ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ “МЭИ”

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Систематизация подходов к обеспечению безопасности и надежности работы цифровых систем РЗА в течении всего жизненного цикла.

Волошин Александр Александрович
К.т.н, доцент
Почетный доктор электротехники,
Чл.-корр. АЭН РФ

Директор Центра НТИ
«Технологии транспортировки электроэнергии и распределенных интеллектуальных энергосистем»
НИУ «МЭИ»

Обеспечение безопасности – это непрерывный процесс на протяжении всего жизненного цикла

Безопасность – это состояние, при котором действие внутренних и внешних факторов не приводит к негативным последствиям (нарушению функционирования/отказам)

Информационная безопасность - это безопасность информации, т.е. обеспечение целостности, доступности и конфиденциальности информации (объект - информация)

Кибербезопасность - это безопасность кибернетических Систем, т.е. обеспечение их устойчивого функционирования (без отказов) в условиях реализации компьютерных атак (объект - система)

Компьютерная атака – это попытка нарушить функционирование Системы путем целенаправленного воздействия с использованием специальных инструментов и/или ПО.
Нарушение функционирования = снижение показателей НАДЖЕНОСТИ

Угроза - потенциально возможное событие, наступление которого приводит к нарушению безопасности

Уязвимость – известный недостаток, который можно использовать чтобы реализовать угрозу

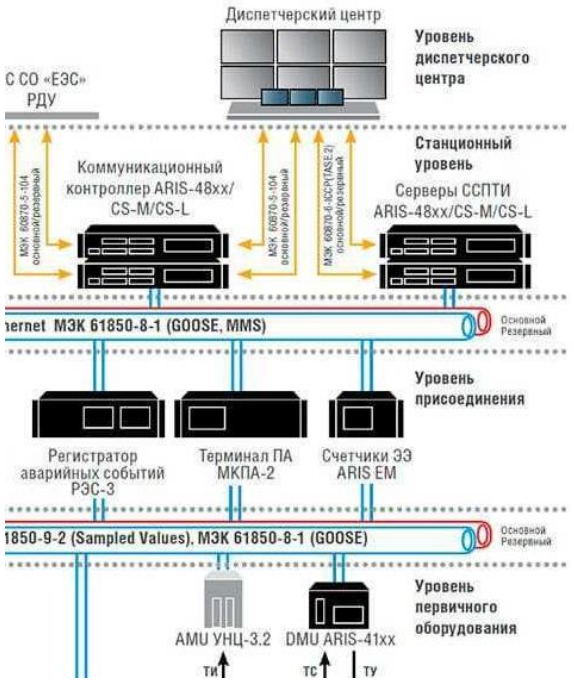
Процесс обеспечения кибербезопасности должен быть проактивным!

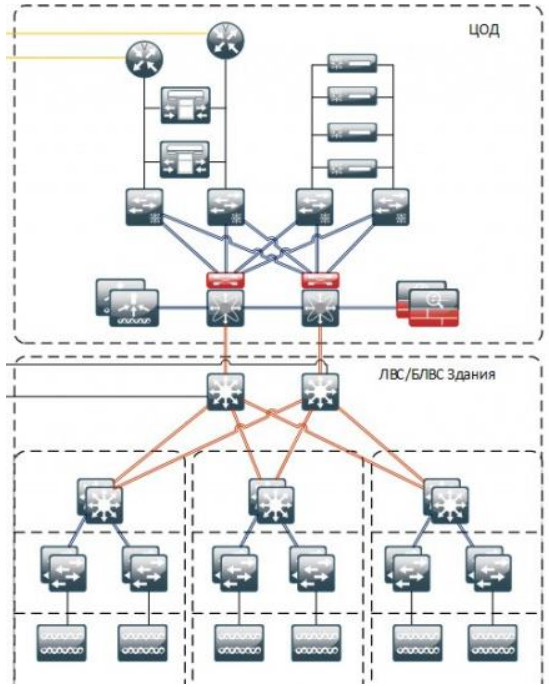
Причем здесь Релейная защита и автоматика?

Современные МП терминалы РЗА :

- CPU
- Оперативная память
- Энергонезависимая память (Flash)
- Сетевые интерфейсы Ethernet
- BIOS/UEFI
- Операционная система (например, Linux)
- Системное ПО
- Прикладное ПО
- ЖК экран

Это РЗА или не РЗА?





Причем здесь Релейная защита и автоматика?

bdu.fstec.ru

БДУ - Уязвимости

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение

Главная / Список уязвимостей / BDU:2019-04217

BDU:2019-04217: Уязвимость программного обеспечения DIGSI 5 и устройств SIPROTEC 5, связанная с недостаточной проверкой вводимых данных, позволяющая нарушителю получать, модифицировать и удалять файлы в системе

Вид

Описание уязвимости	Уязвимость программного обеспечения DIGSI 5 и устройств SIPROTEC 5 связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получать, модифицировать и удалять файлы в определенных частях системы путем отправки специально подготовленных пакетов на порт 443/TCP
Вендор	Siemens AG
Наименование ПО	SIPROTEC 5, DIGSI 5, SIPROTEC 5 6MD85, SIPROTEC 5 6MD86, SIPROTEC 5 6MD89, SIPROTEC 5 7UM85, SIPROTEC 5 7SA87, SIPROTEC 5 7SD87, SIPROTEC 5 7SL87, SIPROTEC 5 7VK87, SIPROTEC 5 7SA82, SIPROTEC 5 7SA86, SIPROTEC 5 7SD82, SIPROTEC 5 7SD86, SIPROTEC 5 7SL82, SIPROTEC 5 7SL86, SIPROTEC 5 7SJ86, SIPROTEC 5 7SK82, SIPROTEC 5 7SK85, SIPROTEC 5 7SJ82, SIPROTEC 5 7SJ85, SIPROTEC 5 7UT82, SIPROTEC 5 7UT85, SIPROTEC 5 7UT86, SIPROTEC 5 7UT87, SIPROTEC 5 7VE85
Версия ПО	- (SIPROTEC 5) до V7.90 (DIGSI 5) до V7.90 (SIPROTEC 5 6MD85) до V7.90 (SIPROTEC 5 6MD86) до V7.90 (SIPROTEC 5 6MD89)
Тип ПО	ПО программно-аппаратного средства АСУ ТП, Средство АСУ ТП

раскрыть

Новое требование к РЗА - устойчивость к кибератакам

Федеральный закон от 26.07.2017 г. № 187-ФЗ

О безопасности критической информационной инфраструктуры Российской Федерации

(В редакции Федерального закона от 10.07.2023 № 312-ФЗ)

Статья 2. Основные понятия

2) безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

КИБЕРУЧЕНИЯ НАТО

- Киберучения НАТО «Locked Shields»
- Организуются и проводятся Центром передового опыта по совместной защите от киберугроз с 2010 года.
- Киберучения НАТО «CyberCoalition»

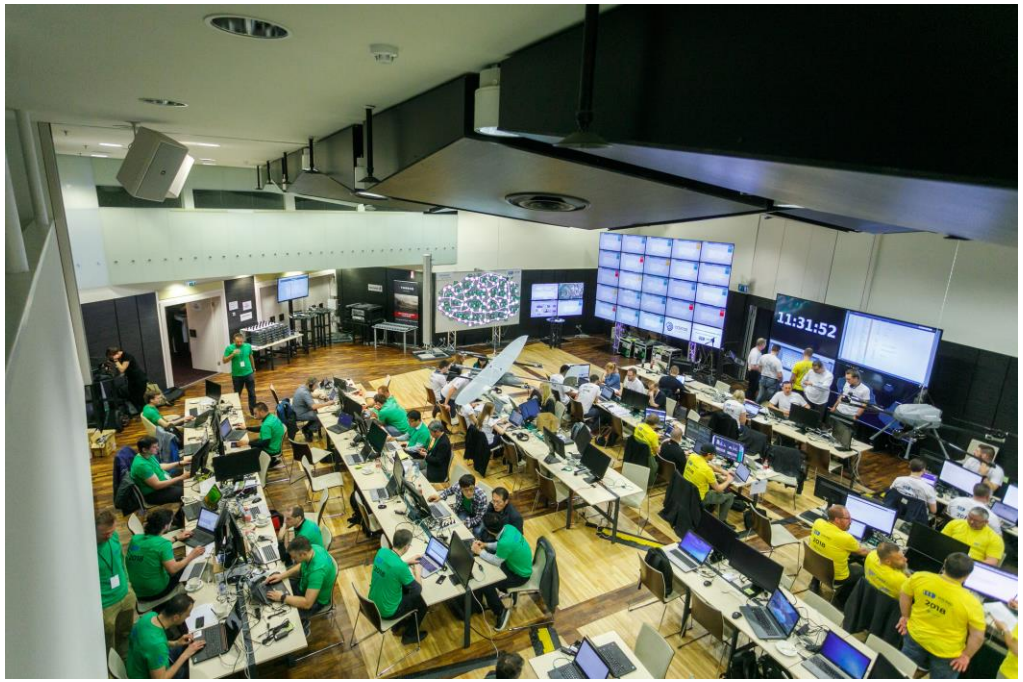
Организуются и проводятся Центром передового опыта по совместной защите от киберугроз (CCDCOE) с 2006 года.

В рамках киберучений имитируются сценарии массированных кибератак на объекты критической инфраструктуры государства или ряда государств.

КИБЕРУЧЕНИЯ НАТО

CCDCOE ежегодно с 2010 года организует мероприятие, позволяющее экспертам по кибербезопасности повысить свои навыки :

- защиты национальных систем ИТ
- защиты критически важной инфраструктуры в условиях атак в режиме реального времени.



Основное внимание уделяется реалистичным сценариям, передовым технологиям и моделированию сложных масштабных киберинцидентов, реагирование на которые требуют принятие стратегических решений, учитывать юридические и коммуникационные аспекты (PR).

КИБЕРУЧЕНИЯ НАТО LOCKED SHIELDS 2023

38 стран участниц

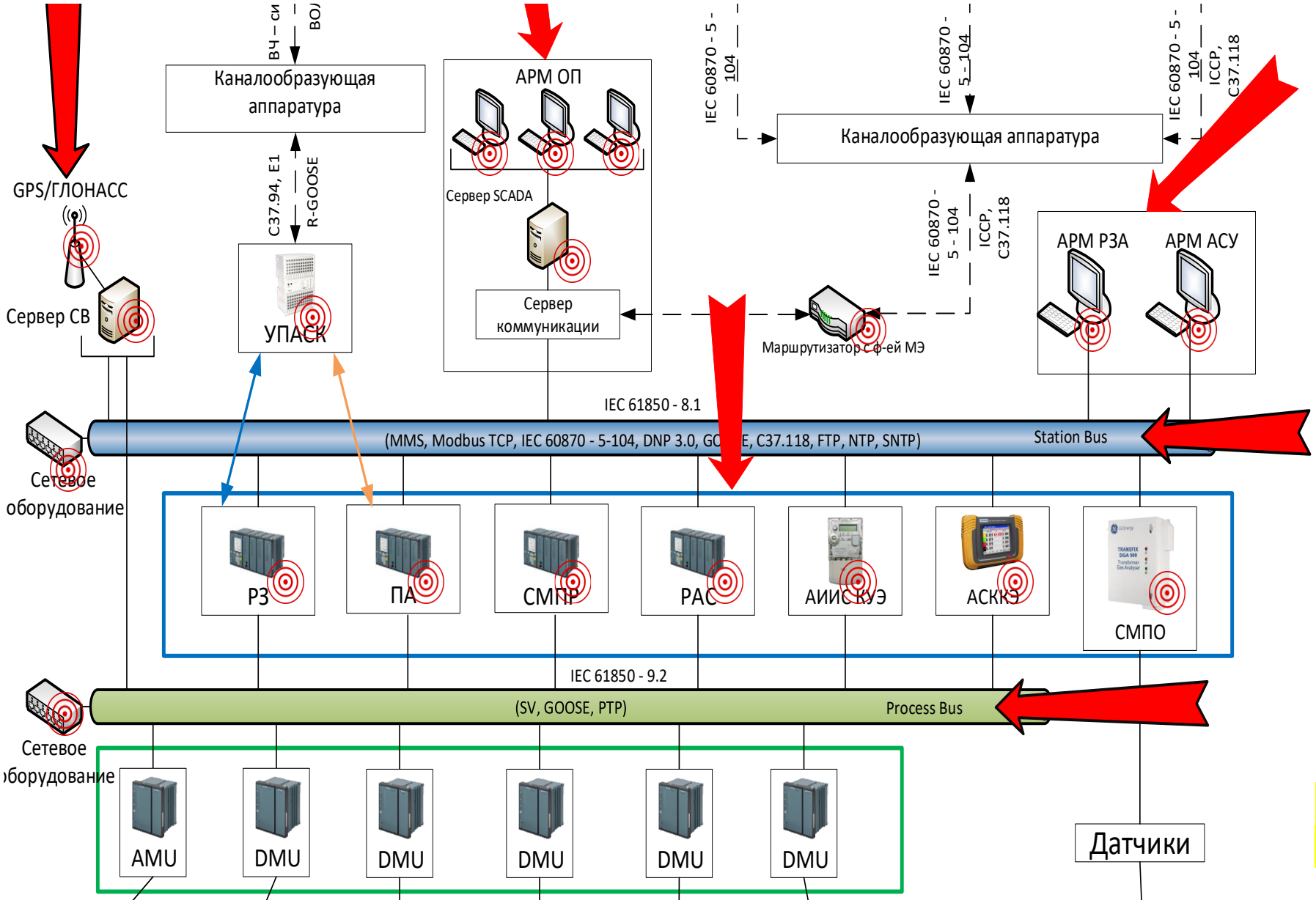
Более 3000 участников

Red Team vs Blue Team training exercise

Более 5500 виртуальных объектов

https://ccdcoe.org/exercises/locked-shields/

Модель угроз РЗА



Виды возможных атак

- GPS/ГЛОНАСС Spoofing
- GOOSE Spoofing
- MITM MMS
- MITM МЭК 60870 - 5 – 104
- Brute Force
- Риски успешных APT с ущербом

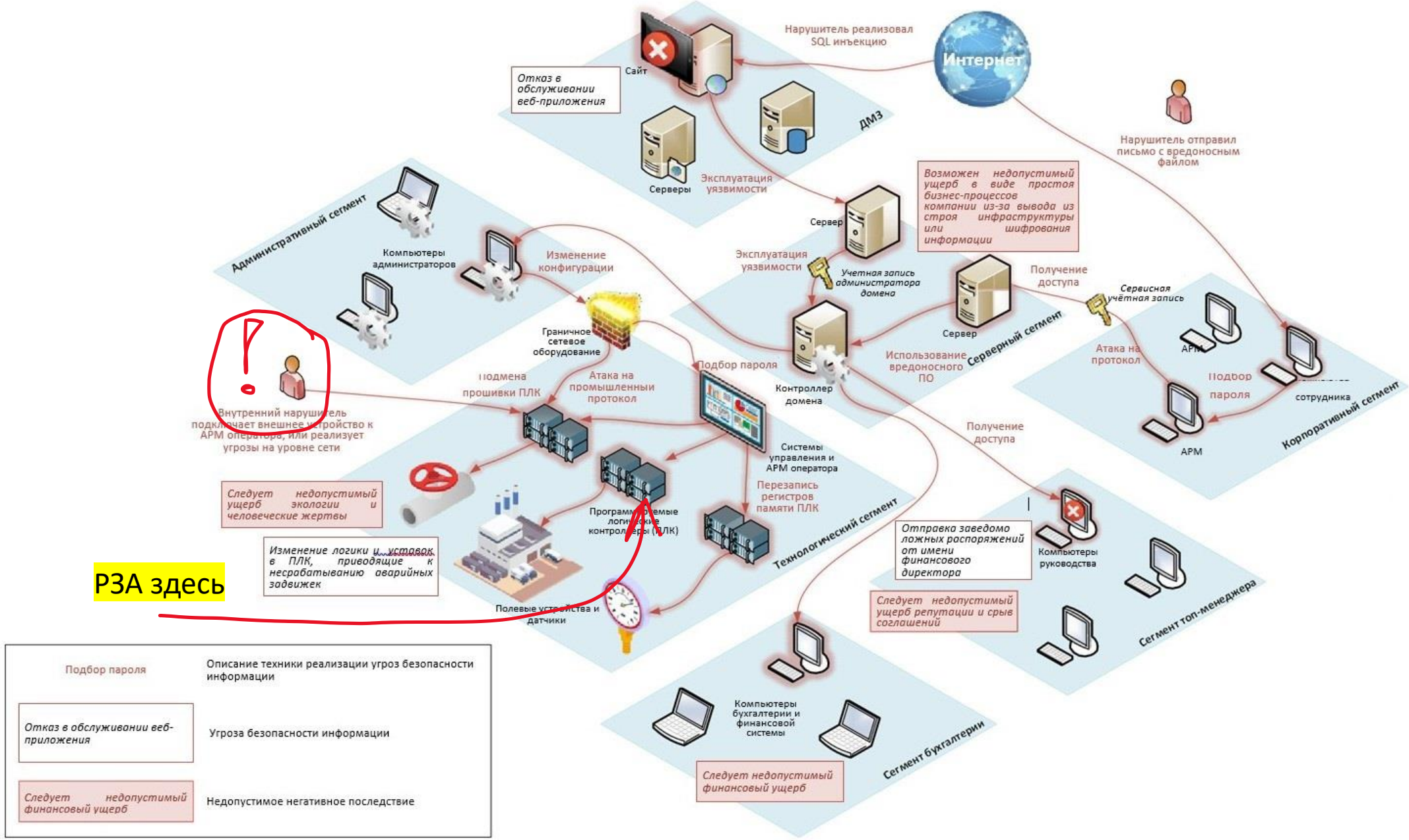
кибер- и физическим характеристикам ЦПС и SmartGrids (ААС ЕЭС, цифровым сетям)

Атаки на устройства

Атаки на протоколы

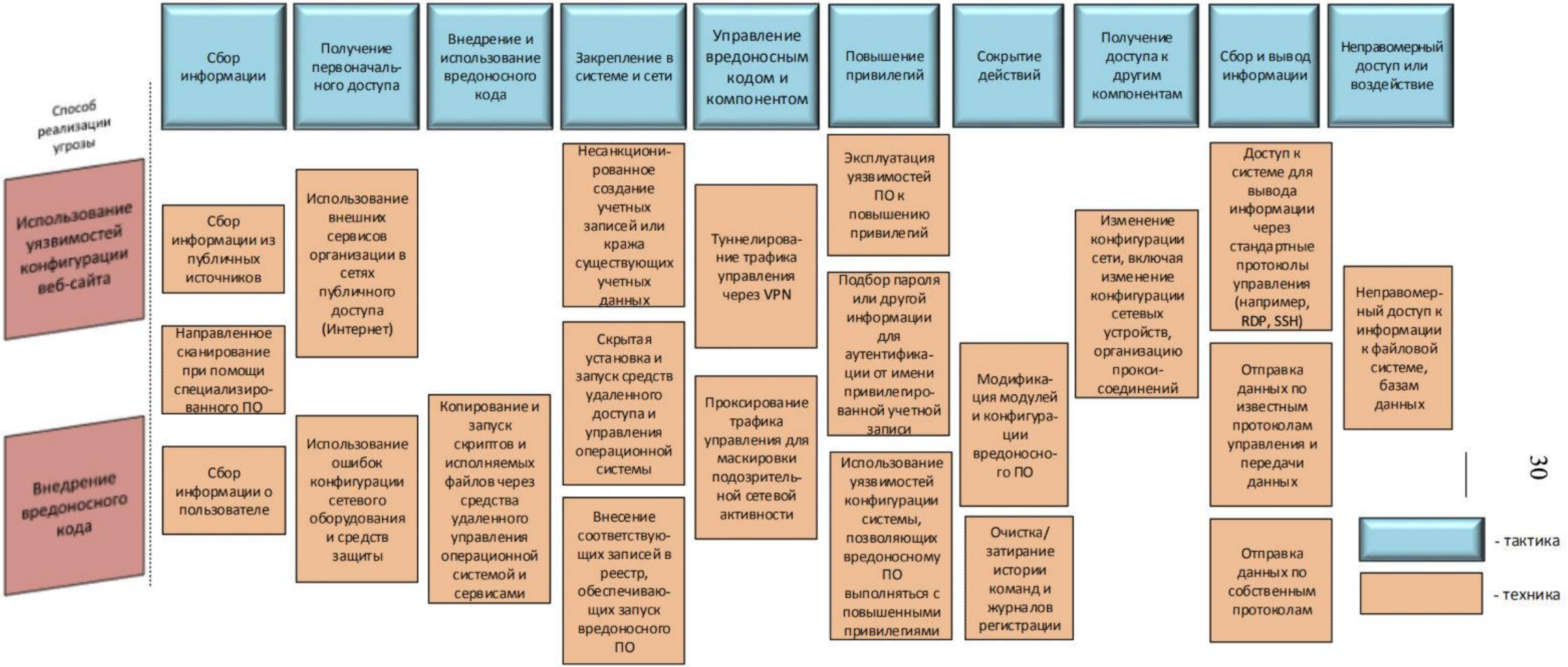
Спасет ли воздушный зазор между РЗА и корпоративной сетью?

Пример сценариев реализации кибератак



https://itsec2012.ru/metodika-ocenki-ugroz-bezopasnosti-informacii-utverzhdena-fstek-rossii-5-fevralya-2021-g-5-ocenka-vozmozhnosti-realizacii-vozniknoveniya-ugroz-bezopasnosti-informacii-i-opredelenie-ih-aktualnosti

Техники и тактики



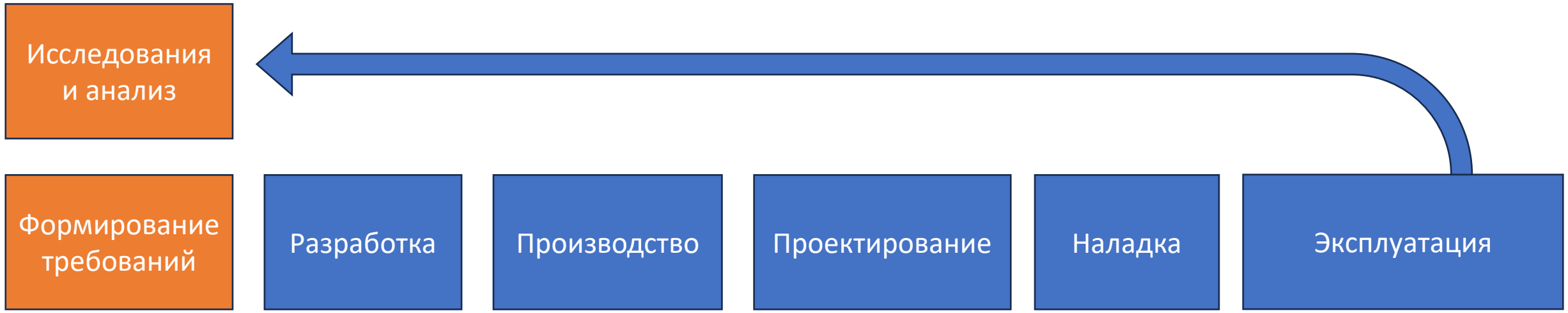
Из методического пособия ФСТЭК

1) Кибератаки осуществляются людьми -> постоянно будут появляться новые типы уязвимостей и атак

2) Кибератака может длиться несколько месяцев (!) -> есть возможность обнаружить и отреагировать

Кибератаки возможны в течение всего жизненного цикла РЗА

Кибератаки возможны в течение всего жизненного цикла РЗА

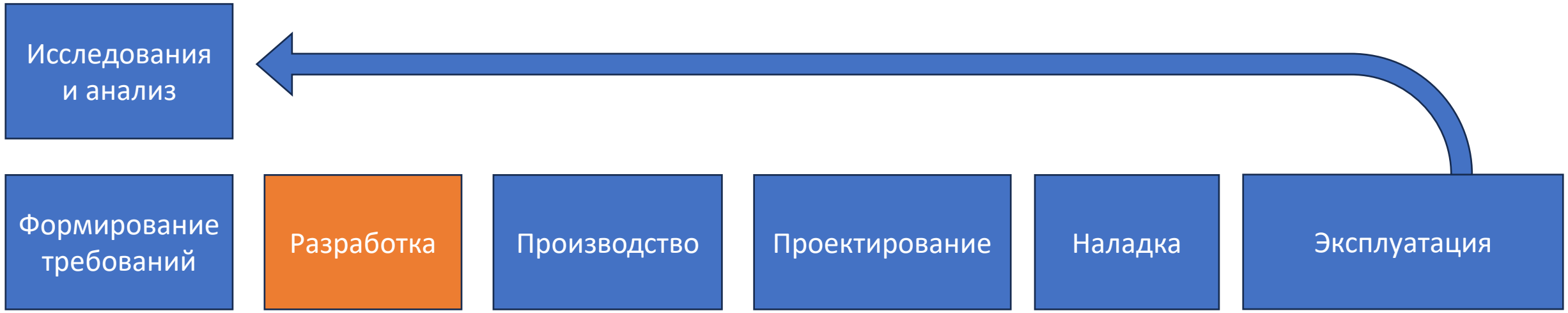


Риски: потеря статистических данных, потеря результатов исследований, подмена результатов, шпионаж

Пример угрозы: фишинг, вирусы-шифровальщики

Решения: антивирусы, резервное копирование, мониторинг трафика, «цифровая гигиена», идентификация и аутентификация, разграничение уровней доступа, периодический аудит и анализ защищенности

Кибератаки возможны в течение всего жизненного цикла РЗА

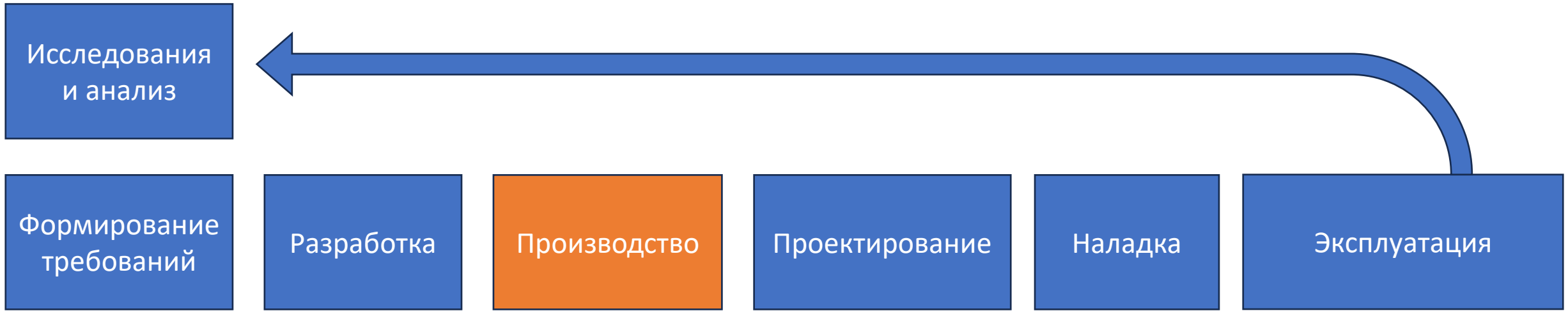


Риски: ПО с легко эксплуатируемыми уязвимостями, недокументированные возможности ПАК, внедрение в ПО вредоносного кода нарушителями, включение в документацию вредоносных инструкций для пользователей

Пример угрозы: ПО из open-source, ПО и компоненты от «недружественных» поставщиков, внедрение в ПО вредоносного кода

Решения: построение конвейера разработки безопасного ПО (управление зависимостями, статический анализ, Фаззинг, динамический анализ), доверенные ОС со встроенными модулями безопасности, доверенные компоненты ПАК, концепция «Zero Thrust», Концепция «Secure by Design», репозитарии с доверенными программными библиотеками, встроенные средства защиты информации, защищенные протоколы передачи данных, внешний аудит защищенности, поиск и устранение уязвимостей с привлечением спец. Лабораторий (pen-test)

Кибератаки возможны в течение всего жизненного цикла РЗА

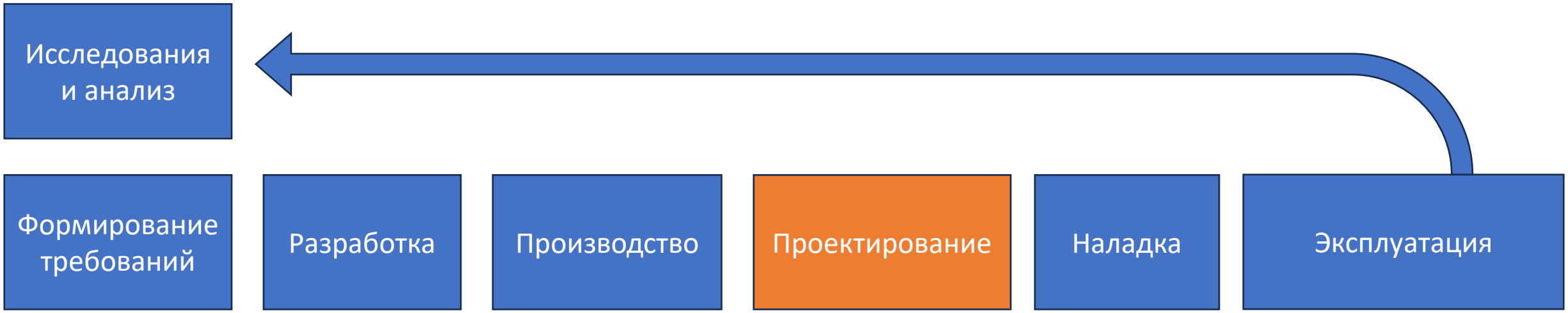


Риски: ПО с легко эксплуатируемыми уязвимостями, внедрение в ПО вредоносного кода нарушителями, включение в документацию вредоносных инструкций для пользователей

Пример угрозы: фишинг, повышение уровня доступа

Решения: антивирусы, резервное копирование, мониторинг трафика, «цифровая гигиена», идентификация и аутентификация, разграничение уровней доступа, периодический аудит и анализ защищенности, контроль целостности ПО и документации, версионирование, управление уязвимостями ПО.

Кибератаки возможны в течение всего жизненного цикла РЗА

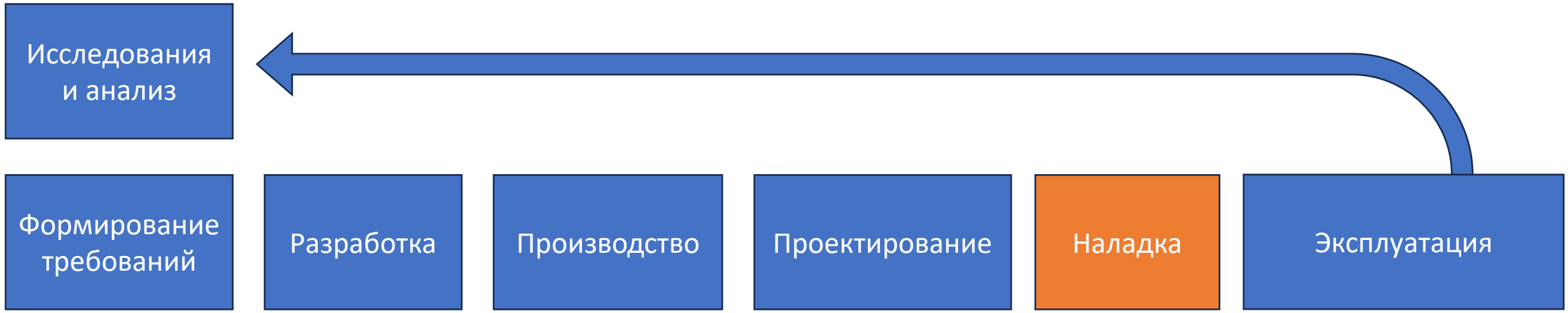


Риски: утрата проектной документации, подмена информации (изменение уставок, настроечных параметров), шпионаж, внедрение вредоносных настроек в файлы электронной документации

Пример угрозы: фишинг, повышение уровня доступа, вирусы-шифровальщики

Решения: антивирусы, резервное копирование, мониторинг трафика, «цифровая гигиена», идентификация и аутентификация, разграничение уровней доступа, периодический аудит и анализ защищенности, контроль целостности документации, версионирование.

Кибератаки возможны в течение всего жизненного цикла РЗА

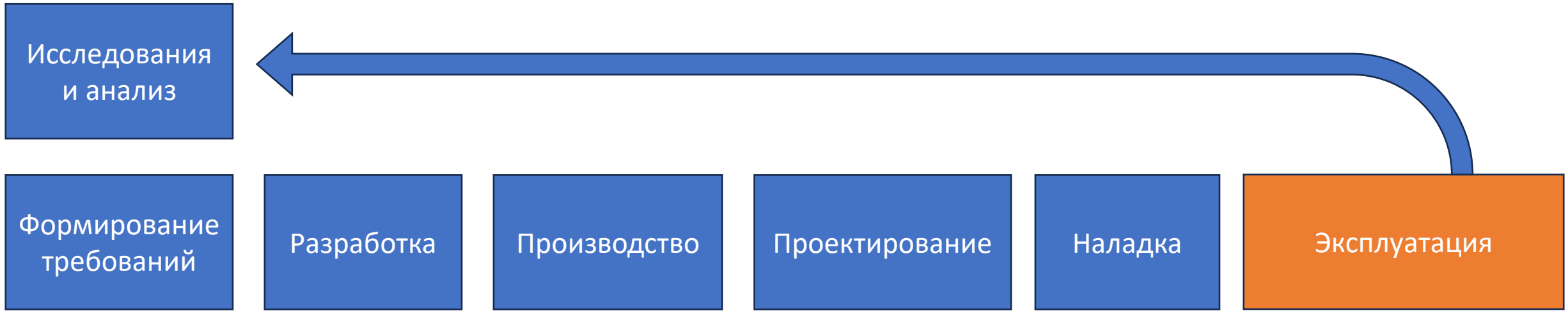


Риски: утрата исполнительной документации, подмена информации (изменение уставок, настроечных параметров), шпионаж, внедрение вредоносных настроек в файлы электронной документации, внедрение вредоносного ПО в МП РЗА, отключение/ослабление защитных мер

Пример угрозы: внедрение вредоносного ПО в РЗА при наладке, ослабление защитных мер, оставление «back door»

Решения: идентификация и аутентификация, **управление паролями**, разграничение уровней доступа, контроль целостности и версионирование документации, конфиг. файлов и ПО, версионирование, контроль реализации всех необходимых мер по обеспечению КБ, **аудит и анализ защищенности РЗА после наладки, настройка и ввод в работу всех предусмотренных проектом средств КБ,**
антивирусы, резервное копирование документации и конфигурационных файлов, «цифровая гигиена».

Кибератаки возможны в течение всего жизненного цикла РЗА

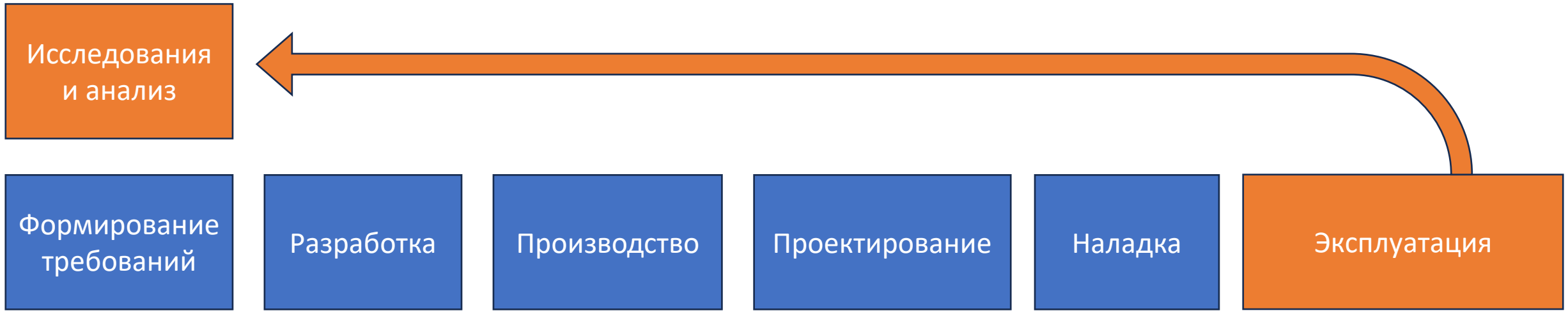


Риски: утрата или подмена данных, вывод из строя оборудования, системные аварии

Пример угрозы: несанкционированное управление КА, подмена уставок, подмена данных ТМ, вывод из строя РЗА

Решения: мониторинг трафика для выявления неправомерных действий, идентификация и аутентификация, **управление паролями**, разграничение уровней доступа, контроль целостности и версионирование документации, конфиг. файлов и ПО, версионирование, контроль реализации всех необходимых мер по обеспечению КБ, **встроенные средства КБ в МП РЗА, криптозащищенные протоколы, периодический аудит и анализ защищенности РЗА, применение всех предусмотренных проектом средств КБ, анализ эффективности средств обеспечения КБ, анализ защищенности МП РЗА, устранение найденных уязвимостей, сбор и анализ статистических данных о технологическом трафике и функционировании МП РЗА (событий безопасности), корреляционный анализ данных с нескольких энергообъектов, информирование через ГосСОПКА,** антивирусы, резервное копирование документации и конфигурационных файлов, «цифровая гигиена».

Кибератаки возможны в течение всего жизненного цикла РЗА



На самом деле с точки зрения обеспечения кибербезопасности этот процесс не выстроен.

НЕОБХОДИМО ВНЕДРЕНИЕ «ЛОВУШЕК ДЛЯ ХАКЕРОВ» (Deception Systems)
для сбора, накопления и анализа действий нарушителей

Процесс обеспечения кибербезопасности должен быть проактивным!

Т.е. мы должны обнаруживать и устранять уязвимости и угрозы до того, как нарушители их смогли использовать.

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Телеграм канал Центра НТИ МЭИ

Вопросы?

Волошин Александр Александрович

Директор Центра НТИ МЭИ
К.т.н., доцент
Почетный доктор электротехники
Чл.-корр. АЭН РФ

voloshinaa@mpei.ru

http://ЦДЭС.РФ