Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина»

Факультет комплексной безопасности ТЭК

# Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак.

Выполнил: Лазорин Д.С., группа КС-21-04.


**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

## Обозначения и сокращения

ИБ – информационная безопасность. ИР – информационный ресурс. КА – компьютерная атака. МОЗ – мероприятия по оценке степени защищенности от компьютерных атак. САЗ – средство анализа защищенности. СЗИ – средство защиты информации. ТКО – телекоммуникационное оборудование.

## Общие положения

МОЗ входят в комплекс работ, проводимых по линии предупреждения КА, и осуществляются в целях повышения состояния защищенности ИР от КА.

## Общие положения

Основными задачами МОЗ являются: выявление недостатков в области обеспечения ИБ исследуемого ИР и обусловленных ими угроз безопасности информации; выработка рекомендаций, направленных на устранение выявленных недостатков в области обеспечения ИБ.

## Порядок проведения МОЗ

МОЗ рекомендуется проводить на плановой (не реже раза в год) и внеплановой основе.

Внеплановые МОЗ рекомендуется проводить в следующих случаях:

# Порядок проведения МОЗ

внесение изменений в архитектуру ИР, которые могут оказать влияние на систему защиты информации ИР; внесение изменений в организационные и технические меры по обеспечению ИБ исследуемого ИР;

# Порядок проведения МОЗ

с целью оценки эффективности мер, направленных на устранение недостатков, выявленных по результатам предыдущих МОЗ; появление новых уязвимостей, актуальных для элементов исследуемого ИР; появление новых угроз безопасности информации, актуальных для исследуемого ИР.

## Этапы проведения МОЗ

МОЗ включают в себя следующие этапы: изучение исходных данных; определение возможностей злоумышленника по проведению КА на исследуемый ИР; подготовка отчетной документации.

## Изучение исходных данных

На данном этапе проводится изучение сведений, раскрывающих назначение, состав и порядок функционирования ИР, а также организационных и технических мер по защите информации, принимаемых владельцем ИР.

# Изучение исходных данных

Указанная информация может быть получена как при изучении нормативных и методических материалов и документации (при их наличии у владельца ИР), так и в ходе бесед с лицами, ответственными за эксплуатацию и обеспечение безопасности исследуемого ИР.

# Изучение исходных данных

Полученная информация должна учитываться при формировании перечня мероприятий, проводимых на этапе определения возможностей злоумышленника по проведению КА, а также при формулировании угроз безопасности информации, актуальных для исследуемого ИР.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

Данный этап предусматривает выполнение следующего комплекса мероприятий: выявление уязвимостей элементов исследуемого ИР; анализ конфигураций ТКО, осуществляющего маршрутизацию и фильтрацию сетевого трафика, циркулирующего в исследуемом ИР; исследование вопросов обеспечения безопасности информации, обрабатываемой с использованием веб-технологий; исследование вопросов обеспечения безопасности информации при использовании в ИР технологий беспроводной передачи данных.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

Выявление уязвимостей элементов исследуемого ИР.

В ходе работ по данному пункту выполняются (в том числе с применением САЗ) следующие мероприятия: выбор точек подключения и настройка САЗ1 ; выбор для исследования элементов ИР2 ; сканирование сетевых портов элементов ИР с целью выявления работающих сервисов; определение версий обнаруженных сервисов; выявление известных уязвимостей элементов ИР.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

В ходе проведения исследований необходимо учитывать требования к непрерывности функционирования ИР. Проведение тестирования на предмет наличия уязвимостей с использованием всех доступных тестов, содержащихся в базе знаний САЗ, может вызвать перебои в работе исследуемых элементов ИР. В случае высокого уровня критичности исследуемых элементов ИР следует отключать тесты, направленные на выявление уязвимостей элементов ИР к КА типа «отказ в обслуживании».

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

В случае необходимости проведения тестирования, направленного на выявление уязвимостей к КА типа «отказ в обслуживании», указанное тестирование целесообразно проводить на тестовых стендах (при их наличии) или во время технологических перерывов, когда нарушение штатного режима функционирования элементов ИР не будет иметь негативных последствий.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

Анализ конфигураций ТКО, осуществляющего маршрутизацию и фильтрацию сетевого трафика, циркулирующего в исследуемом ИР.

В ходе работ по данному пункту проводятся (методом анализа конфигурационных файлов исследуемого ТКО) следующие мероприятия:

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

анализ конфигураций ТКО на предмет присутствия небезопасных параметров удаленного доступа и хранения аутентификационных данных; проверка соответствия правил фильтрации и маршрутизации трафика, заданных на ТКО, требованиям документов, регламентирующих вопросы разграничения сетевого доступа;

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

анализ конфигураций ТКО на предмет использования функций защиты от КА, направленных на перехват сетевого трафика, циркулирующего в исследуемом ИР (в случае поддержки ТКО указанных функций).

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

Исследование вопросов обеспечения безопасности информации, обрабатываемой с использованием веб-технологий.

В ходе работ по данному пункту осуществляется исследование возможностей злоумышленника по воздействию на элементы ИР, использующие для обработки информации веб-технологии. При этом выполняются (вручную или с использованием САЗ) следующие мероприятия:

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

сбор информации о веб-приложении; проверка возможности получения расширенной информации о вебприложении («раскрытие информации о веб-приложении»); проверка механизмов обработки веб-приложением входных данных; проверка механизмов аутентификации пользователей вебприложения. В рамках сбора информации о веб-приложении осуществляется сбор информации об элементах, входящих в состав веб-приложения, на основании которой строятся все последующие проверки.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

В эти данные входят: ссылочная структура веб-приложения; структура каталогов; множество точек «входа» веб-приложения.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

В рамках проверки механизмов аутентификации пользователей вебприложения осуществляется оценка их безопасности. К основным недостаткам указанных механизмов, влияющим на безопасность информации, относятся: передача аутентификационных данных без использования средств криптографической защиты; отсутствие механизмов защиты от попыток подбора актуальных аутентификационных данных (CAPTCHA, блокировка пользователя после нескольких попыток неудачного перебора и т.п.).

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

Исследование вопросов обеспечения безопасности информации при использовании в ИР технологий беспроводной передачи данных.

В ходе работ по данному пункту осуществляется анализ фактического состояния дел в области защиты информации, передаваемой с использованием технологий беспроводной передачи данных.

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

При этом проводятся (с использованием программных или программноаппаратных комплексов, предназначенных для выявления признаков использования в ИР технологий беспроводной передачи данных) следующие мероприятия: поиск и обнаружение сигналов устройств беспроводной передачи данных; определение возможного местоположения устройств беспроводной передачи данных;

## Определение возможностей злоумышленника по проведению КА на исследуемый ИР

определение границ зоны покрытия беспроводных сегментов ИР и мест выхода зоны покрытия за пределы контролируемой зоны владельца ИР; оценка возможности злоумышленника по несанкционированному подключению к беспроводным сетям передачи данных, получению доступа и осуществлению воздействий на ИР; оценка возможностей злоумышленника по несанкционированному подключению к клиентским устройствам, функционирующим на территории владельца ИР.

# Подготовка отчетной документации

В общем случае отчетные материалы должны содержать: описание предмета МОЗ; результаты МОЗ; заключение.

# Список использованных источников

1. Методические документы // ГОССОПКА URL: https://gossopka.ru/doc/method/ (дата обращения: 06.10.2025).