеспечения тотального контроля над процессами и информацией в
инфраструктуре крупной на всех уровнях



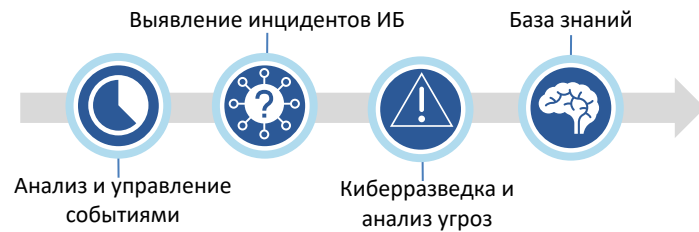
Цель 2: Эффективная система оперативного управления инцидентами

Создание инфраструктуры и организационной модели SOC
для обеспечения тотального контроля над процессами и информацией в инфраструктуре крупной на всех уровнях

ОБРАБАТЫВАЕМЫЕ ВИДЫ ИСТОЧНИКОВ СОБЫТИЙ



ПРАВИЛА КОРРЕЛЯЦИИ СОБЫТИЙ



ПЛАНЫ РЕАГИРОВАНИЯ (PLAYBOOK)



Цель 2: Эффективная система оперативного управления инцидентами

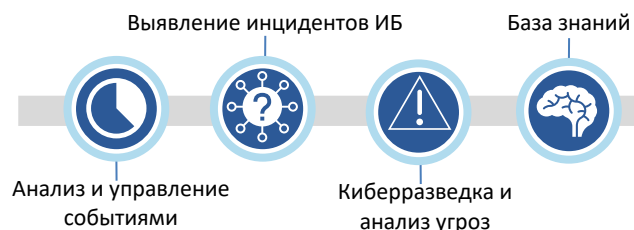
Создание инфраструктуры и организационной модели SOC

для обеспечения тотального контроля над процессами и информацией в инфраструктуре крупной на всех уровнях

ОБРАБАТЫВАЕМЫЕ ВИДЫ ИСТОЧНИКОВ СОБЫТИЙ



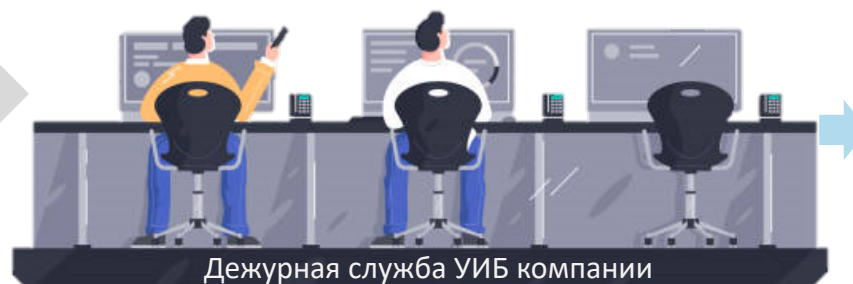
ПРАВИЛА КОРРЕЛЯЦИИ СОБЫТИЙ



ПЛАНЫ РЕАГИРОВАНИЯ (PLAYBOOK)



АНАЛИТИЧЕСКИЕ ОТЧЕТЫ И ДАШБОРДЫ



Экспертная команда мониторинга и реагирования на инциденты ИБ

Формирование и поддержание экспертной зрелости команды SOC компании ресурсное обеспечение подразделений мониторинга и реагирования



Цель 2: Эффективная система оперативного управления инцидентами

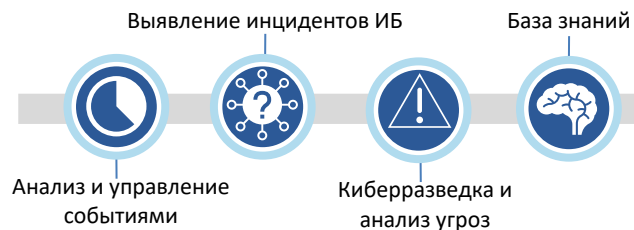
Создание инфраструктуры и организационной модели SOC

для обеспечения тотального контроля над процессами и информацией в инфраструктуре крупной на всех уровнях

ОБРАБАТЫВАЕМЫЕ ВИДЫ ИСТОЧНИКОВ СОБЫТИЙ



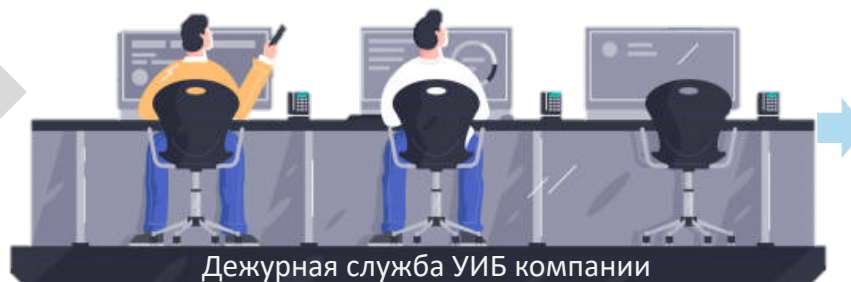
ПРАВИЛА КОРРЕЛЯЦИИ СОБЫТИЙ



ПЛАНЫ РЕАГИРОВАНИЯ (PLAYBOOK)



АНАЛИТИЧЕСКИЕ ОТЧЕТЫ И ДАШБОРДЫ



Экспертная команда мониторинга и реагирования на инциденты ИБ

Формирование и поддержание экспертной зрелости команды SOC компании ресурсное обеспечение подразделений мониторинга и реагирования



СИСТЕМА KPI

Запуск и исполнение целевых KPI по отражению атак в отношении активов компании



Цель 2: Эффективная система оперативного управления инцидентами

BEST PRACTICE

BUSINESS CONTINUITY



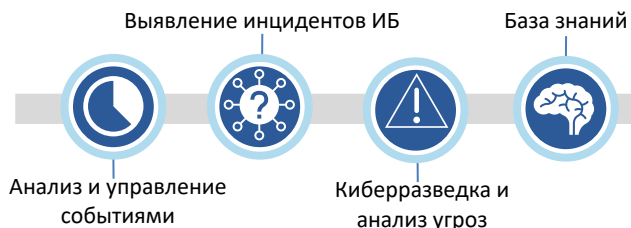
Создание инфраструктуры и организационной модели SOC

для обеспечения тотального контроля над процессами и информацией в инфраструктуре крупной на всех уровнях

ОБРАБАТЫВАЕМЫЕ ВИДЫ ИСТОЧНИКОВ СОБЫТИЙ



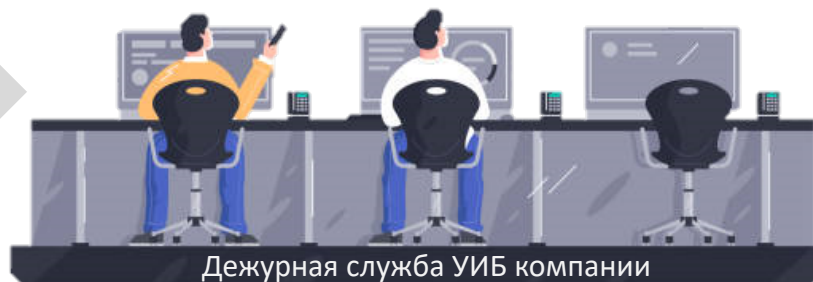
ПРАВИЛА КОРРЕЛЯЦИИ СОБЫТИЙ



ПЛАНЫ РЕАГИРОВАНИЯ (PLAYBOOK)



АНАЛИТИЧЕСКИЕ ОТЧЕТЫ И ДАШБОРДЫ



Экспертная команда мониторинга и реагирования на инциденты ИБ

Формирование и поддержание экспертной зрелости команды SOC компании ресурсное обеспечение подразделений мониторинга и реагирования



СИСТЕМА KPI

Запуск и исполнение целевых KPI по отражению атак в отношении активов компании



ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

Развертывание и достижение целевой эффективности ядра системы управления ИБ

- защищенный периметр технологического и бизнес-сегмента
- эффективный процесс управления активами и уязвимостями
- готовность персонала к отражению атак
- оценка текущей зрелости процессов и непрерывное развитие



Взаимодействие с регуляторами

Взаимодействие с ФСБ, ФСТЭК и национальными CERT в части информирования об инцидентах ИБ



Цель 3: Противодействие мошенническим операциям



Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности





Введение системы контролей надлежащего **исполнения дизайна бизнес-процессов компании**, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов



Контроль утечек информации





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов



Контроль утечек информации



Контроль нецелевого использования активов





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов



Обеспечение непрерывности критических операций



Контроль утечек информации



Контроль нецелевого использования активов





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов



Обеспечение непрерывности критических операций



Контроль утечек информации



Контроль физического доступа



Контроль нецелевого использования активов





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов



Обеспечение непрерывности критических операций



Контроль утечек информации



Контроль физического доступа



Контроль нецелевого использования активов



Выявление мошенничества





Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании, поведенческий анализ, поиск отклонений, расследования и привлечение к ответственности



Контроль критических операций и процессов

Создание и поддержание набора превентивных, выявляющих и компенсирующих контролей критических операций и процессов управления активами Компании (Закупки, Логистика, Кадры, Бухгалтерская и Управленческая отчетность и т.д.)



Контроль утечек информации

Контроль перемещения информации внутри и за пределы Компании, анализ взаимодействия сотрудников в рамках ролевых моделей бизнес-процессов



Контроль нецелевого использования активов

Выявление неправомерного использования инфраструктуры компании



Обеспечение непрерывности критических операций

Мониторинг событий безопасности и критических операций Mission-critical и Business critical – систем, контроль авторизации изменений



Контроль физического доступа

Мониторинг акустических и визуальных каналов, систем контроля физического доступа



Выявление мошенничества

Сбор юридически значимых доказательств фрод-деятельности



Цель 3: Противодействие мошенническим операциям

Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании и выявления несанкционированных действий



Создание и поддержание набора превентивных, выявляющих и компенсирующих контролей критических операций и процессов управления активами компании



Сбор юридически значимых доказательств мошеннической деятельности

Формирование поведенческих профилей пользователей в сети

Формирование правил выявления мошеннических действий и утечек данных



Выявление отклонений в поведении пользователей



Выявление неправомерного использования инфраструктуры



Контроль перемещения информации внутри и за пределы компании



Подтверждение мошеннических/неправомерных действий



Сбор доказательств и расследование инцидентов ИБ



Привлечение виновных к ответственности



Цель 3: Противодействие мошенническим операциям

Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании и выявления несанкционированных действий



Создание и поддержание набора превентивных, выявляющих и компенсирующих контролей критических операций и процессов управления активами компании



Сбор юридически значимых доказательств мошеннической деятельности

Система анализа и выявления мошеннических действий

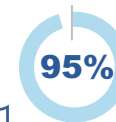
Формирование поведенческих профилей пользователей в сети

Формирование правил выявления мошеннических действий и утечек данных



СИСТЕМА KPI

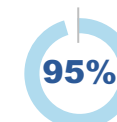
Запуск и исполнение целевых KPI по выявлению мошеннической деятельности



Своевременно выявленных мошеннических действий



Контролируются все критические для бизнеса процессы



Контроль активности пользователей-участников критических бизнес-процессов



Цель 3: Противодействие мошенническим операциям

(BEST PRACTICE)



Введение системы контролей надлежащего исполнения дизайна бизнес-процессов компании и выявления несанкционированных действий



Создание и поддержание набора превентивных, выявляющих и компенсирующих контролей критических операций и процессов управления активами компании



Сбор юридически значимых доказательств мошеннической деятельности

Система анализа и выявления мошеннических действий

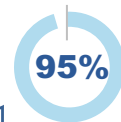
Формирование поведенческих профилей пользователей в сети

Формирование правил выявления мошеннических действий и утечек данных



СИСТЕМА KPI

Запуск и исполнение целевых KPI по выявлению мошеннической деятельности



Своевременно выявленных мошеннических действий



Контролируются все критические для бизнеса процессы



Контроль активности пользователей-участников критических бизнес-процессов



ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

Защита от неправомерных действий пользователей бизнес-сегментов компании

- предотвращение утечки конфиденциальной информации в рамках всех критических бизнес-процессов
- защита интересов компании в суде при выявлении мошенничества и в случаях инцидентов утечки ценной информации
- минимальный потенциальный ущерб вследствие мошеннических действий
- реализован контроль событий безопасности и критических операций Mission-critical и Business critical – систем, контроль авторизации изменений





Мероприятия по противодействию коммерческому шпионажу





Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



Введение режима коммерческой тайны





Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании

Введение режима коммерческой тайны



Актуализация регламентирующих документов, возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Управление доступом к информации, составляющей коммерческую тайну





Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



Введение режима коммерческой тайны

Актуализация регламентирующих документов, возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Управление доступом к информации, составляющей коммерческую тайну

Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Взаимодействие с регуляторами





Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



Введение режима коммерческой тайны

Актуализация регламентирующих документов, возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Контроль потоков информации



Управление доступом к информации, составляющей коммерческую тайну

Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Взаимодействие с регуляторами

Взаимодействие с регуляторами в части информирования о применяемых мерах, процессах и инцидентах в отношении информации, составляющей коммерческую тайну, и персональных данных





Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



Введение режима коммерческой тайны

Актуализация регламентирующих документов и состава ПДЭК, возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Управление доступом к информации, составляющей коммерческую тайну

Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Взаимодействие с регуляторами

Взаимодействие с регуляторами в части информирования о применяемых мерах, процессах и инцидентах в отношении информации, составляющей коммерческую тайну, и персональных данных



Контроль потоков информации

Развертывание и детальная настройка системы DLP для контроля неавторизованных каналов утечек информации, составляющей коммерческую тайну, за пределы компании, отработка инцидентов, эскалация, обучение сотрудников



Защита конфиденциальной информации

Реализация процессных и технических мер защиты чувствительной информации для установленной среды жизненного цикла информации, составляющую коммерческую тайну компании и персональных данных





Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



Введение режима коммерческой тайны

Актуализация регламентирующих документов и состава ПДЭК, возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Управление доступом к информации, составляющей коммерческую тайну

Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Взаимодействие с регуляторами

Взаимодействие с регуляторами в части информирования о применяемых мерах, процессах и инцидентах в отношении информации, составляющей коммерческую тайну, и персональных данных



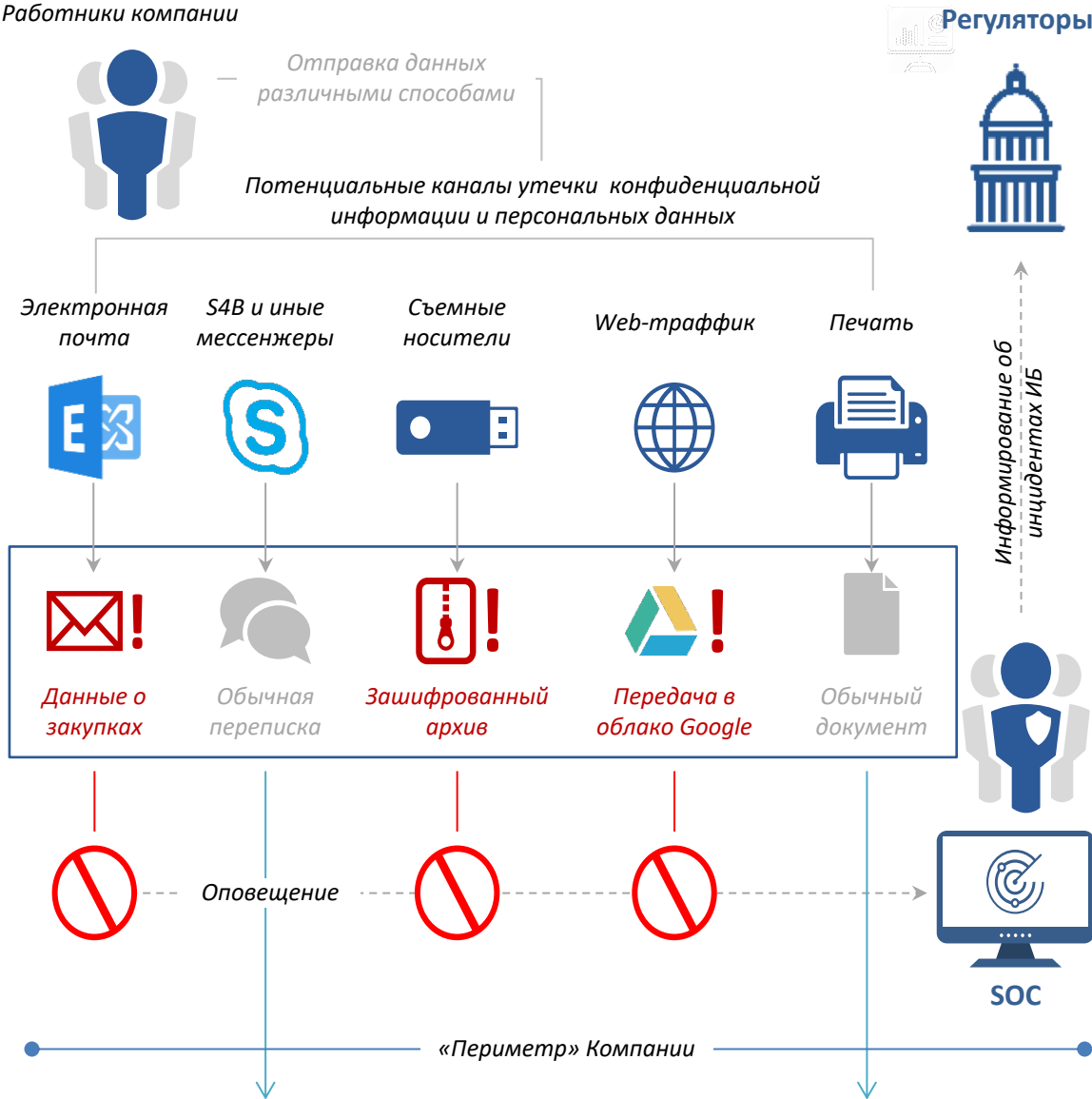
Контроль потоков информации

Развертывание и детальная настройка системы DLP для контроля неавторизованных каналов утечек информации, составляющей коммерческую тайну, за пределы компании, отработка инцидентов, эскалация, обучение сотрудников



Защита конфиденциальной информации

Цель 4: Контроль утечек коммерческой тайны и персональных данных



Цель 4: Контроль утечек коммерческой тайны и персональных данных

Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



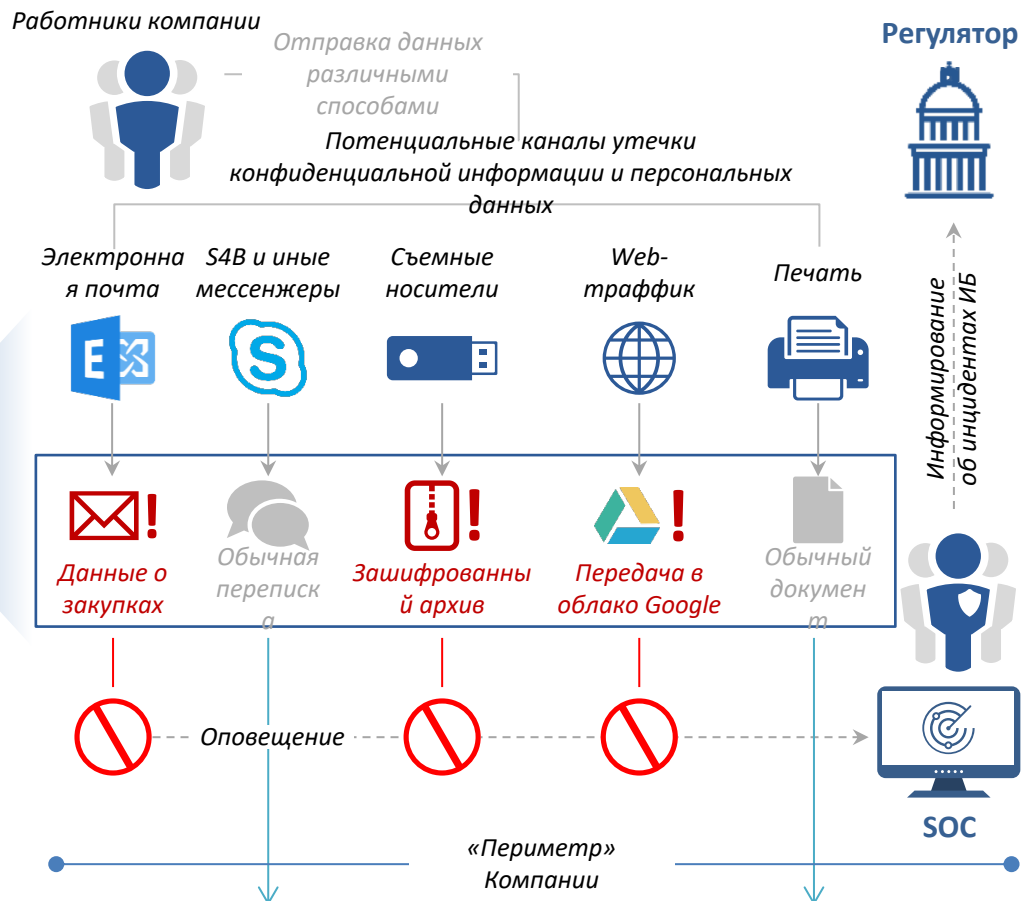
Возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Развертывание и детальная настройка системы DLP для контроля неавторизованных каналов утечек информации, составляющей коммерческую тайну, за компании, обработка инцидентов, эскалация, обучение сотрудников



Цель 4: Контроль утечек коммерческой тайны и персональных данных

Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



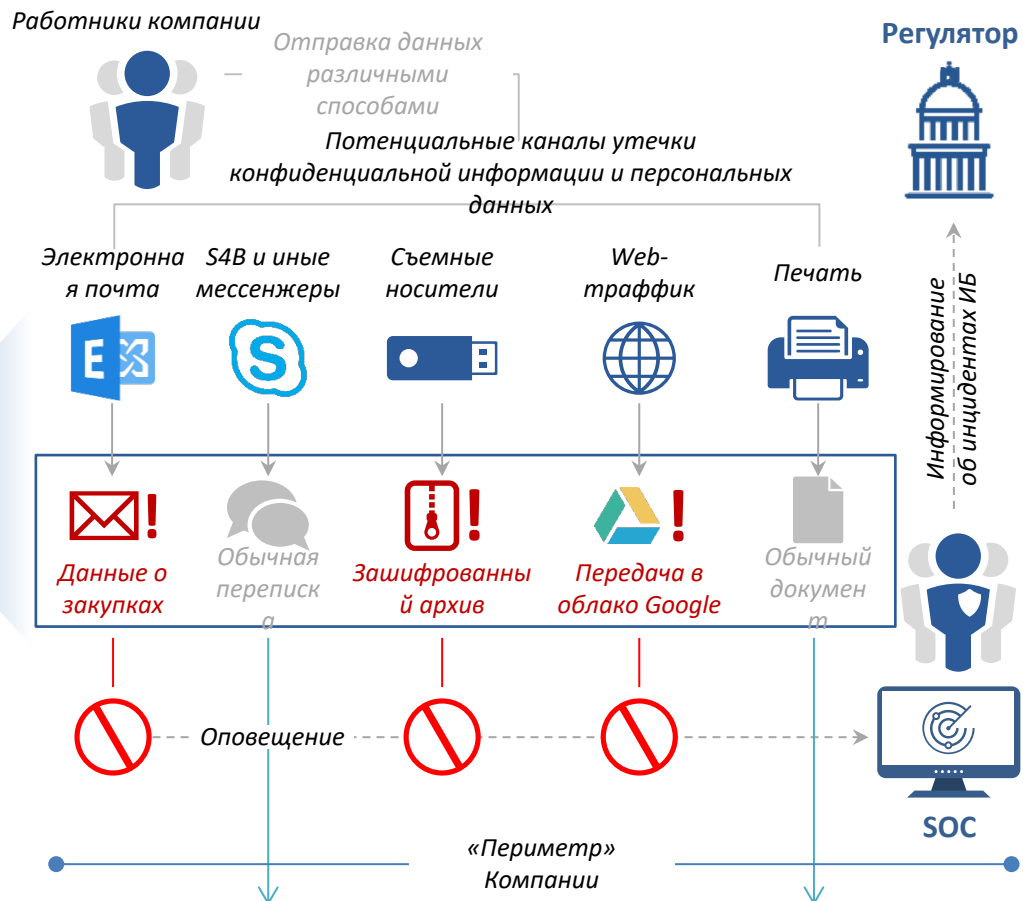
Возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Развертывание и детальная настройка системы DLP для контроля неавторизованных каналов утечек информации, составляющей коммерческую тайну, за компании, обработка инцидентов, эскалация, обучение сотрудников



Цель 4: Контроль утечек коммерческой тайны и персональных данных

Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



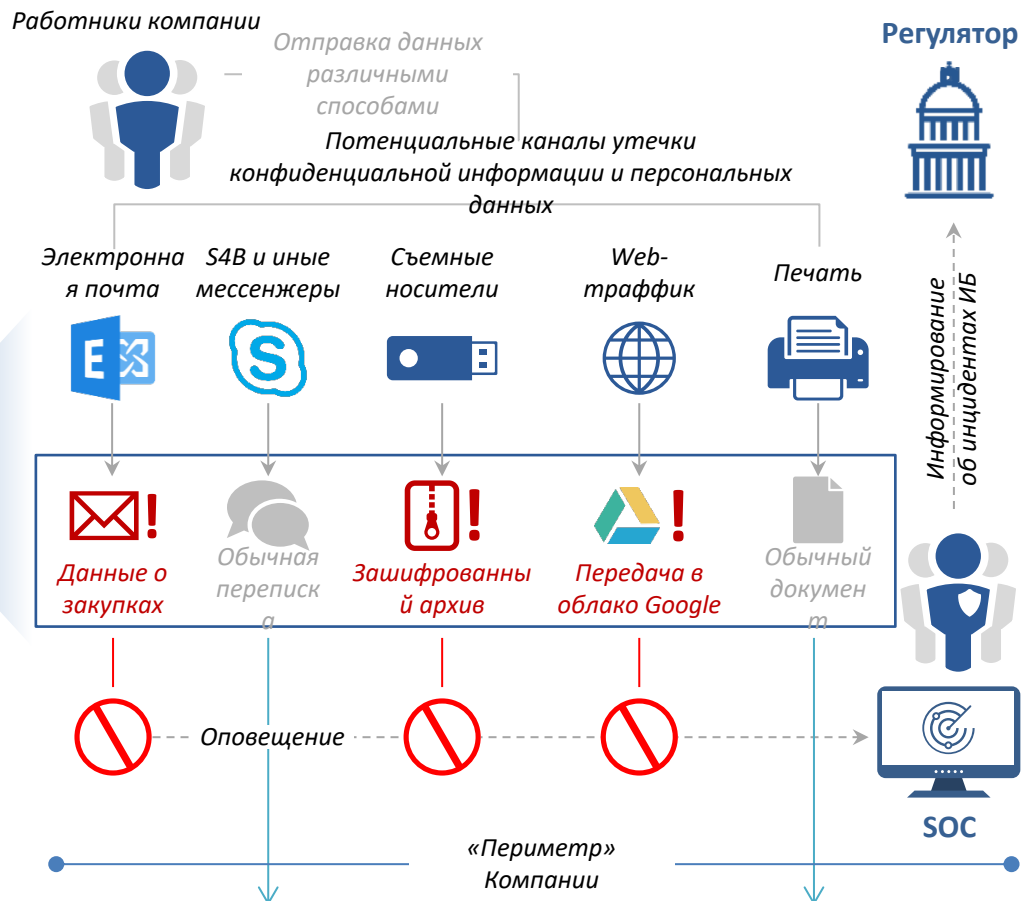
Возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Развертывание и детальная настройка системы DLP для контроля неавторизованных каналов утечек информации, составляющей коммерческую тайну, за компании, отработка инцидентов, эскалация, обучение сотрудников



Цель 4: Контроль утечек коммерческой тайны и персональных данных

Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



Возобновление работы по присвоению и выводу из обращения информации, составляющую коммерческую тайну компании



Разработка и внедрение дизайна контроля доступа сотрудников к информации, составляющей коммерческую тайну, микро-сегментация доступов



Развертывание и детальная настройка системы DLP для контроля неавторизованных каналов утечек информации, составляющей коммерческую тайну, за компании, обработка инцидентов, эскалация, обучение сотрудников

Работники компании



Отправка данных различными способами
Потенциальные каналы утечки конфиденциальной информации и персональных данных

Электронная почта



Данные о закупках

S4B и иные мессенджеры



Обычная переписка

Съемные носители



Зашифрованный архив

Web-трафик



Передача в облако Google

Печать



Обычный документ

Регулятор



Информирование об инцидентах ИБ



SOC



Оповещение



«Периметр» Компании



СИСТЕМА KPI

Запуск и исполнение целевых KPI по контролю утечек данных



Успешно расследованных инцидентов ИБ, связанных с утечкой данных



Отсутствие штрафов со стороны регуляторов



Непрерывный мониторинг и реагирование на инциденты ИБ



Своевременное информирование регуляторов об инцидентах ИБ



Развертывание и обеспечение эффективности процесса контроля утечек чувствительной информации компании



СИСТЕМА KPI

Запуск и исполнение целевых KPI по контролю утечек данных

95%

Успешно расследованных инцидентов ИБ, связанных с утечкой данных

100%

Отсутствие штрафов со стороны регуляторов

24ч

Непрерывный мониторинг и реагирование на инциденты ИБ

100%

Своевременное информирование регуляторов об инцидентах ИБ

ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

Обеспечение защиты конфиденциальной информации

Реализованы процессные и технические меры защиты чувствительной информации для установленной среды жизненного цикла информации, составляющей коммерческую тайну компании и персональных данных

Выполнение требований законодательства

- Соблюдение требований GDPR
- Поддержание режима коммерческой тайны, сбор доказательств и защита интересов компании в суде



Планируется на основе запуска ежегодной Программы повышения осведомленности персонала в вопросах ИБ



Тестирование персонала в области ИБ

Развертывание платформы тестирования состояния осведомленности, проведение акций, эскалация результатов, обучение



Информирование персонала в области ИБ

Определение списка каналов эффективного распространения информации сотрудникам (портал, e-mail, скринсейвер, корп. телевидение и online-курсы)



Реализация программ обучения в области ИБ

Разработка контента online-курсов по ИБ для различных категорий сотрудников (администраторы, персонал ИТ, бизнес), внедрение процесса непрерывного обучения ВСЕГО персонала на базе компании



Формирование программ обучения в области ИБ

Формирование перечня ключевых актуальных тем осведомленности



Проведение тренингов в области ИБ

Введение очных обязательных тренингов для руководителей среднего звена



Обеспечение ресурсами для обучения

Производство и распространение раздаточного материала: головоломки, канц. товары



Предупреждение инцидентов ИБ

Обязательное обучение фигурантов инцидентов ИБ



**Благодарю
за внимание!**

