МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«МИРЭА - Российский технологический университет»**
**РТУ МИРЭА**

| | |
|---|---|
| **ПРИНЯТО** | **УТВЕРЖДАЮ** |
| Решением Ученого совета ИКБ | И.о. директора ИКБ |
| от «26» августа 2025 г. | _____А.А. |
| протокол № 8 | Бакаев «26» августа 2025 г. |

# Методические указания по выполнению практических работ по дисциплине «Принципы построения, проектирования и эксплуатации информационно-аналитических систем»

*( наименование дисциплины (модуля) в соответствии с учебным планом подготовки специалистов/бакалавров)*

Специальность/направление 10.05.04 «Информационно-аналитические системы безопасности»

*(код и наименование)*

Специализация /профиль Технологии информационно-аналитического мониторинга

*(код и наименование)*

Институт кибербезопасности и цифровых технологий (ИКБ)

*(краткое и полное наименование)*

Форма обучения очная

*(очная, очно-заочная, заочная)*

Программа подготовки специалитет

*(специалитет, бакалавриат)*

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

*(краткое и полное наименование кафедры, разработавшей РП дисциплины (модуля) и реализующей ее (его))*

Москва 2025

Программа дисциплины разработана **к.т.н. Бойков Д.В.**

*(степень, звание, Фамилия И.О. разработчиков)*

Программа дисциплины рассмотрена и принята

на заседании кафедры КБ-2 «Информационно-аналитические системы кибербезопасности»

*(название кафедры)*

Протокол заседания кафедры от «23» августа 2025 г. №

1 Заведующий кафедрой О.В.Трубиенко

*(подпись)* *(И.О. Фамилия)*

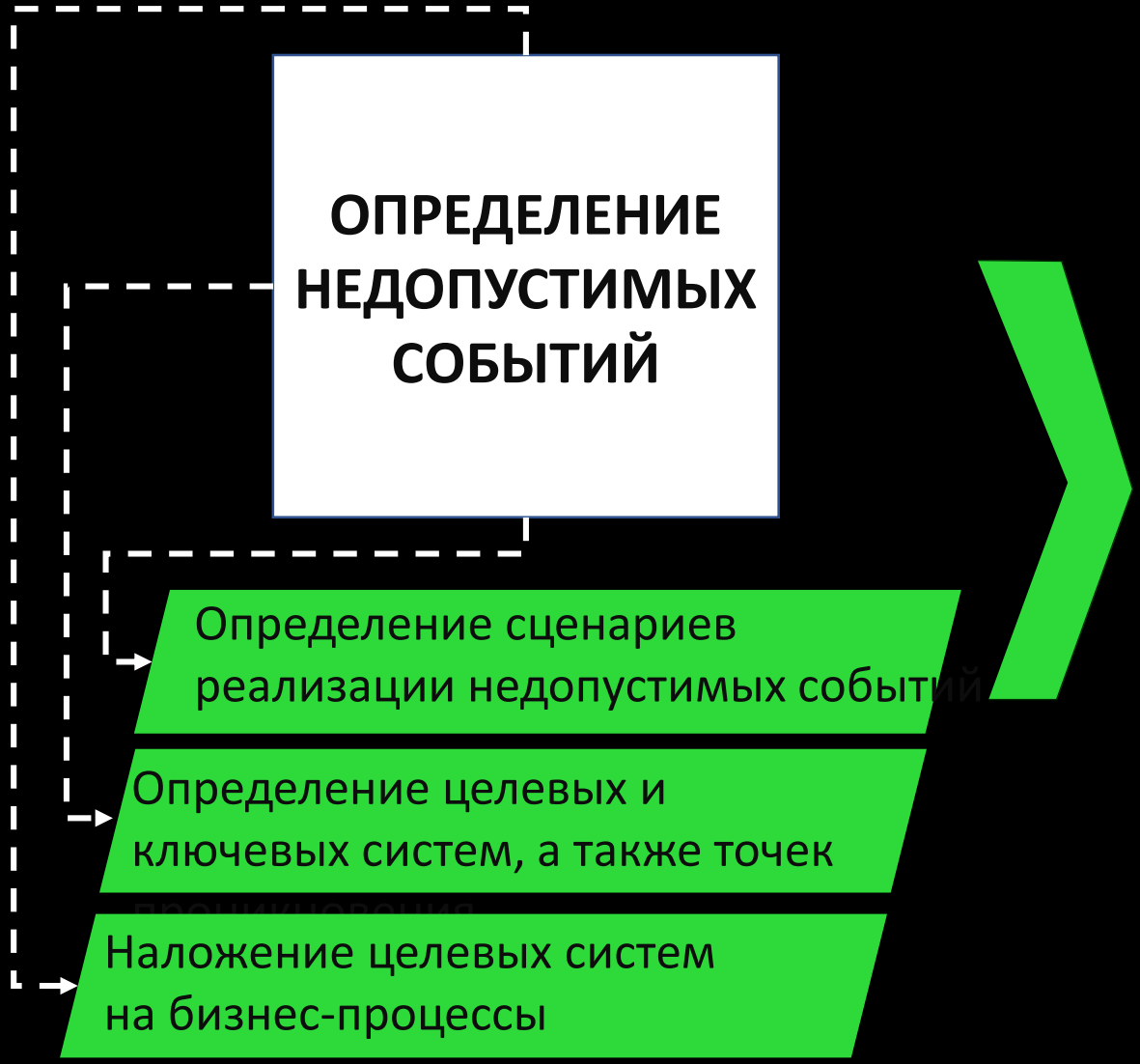
# КИБЕРТРАНСФОРМАЦИЯ - ЭТО

Процесс построения эффективной системы защиты от кибератак, включающий комплекс изменений
в IT-инфраструктуре и бизнес-процессах, обучение сотрудников практическим аспектам кибербезопасности, внедрение систем защиты информации, а также создание центра противодействия киберугрозам

# ЦЕЛЬ КИБЕРТРАНСФОРМАЦИИ

Создание таких условий, при которых злоумышленник не сможет реализовать недопустимые события в результате кибератаки

# МЕСТО КИБЕРТРАНСФОРМАЦИИ В РКБ




**КИБЕРТРАНСФОРМАЦИЯ**

ОПРЕДЕЛЕНИЕ ПЕРВООЧЕРЕДНЫХ ШАГОВ КИБЕРТРАНСФОРМАЦИ

ФОРМИРОВАНИЕ ПРОГРАММЫ КИБЕРТРАНСФОРМАЦИИ

# ОПРЕДЕЛЕНИЕ ПЕРВООЧЕРЕДНЫХ ШАГОВ КИБЕРТРАНСФОРМАЦИ

Кибертрансформация осуществляется на существующей IT-инфраструктуре, принимая во внимание ее нынешнюю конфигурацию, бизнес-процессы, используемые средства защиты информации, а также состав и квалификацию сотрудников отдела безопасности

# УЧАСТНИКИ ПРОЦЕССА ОПРЕДЕЛЕНИЯ ПЕРВООЧЕРЕДНЫХ ШАГОВ КИБЕРТРАНСФОРМАЦИИ

- Руководитель подразделения информационной безопасности либо заместитель генерального директора по ИБ
- Руководитель подразделения информационных технологий

# АНАЛИЗ УЯЗВИМЫХ МЕСТ С ЧЕТЫРЕХ СТОРОН

- СО СТОРОНЫ ИНФОРМАЦИОННЫХ СИСТЕМ
- СО СТОРОНЫ БИЗНЕС-ПРОЦЕССОВ
- СО СТОРОНЫ ПОЛЬЗОВАТЕЛЕЙ
- СО СТОРОНЫ СЕТИ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Анализ текущего IT-ландшафта в контексте информационных систем — составление перечней целевых и ключевых систем для каждого недопустимого события и всех точек проникновения

БИЗНЕС-ПРОЦЕССЫ

Анализ текущего IT-ландшафта в контексте бизнес-процессов — это определение тех бизнес-процессов,
в которых задействованы целевые системы, и оценка безопасности реализации таких процессов с точки зрения угрозы наступления недопустимого события

# ПОЛЬЗОВАТЕЛИ ЦЕЛЕВЫХ СИСТЕМ

Анализ текущего IT-ландшафта в контексте пользователей целевых систем — это оценка избыточности доступа к целевым системам как с точки зрения количества пользователей, так и с точки зрения их привилегий

# АНАЛИЗ В КОНТЕКСТЕ ПОЛЬЗОВАТЕЛЕЙ ЦЕЛЕВЫХ СИСТЕМ

Получение в IT-подразделении списков пользователей целевых систем
с указанием уровня их привилегий

Определение целесообразности и уровня доступа

Определение пользователей, не задействованных в целевом бизнес-процессе

# СЕГМЕНТАЦИЯ СЕТИ

Анализ текущего IT-ландшафта в контексте сегментации сети — это выявление кратчайших путей нарушителя к целевым системам

Путь является кратчайшим, если:

- атаковать целевую систему можно напрямую без необходимости преодолевать границы сетевых сегментов
- атаковать целевую систему напрямую нельзя без необходимости преодолевать границы сетевых сегментов, но в сегменте с целевой системой расположена точка проникновения

# РЕЗУЛЬТАТ ОПРЕДЕЛЕНИЕ ПЕРВООЧЕРЕДНЫХ ШАГОВ КИБЕРТРАНСФОРМАЦИИ

Формулирует выводы о текущей готовности IT-инфраструктуры и бизнес-процессов
к исключению возможности реализации недопустимых событий

Формулирует перечень первоочередных действий, направленных на устранение выявленных недостатков

# ФОРМИРОВАНИЕ ПРОГРАММЫ КИБЕРТРАНСФОРМАЦИИ

Определив первоочередные шаги кибертрансформации  следующим этапом является – формирование программы кибертрансформации. На основании данной программы, организация приступает к внесению изменений, в результате которых обретет устойчивость к возможным атакам хакеров

# 4 КОМПОНЕНТЫ КИБЕРТРАНСФОРМАЦИИ

## ВЫСТРАИВАНИЕ БИЗНЕС-ПРОЦЕССОВ

Изолировать критически значимые бизнес-процессы. Увеличить число шагов, необходимых для проведения успешной кибератаки. Сократить число пользователей целевых систем

## ОБУЧЕНИЕ СОТРУДНИКОВ

Обучить сотрудников способам защиты от современных киберугроз. Сократить роль человеческого фактора в возможных сценариях кибератак

## МОНИТОРИНГ И ПРЕДОТВРАЩЕНИЕ КИБЕРИНЦИДЕНТОВ

Обучить сотрудников способам защиты от современных киберугроз. Сократить роль человеческого фактора в возможных сценариях кибератак

## ХАРДЕНИНГ И ПЕРЕСТРОЕНИЕ IT-ИНФРАСТРУКТУРЫ

Свести к минимуму число точек проникновения. Настроить параметры безопасности и обновить оборудование и программное обеспечение

# ВЫСТРАИВАНИЕ БИЗНЕС-ПРОЦЕССОВ

Внесение изменений в бизнес-процесс обычно называют реинжинирингом.
В рамках концепции результативной кибербезопасности он проводится для повышения защищенности целевых систем.

ВНЕСЕНИЕ ИЗМЕНЕНИЙ В БИЗНЕС-ПРОЦЕССЫ ПОЗВОЛИТ:

- минимизировать использование целевых систем и тем самым повысить уровень их защищенности
- сократить поверхность атаки злоумышленников путем исключения целевых систем из малозначимых бизнес-процессов
- увеличить количество шагов, необходимых для реализации атаки, и сделать действия хакеров более прогнозируемыми

# ОБУЧЕНИЕ СОТРУДНИКОВ

Обучение должно содержать сведения о популярности фишинговых атак, о практике использования информационных систем, обращения с конфиденциальными данными, идентификации потенциальных угроз
и реагирования на них.

# ХАРДЕНИНГ И ПЕРЕСТРОЕНИЕ IT-ИНФРАСТРУКТУРЫ

ПРИ РАЗРАБОТКЕ ИНСТРУКЦИЙ ПО ХАРДЕНИНГУ ВАЖНО:

- определить назначение IT-актива и сетевые связи с другими объектами
- проанализировать возможность отключения неиспользуемых сервисов
- деактивировать стандартные учетные записи и сменить базовые пароли
- оценить влияние внесенных изменений на функциональность актива и безопасность

# МОНИТОРИНГ И ПРЕДОТВРАЩЕНИЕ КИБЕРИНЦИДЕНТОВ

При выстраивании или адаптации процессов мониторинга и реагирования приоритет отдается объектам, которые могут быть интересны хакеру:

## ПОПУЛЯРНЫЕ ТОЧКИ ПРОНИКНОВЕНИЯ

*сервисы электронной почты, веб-приложения и сетевое оборудование*

## РАБОЧИЕ СТАНЦИИ ПОЛЬЗОВАТЕЛЕЙ С ДОСТУПОМ К КЛЮЧЕВЫМ СИСТЕМАМ

*через них хакер может развивать атаку на вышестоящие в иерархии системы*

## ЦЕЛЕВЫЕ СИСТЕМЫ

*системы «банк — клиент» или базы данных, являющиеся целевыми системами и конечными точками атаки хакеров*

# ВЕРИФИКАЦИЯ ВЫБРАННЫХ МЕР

## ПРЕДВАРИТЕЛЬНАЯ ОЦЕНКА

Исключения возможности реализации недопустимых событий в результате кибератаки

## ПРАКТИЧЕСКАЯ ВЕРИФИКАЦИЯ

Проведение практической верификации НС на действующей IT-инфраструктуре