

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 2

Структура бизнес-машины

Спикер: Ануфриев Иван



ЗАНЯТИЕ 2.1

Направления защиты информации



Условное разделение информации. «Метки» на слайдах *



«Машина-времени-Time-machnine» 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

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



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ЗАНЯТИЯ

ВОПРОС 1

Направление
защиты –
«Идентификация»

ВОПРОС 2

Направление
защиты –
«Защита»

ВОПРОС 3

Направление
защиты –
«Обнаружение»

ВОПРОС 4

Направление
защиты –
«Реагирование»

ВОПРОС 5

Направление
защиты –
«Восстановление»

ВОПРОС 6

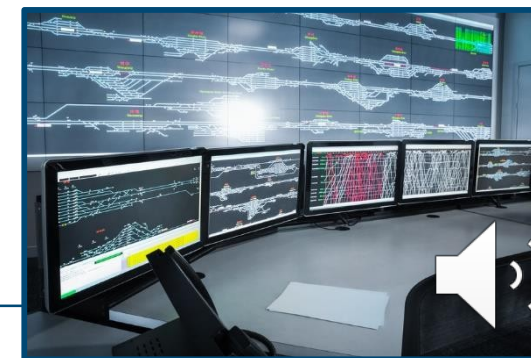
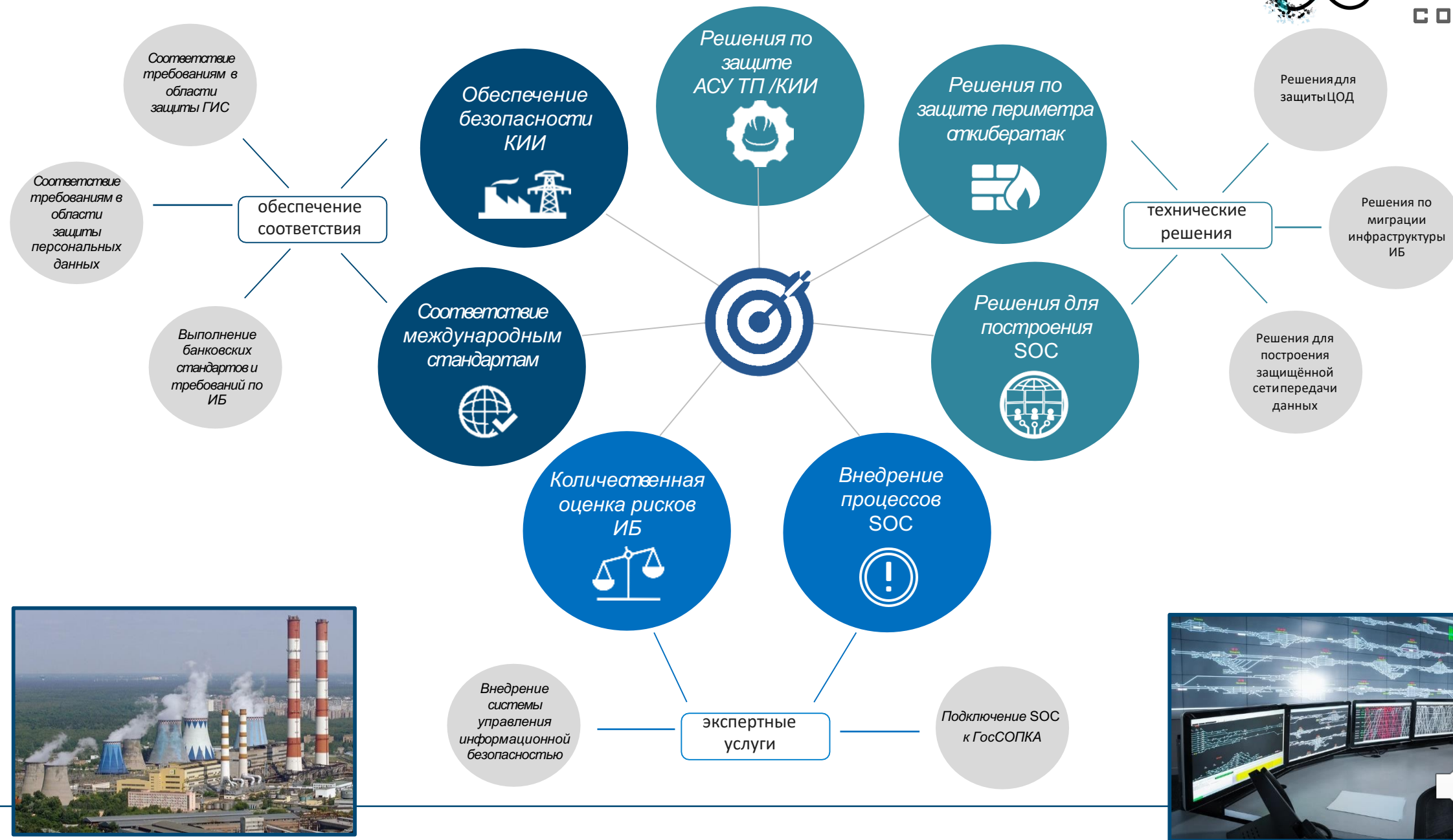
Эшелонированная
защита
информации

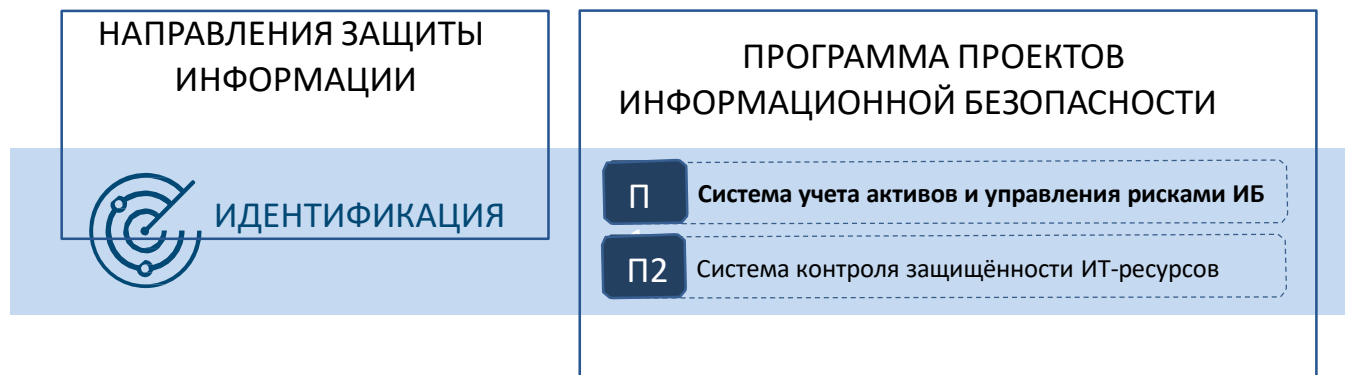
ВОПРОС 7

Полный цикл
работ по ИБ



Ключевая карта для рассмотрения на занятиях





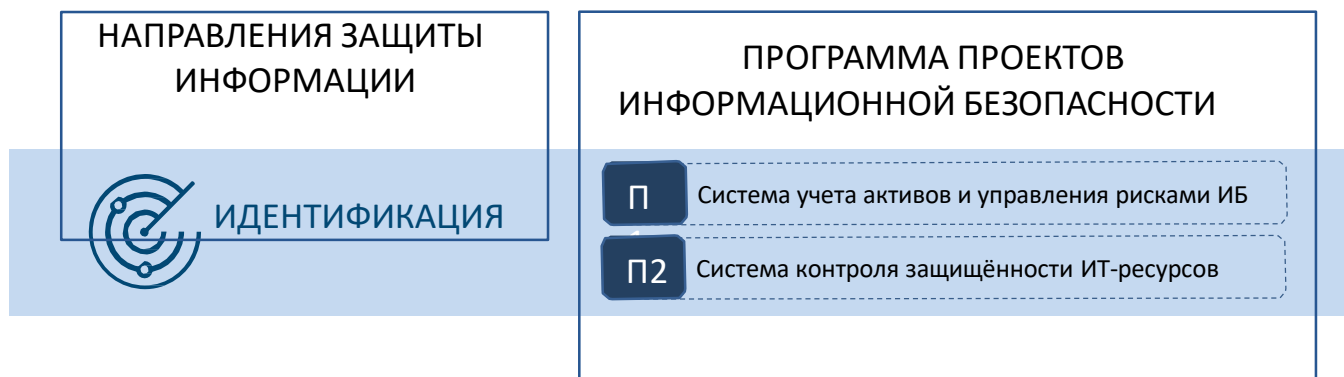
Управление ИТ-активами предприятия (ITAM) – комплексные решения для физического учета, финансового контроля и следования контрактным обязательствам на протяжении всего жизненного цикла IT-активов: от приобретения, перераспределения до удаления.



Идентификация – схема автоматизации основных позиций внутри компании



Идентификация – основные задачи системы управления активами



- экономия ресурсов за счет совершенствования процессов поддержки принятия решения;
- повышение эффективности учёта активов;
- обеспечение соответствия к требованиям и ограничениям каждого актива;
- повышение производительности и увеличение жизненного цикла актива;
- увеличение показателей доступности;
- снижение влияния человеческого фактора;
- отражение полной картины владения ИТ-активами, текущего состояния КИС.



Основные направления обеспечения информационной безопасности – Защита

(BEST PRACTICE)



НАПРАВЛЕНИЯ ЗАЩИТЫ
ИНФОРМАЦИИ



ЗАЩИТА

ПРОГРАММА ПРОЕКТОВ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П3

Система защиты периметра сети

П4

Системы управления доступом, антивирусной
защиты и защиты хостов

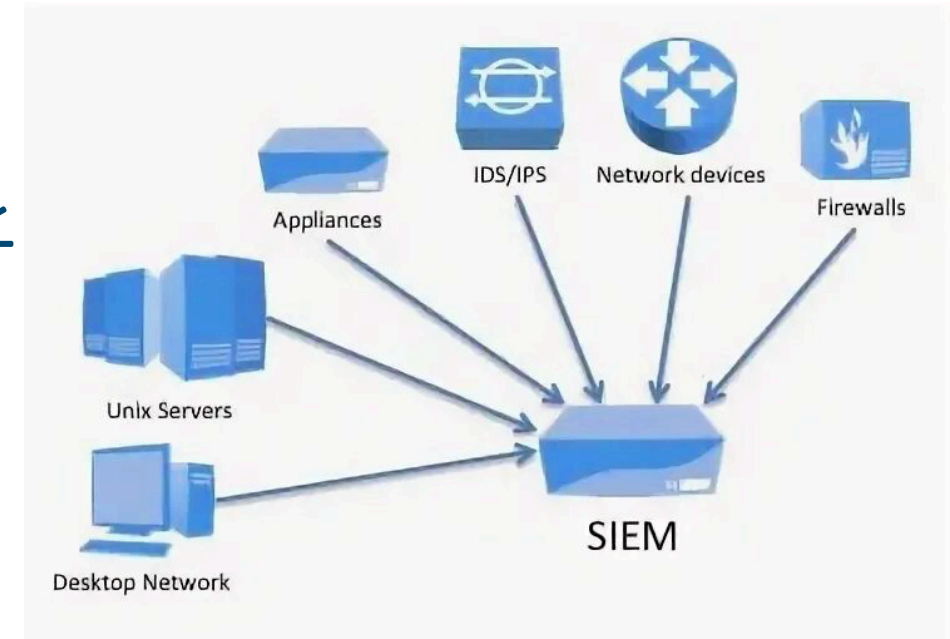
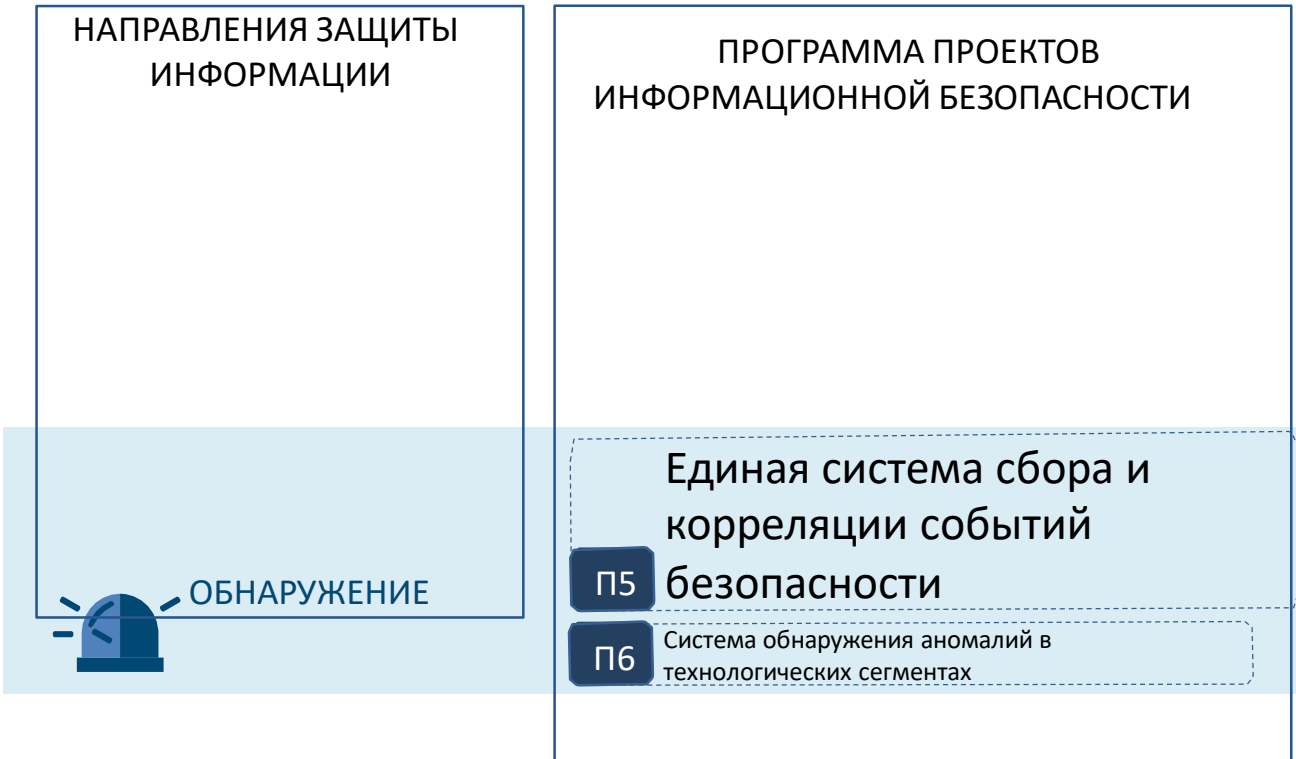


Основные направления обеспечения информационной безопасности – защита. Развитие типов угроз и мер защиты

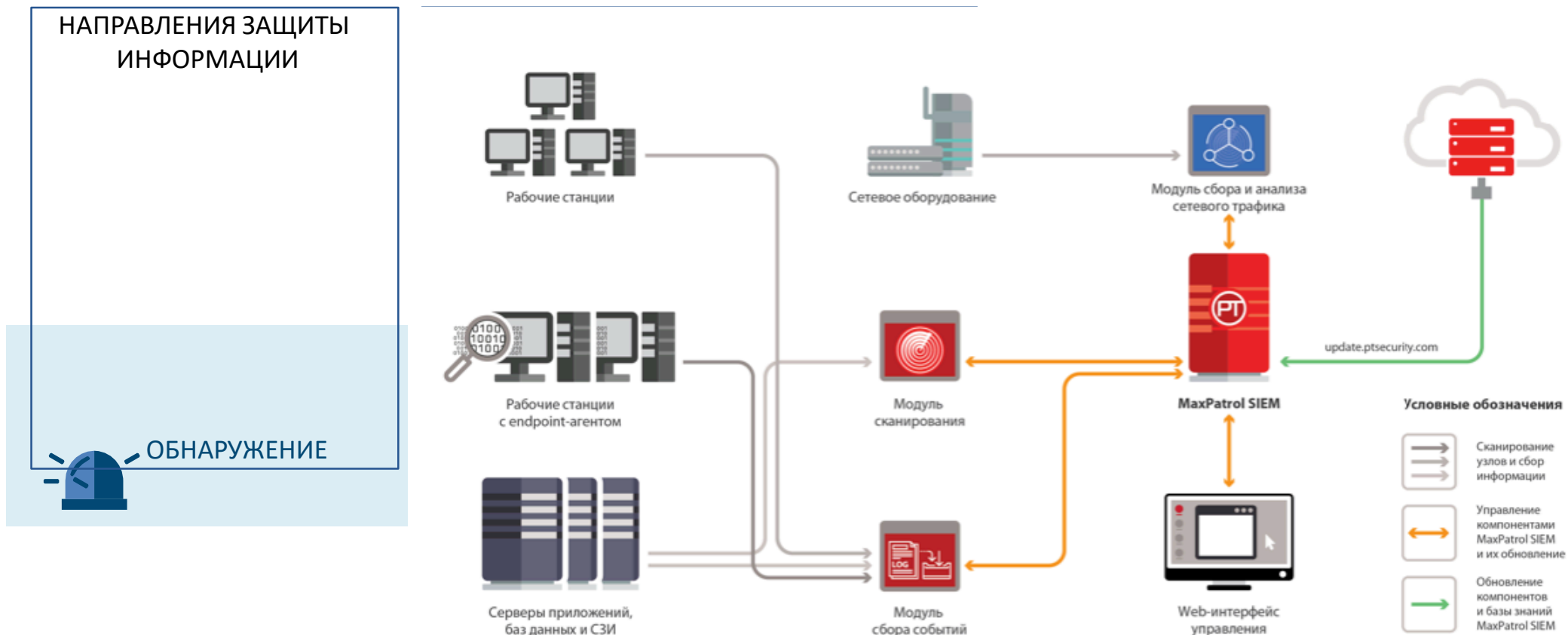


Основные направления защиты информации – Обнаружение

(BEST PRACTICE)



Основные направления защиты информации – Обнаружение



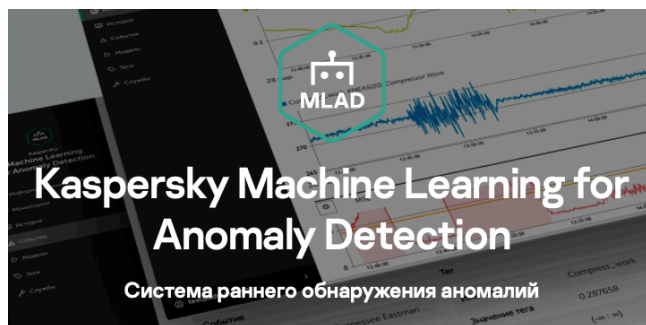
Основные направления защиты информации и программы проектов ИБ

НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ



ОБНАРУЖЕНИЕ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



П5

Единая система сбора и корреляции событий безопасности

П6

Система обнаружения аномалий в технологических сегментах



Мониторинг

Kaspersky MLAD поможет обнаружить дефект оборудования или ошибку персонала и предотвратить опасную ситуацию на ранних этапах ее развития



Контроль

Наша система выявляет нетипичные действия сотрудников и таким образом поможет раскрыть фрод или саботаж на предприятии



Эффективность

Наша система поможет повысить эффективность технологического процесса посредством выявления и устранения слабо проявляющихся сбоев технологического процесса



Защита

Kaspersky MLAD выявит атаки злоумышленников, скрытно воздействующие на оборудование для выведения его из строя



Основные направления защиты информации – Реагирование

(BEST PRACTICE)



НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ



РЕАГИРОВАНИЕ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

R-Vision Incident Response Platform (IRP)



Единая точка консолидации информации
обо всех инцидентах информационной безопасности в компании (корпоративный SOC)

Платформа для совместной работы
группы реагирования на инциденты ИБ с возможностью сбора, анализа и хранения сведений, относящихся к инцидентам ИБ

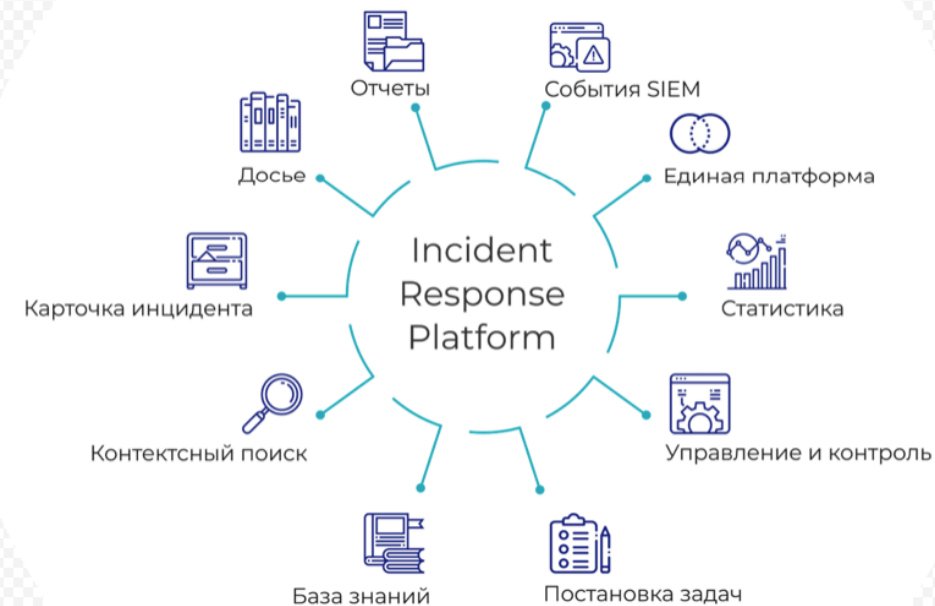
Центр координации деятельности
сотрудников компании, распределения задач и учета выполненных мероприятий по реагированию на инциденты ИБ

Система мониторинга, обработки и реагирования на инциденты ИБ

П7

П8

Система повышения осведомленности
персонала в вопросах ИБ



Основные направления защиты информации – Реагирование.

SOAR как продолжение IRP

НАПРАВЛЕНИЯ ЗАЩИТЫ
ИНФОРМАЦИИ

ПРОГРАММА ПРОЕКТОВ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



РЕАГИРОВАНИЕ

Система мониторинга, обработки и
реагирования на инциденты ИБ

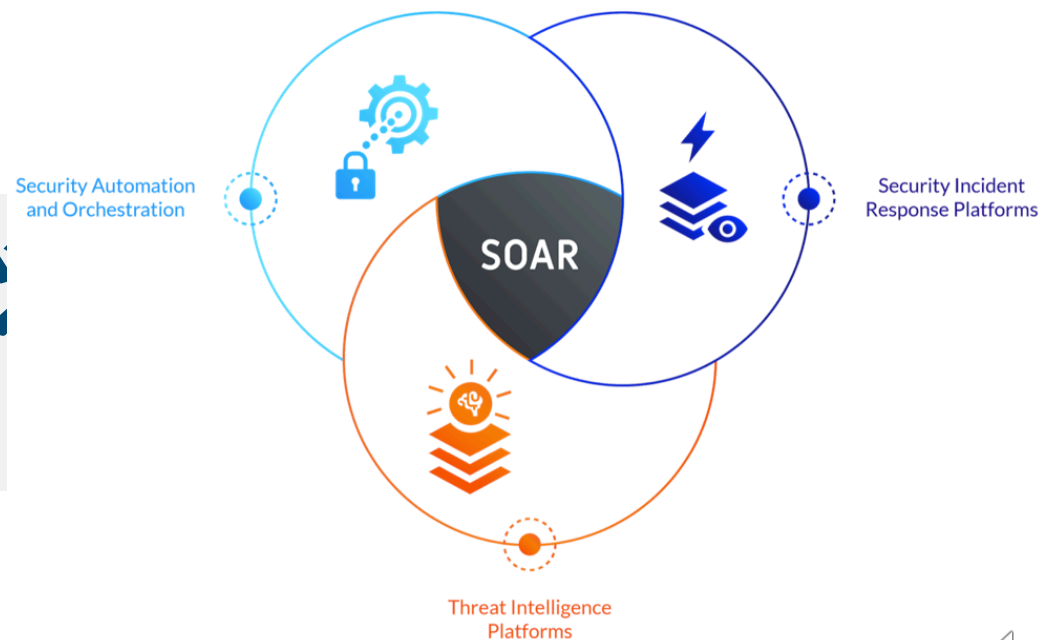
П7

П8

Система повышения осведомленности
персонала в вопросах ИБ

Описание и назначение IRP (Incident Response Platforms) – платформа, предназначенная для автоматизации процессов мониторинга, учета и реагирования на инциденты информационной безопасности (ИБ).

$SOAR = SAO + SIRP + TIP$

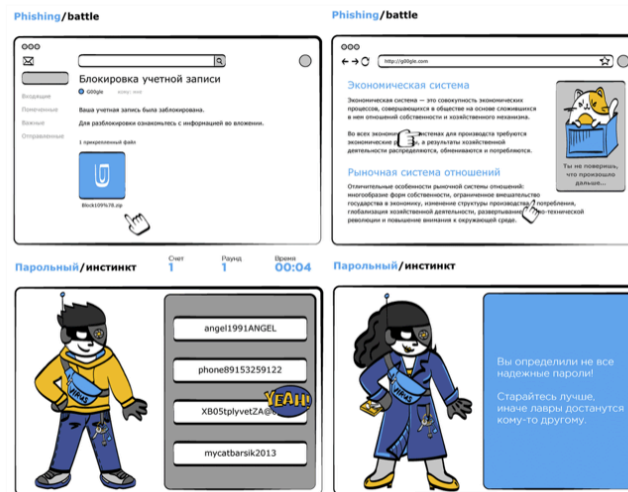


НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ



РЕАГИРОВАНИЕ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



П7

Система мониторинга, обработки и реагирования на инциденты ИБ

П8

Система повышения осведомленности персонала в вопросах ИБ

Повышение осведомлённости сотрудников о правилах кибербезопасности — один из вечных трендов ИБ-сферы. И один из тех, которыми особенно часто пренебрегают, согласно ежегодно публикуемой статистике. Финансовые потери, операционные сбои, утрата партнёров и клиентов и, как следствие, ухудшение делового имиджа случаются гораздо чаще, чем это можно себе представить.



Основные направления защиты информации – Восстановление

(BEST PRACTICE)



НАПРАВЛЕНИЯ ЗАЩИТЫ
ИНФОРМАЦИИ

ПРОГРАММА ПРОЕКТОВ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Система резервного
копирования и
восстановления

п9 данных

п1 Система контроля неизменности конфигурации



ВОССТАНОВЛЕНИЕ

PBVA target systems (целевые системы). Данные комплексы выступают только в качестве целевого устройства для резервного копирования.

PBVA integrated systems (интегрированные системы). Это полностью законченные решения, не требующее дополнительных составляющих для полноценной работы.



Основные направления защиты информации – Восстановление

НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КОД
безопасности

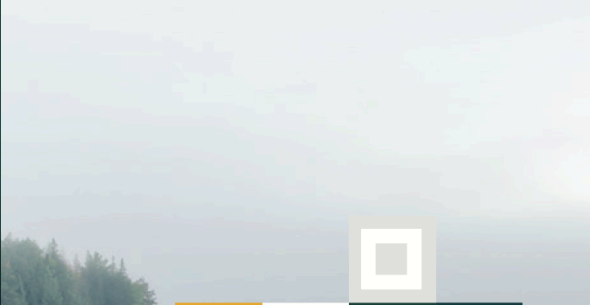
**ЭЛЕКТРОННЫЙ ЗАМОК
СОБОЛЬ 4**

Аппаратно-программный модуль доверенной загрузки,
функционирующий в среде UEFI

ПРЕИМУЩЕСТВА

 КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМНОГО
РЕЕСТРА WINDOWS, АППАРАТНОЙ
КОНФИГУРАЦИИ КОМПЬЮТЕРА И ФАЙЛОВ
ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ

 ИНТЕГРАЦИЯ С СЗИ SECRET NET STUDIO
И SECRET NET LSP



ВОССТАНОВЛЕНИЕ

- П9** Система резервного копирования и
восстановления данных
- П1** Система контроля
неизменности конфигурации



Основные направления защиты информации – Восстановление



НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**КОД**
безопасности

**ЭЛЕКТРОННЫЙ ЗАМОК
СОБОЛЬ 4**
Аппаратно-программный модуль доверенной загрузки,
функционирующий в среде UEFI

ПРЕИМУЩЕСТВА
КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМНОГО
РЕЕСТРА WINDOWS, АППАРАТНОЙ
КОНФИГУРАЦИИ КОМПЬЮТЕРА И ФАЙЛОВ
ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ
ИНТЕГРАЦИЯ С СЗИ SECRET NET STUDIO
И SECRET NET LSP



ВОССТАНОВЛЕНИЕ

- п9** Система резервного копирования и
восстановления данных
- п1** Система контроля
неизменности конфигурации

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОЙ СРЕДЫ

Контроль неизменности файлов и физических секторов жесткого диска, а также файловых систем: NTFS, FAT16, FAT32, EXT2, EXT3, EXT4 в ОС семейства Linux и Windows. Поддержка широкого списка операционных систем семейства Windows и Linux.



Основные направления защиты информации – Восстановление

НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**КОД**
безопасности

**ЭЛЕКТРОННЫЙ ЗАМОК
СОБОЛЬ 4**
Аппаратно-программный модуль доверенной загрузки,
функционирующий в среде UEFI

ПРЕИМУЩЕСТВА
КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМНОГО
РЕЕСТРА WINDOWS, АППАРАТНОЙ
КОНФИГУРАЦИИ КОМПЬЮТЕРА И ФАЙЛОВ
ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ
ИНТЕГРАЦИЯ С СЗИ SECRET NET STUDIO
И SECRET NET LSP



ВОССТАНОВЛЕНИЕ

- п9** Система резервного копирования и
восстановления данных
- п1** Система контроля
неизменности конфигурации

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОЙ СРЕДЫ

Контроль неизменности файлов и физических секторов жесткого диска, а также файловых систем: NTFS, FAT16, FAT32, EXT2, EXT3, EXT4 в ОС семейства Linux и Windows. Поддержка широкого списка операционных систем семейства Windows и Linux.

КОНТРОЛЬ ЦЕЛОСТНОСТИ РЕЕСТРА WINDOWS

Контроль неизменности системного реестра Windows повышает защищенность рабочих станций от несанкционированных действий внутри операционной системы.



Основные направления защиты информации – Восстановление

НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КОД
безопасности

ЭЛЕКТРОННЫЙ ЗАМОК
СОБОЛЬ 4
Аппаратно-программный модуль доверенной загрузки,
функционирующий в среде UEFI

ПРЕИМУЩЕСТВА

- КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМНОГО РЕЕСТРА WINDOWS, АППАРАТНОЙ КОНФИГУРАЦИИ КОМПЬЮТЕРА И ФАЙЛОВ ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ
- ИНТЕГРАЦИЯ С СМ SECRET NET STUDIO И SECRET NET LSP



ВОССТАНОВЛЕНИЕ

- П9** Система резервного копирования и восстановления данных
- П1** Система контроля неизменности конфигурации

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОЙ СРЕДЫ

Контроль неизменности файлов и физических секторов жесткого диска, а также файловых систем: NTFS, FAT16, FAT32, EXT2, EXT3, EXT4 в ОС семейства Linux и Windows. Поддержка широкого списка операционных систем семейства Windows и Linux.

КОНТРОЛЬ ЦЕЛОСТНОСТИ РЕЕСТРА WINDOWS

Контроль неизменности системного реестра Windows повышает защищенность рабочих станций от несанкционированных действий внутри операционной системы.

КОНТРОЛЬ КОНФИГУРАЦИИ

Контроль неизменности конфигурации компьютера: PCI-устройств, SMBIOS.



НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ	ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
 ИДЕНТИФИКАЦИЯ	П Система учета активов и управления рисками ИБ П2 Система контроля защищённости ИТ-ресурсов
 ЗАЩИТА	П3 Система защиты периметра сети П4 Системы управления доступом, антивирусной защиты и защиты хостов
 ОБНАРУЖЕНИЕ	П5 Единая система сбора и корреляции событий безопасности П6 Система обнаружения аномалий в технологических сегментах
 РЕАГИРОВАНИЕ	П7 Система мониторинга, обработки и реагирования на инциденты ИБ П8 Система повышения осведомленности персонала в вопросах ИБ
 ВОССТАНОВЛЕНИЕ	П9 Система резервного копирования и восстановления данных П1 Система контроля неизменности конфигурации



Основные направления защиты информации и программы проектов ИБ



МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ



- определяет состав и содержание мер защиты информации
- определяет порядок выбора и применимость мер защиты информации в зависимости от типа ИС и АСУ ТП и сегментах их функционирования
- определяет требования к техническим решениям

ТЕХНИЧЕСКИЙ СТАНДАРТ



НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ



ИДЕНТИФИКАЦИЯ



ЗАЩИТА



ОБНАРУЖЕНИЕ



РЕАГИРОВАНИЕ



ВОССТАНОВЛЕНИЕ

ПРОГРАММА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П

Система учета активов и управления рисками ИБ

П2

Система контроля защищённости ИТ-ресурсов

П3

Система защиты периметра сети

П4

Системы управления доступом, антивирусной защиты и защиты хостов

П5

Единая система сбора и корреляции событий безопасности

П6

Система обнаружения аномалий в технологических сегментах

П7

Система мониторинга, обработки и реагирования на инциденты ИБ

П8

Система повышения осведомленности персонала в вопросах ИБ

П9

Система резервного копирования и восстановления данных

П1

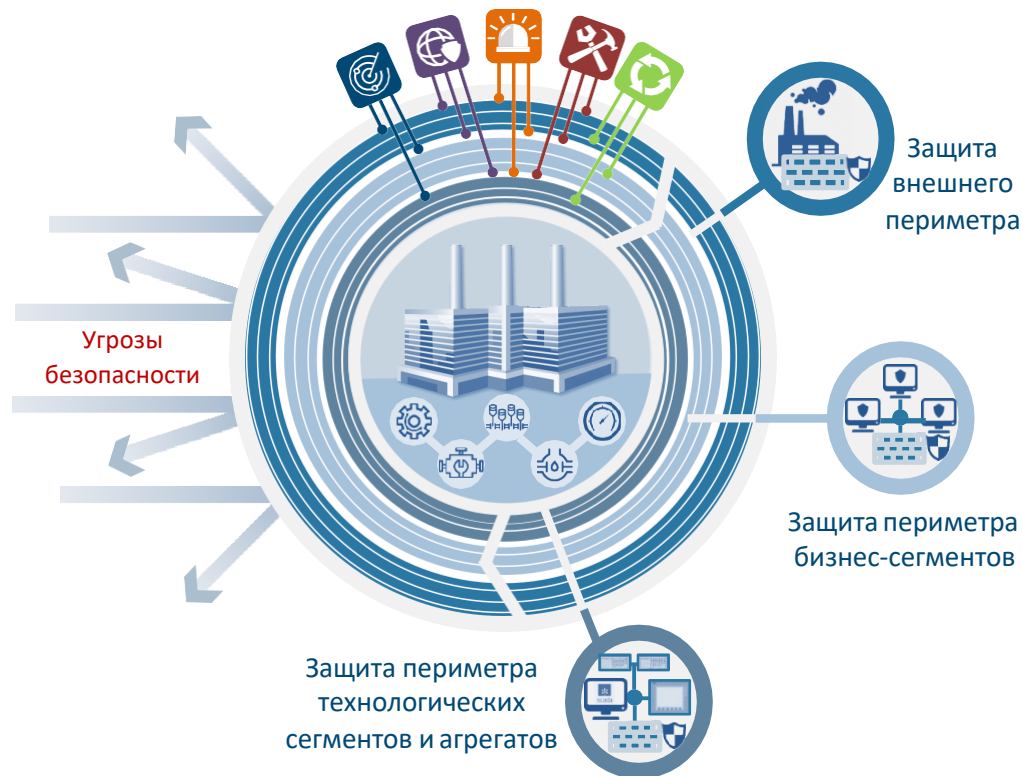
Система контроля неизменности конфигурации



Эшелонированная система защиты

Определяющие факторы

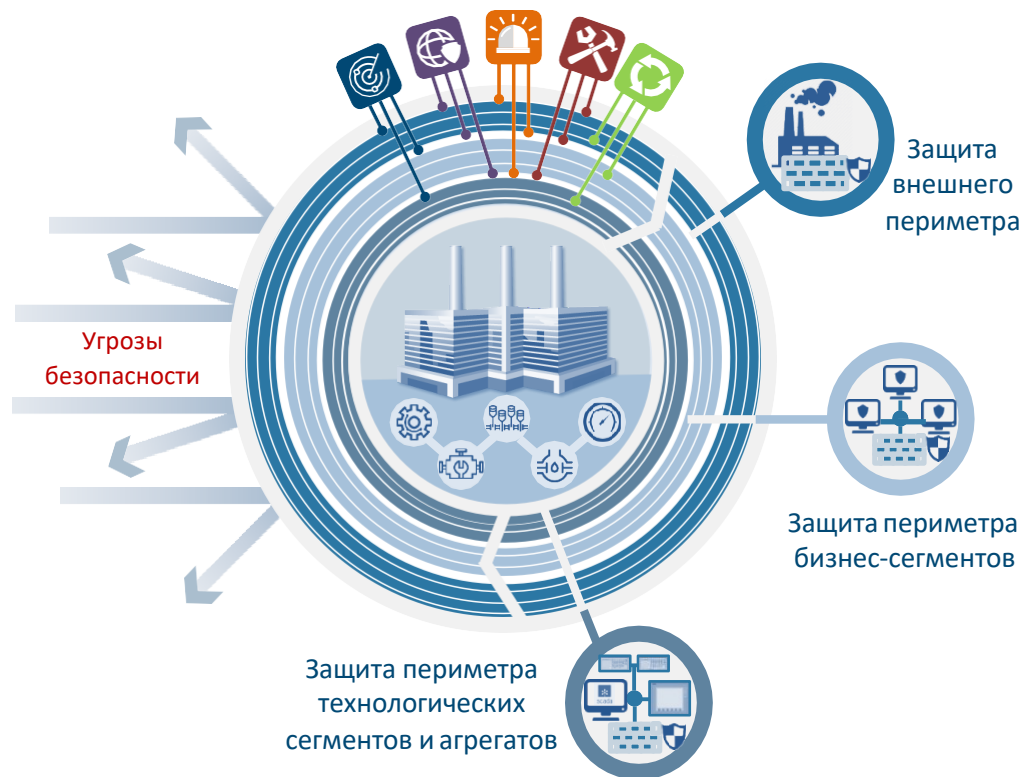
- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски
- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ
- ✓ География объектов защиты
- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA
- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов
- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики
- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты



Эшелонированная система защиты

Определяющие факторы

- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски
- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ
- ✓ География объектов защиты
- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA
- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов
- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики
- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты



Структура и состав

Сетевая безопасность

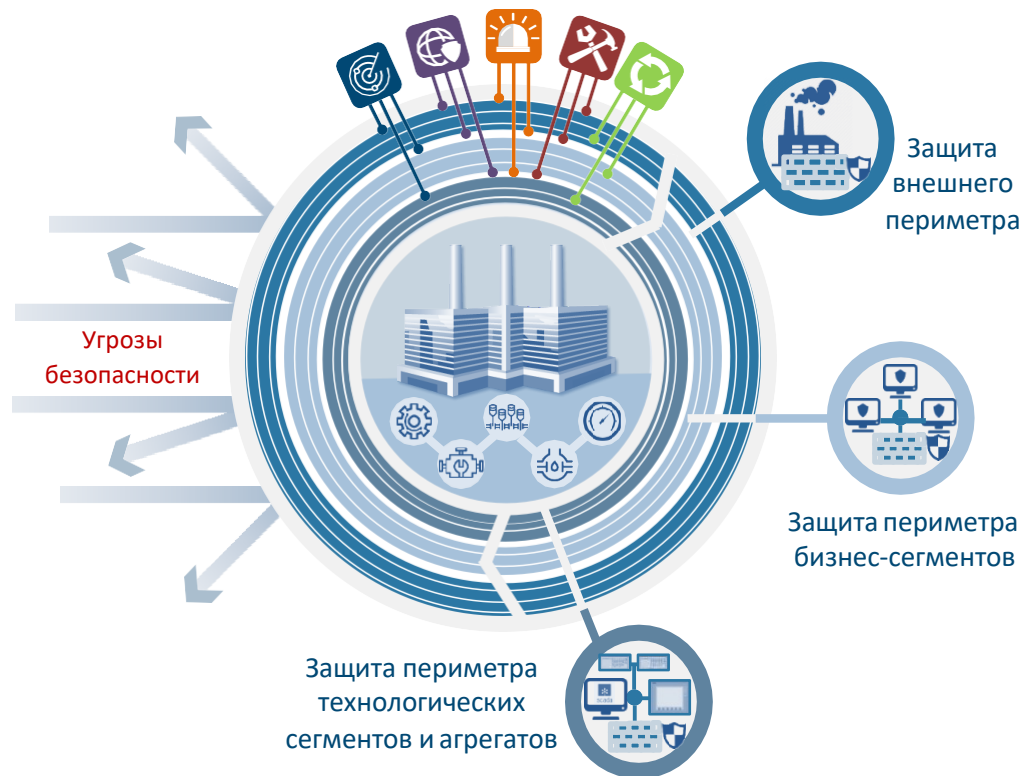


Эшелонированная система защиты

Определяющие факторы

- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски
- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ
- ✓ География объектов защиты
- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA
- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов
- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики
- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты

Эшелонированная система защиты



Структура и состав

Сетевая безопасность



- ✓ Многофункциональные МЭ (NGFW)
- ✓ Микросегментация (Microsegmentation)
- ✓ Межсетевой экран веб-приложений (WAF)
- ✓ Защищенный удаленный доступ (VPN)
- ✓ Контроль доступа в Интернет (Web-Gateway)
- ✓ Защита электронной почты (Email Gateway)
- ✓ Предотвращение вторжений (IPS)
- ✓ Защита от DDoS-атак

Прикладная безопасность

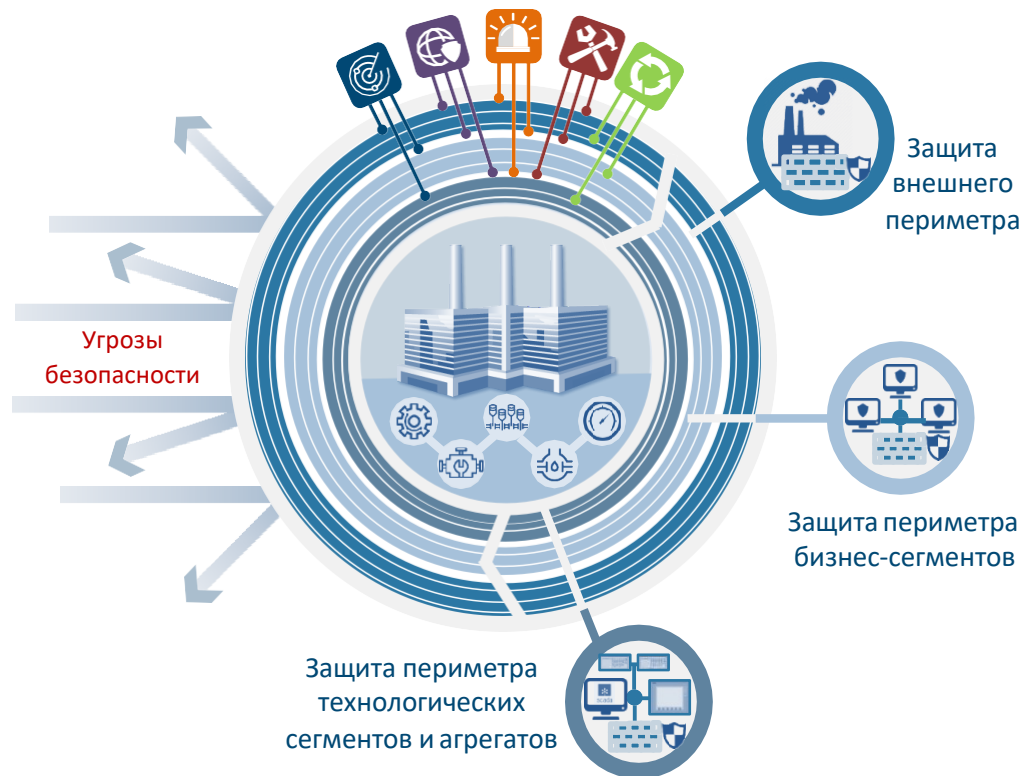


Эшелонированная система защиты

Определяющие факторы

- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски
- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ
- ✓ География объектов защиты
- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA
- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов
- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики
- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты

Эшелонированная система защиты



Структура и состав

Сетевая безопасность

- ✓ Многофункциональные МЭ (NGFW)
- ✓ Микросегментация (Microsegmentation)
- ✓ Межсетевой экран веб-приложений (WAF)
- ✓ Защищенный удаленный доступ (VPN)
- ✓ Контроль доступа в Интернет (Web-Gateway)
- ✓ Защита электронной почты (Email Gateway)
- ✓ Предотвращение вторжений (IPS)
- ✓ Защита от DDoS-атак

Прикладная безопасность

- ✓ Антивирусная защита (Antivirus)
- ✓ Защита от утечек данных (DLP)
- ✓ Шифрование данных (Data/Disc Encryption)
- ✓ Защита от APT и 0-Day угроз (Sandbox)
- ✓ Защита баз данных (Database Protection)

Управление доступом

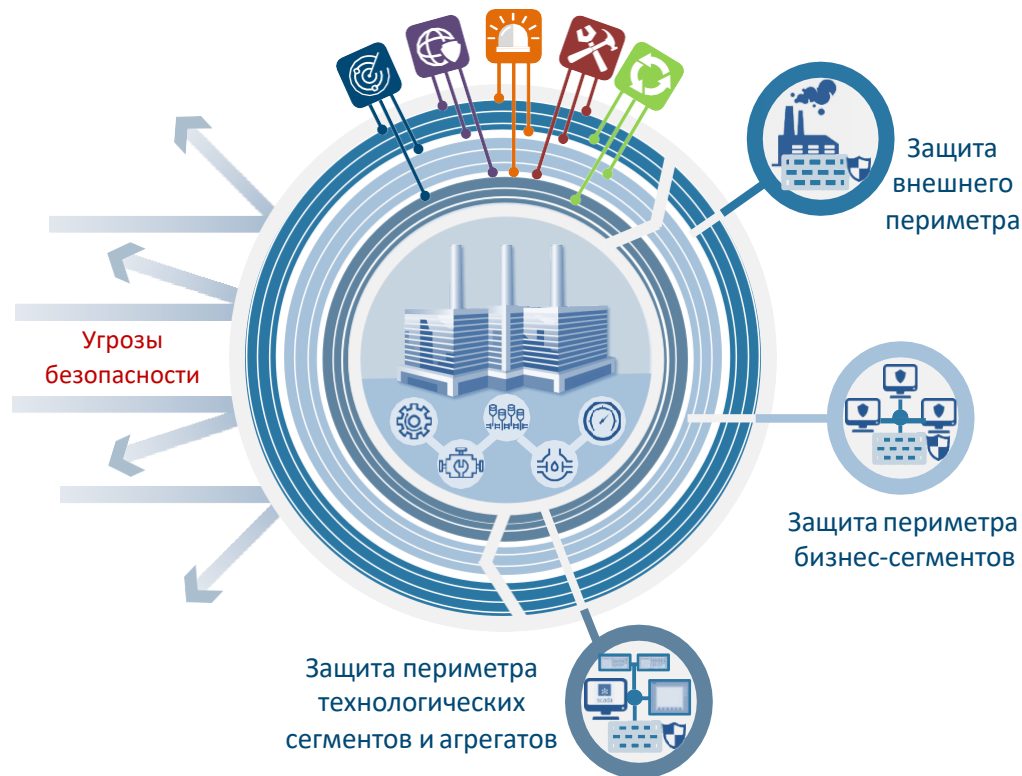


Эшелонированная система защиты

Определяющие факторы

- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски
- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ
- ✓ География объектов защиты
- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA
- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов
- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики
- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты

Эшелонированная система защиты



Структура и состав

Сетевая безопасность

- ✓ Многофункциональные МЭ (NGFW)
- ✓ Микросегментация (Microsegmentation)
- ✓ Межсетевой экран веб-приложений (WAF)
- ✓ Защищенный удаленный доступ (VPN)
- ✓ Контроль доступа в Интернет (Web-Gateway)
- ✓ Защита электронной почты (Email Gateway)
- ✓ Предотвращение вторжений (IPS)
- ✓ Защита от DDoS-атак

Прикладная безопасность

- ✓ Антивирусная защита (Antivirus)
- ✓ Защита от утечек данных (DLP)
- ✓ Шифрование данных (Data/Disc Encryption)
- ✓ Защита от APT и 0-Day угроз (Sandbox)
- ✓ Защита баз данных (Database Protection)

Управление доступом

- ✓ Аутентификация и авторизация (AAA)
- ✓ Многофакторная аутентификация
- ✓ Управление мобильными устройствами (MDM)
- ✓ Управление привилегированным доступом (PIM)
- ✓ Управление идентификационными данными (IDM)

Аудит и мониторинг



Эшелонированная система защиты

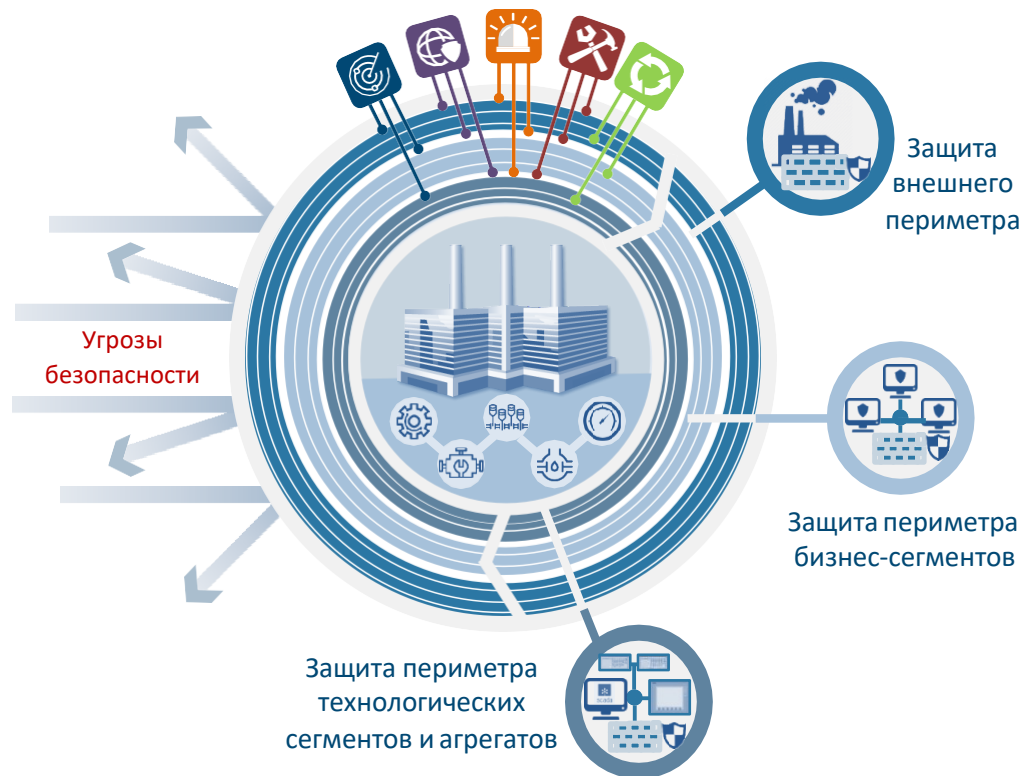
(INSIGHTS) (BEST PRACTICE)



Определяющие факторы

- ✓ Специфика бизнес-процессов
- ✓ Производственные и операционные риски
- ✓ Ландшафт безопасности (тенденции)
- ✓ Актуальные угрозы и мотивация нарушителя
- ✓ Актуальные сценарии ИБ
- ✓ География объектов защиты
- ✓ Организационно-штатная структура
- ✓ Квалификация персонала
- ✓ Модель эксплуатации АСУ и ИТ-систем
- ✓ Требования к непрерывности, SLA
- ✓ Наличие и зрелость процессов
- ✓ Степень централизации процессов
- ✓ Требования законодательства
- ✓ Отраслевые требования
- ✓ Внутренние нормативные акты
- ✓ Стандарты и мировые практики
- ✓ Топология и инфраструктура
- ✓ Архитектура АСУ и ИТ-систем
- ✓ Программные и технические средства
- ✓ Существующие средства защиты

Эшелонированная система защиты



SOC / SOAR



Кросс-интеграции со средствами системой мониторинга и анализа состояния и системой автоматизации процессов ИБ

Структура и состав

Сетевая безопасность



- ✓ Многофункциональные МЭ (NGFW)
- ✓ Микросегментация (Microsegmentation)
- ✓ Межсетевой экран веб-приложений (WAF)
- ✓ Защищенный удаленный доступ (VPN)
- ✓ Контроль доступа в Интернет (Web-Gateway)
- ✓ Защита электронной почты (Email Gateway)
- ✓ Предотвращение вторжений (IPS)
- ✓ Защита от DDoS-атак

Прикладная безопасность



- ✓ Антивирусная защита (Antivirus)
- ✓ Защита от утечек данных (DLP)
- ✓ Шифрование данных (Data/Disc Encryption)
- ✓ Защита от APT и 0-Day угроз (Sandbox)
- ✓ Защита баз данных (Database Protection)

Управление доступом



- ✓ Аутентификация и авторизация (AAA)
- ✓ Многофакторная аутентификация
- ✓ Управление мобильными устройствами (MDM)
- ✓ Управление привилегированным доступом (PIM)
- ✓ Управление идентификационными данными (IDM)

Аудит и мониторинг



- ✓ Управление уязвимостями (Vulnerability Manager)
- ✓ Выявление сетевых аномалий (Anomaly Detection)
- ✓ Профилирование сетевой активности (NBA)
- ✓ Профилирование активности пользователей (UAA)
- ✓ Анализаторы исходного кода

Полный цикл работ по ИБ



**Благодарю
за внимание!**

