



**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по проведению мероприятий по оценке степени защищенности от
компьютерных атак

СОДЕРЖАНИЕ

1. Термины и определения	3
2. Обозначения и сокращения.....	4
3. Общие положения	4
4. Порядок проведения МОЗ.....	5
5. Этапы проведения МОЗ.....	5
5.1. Изучение исходных данных.....	5
5.2. Определение возможностей злоумышленника по проведению КА на исследуемый ИР	6
5.2.1. Выявление уязвимостей элементов исследуемого ИР.....	6
5.2.2. Анализ конфигураций ТКО, осуществляющего маршрутизацию и фильтрацию сетевого трафика, циркулирующего в исследуемом ИР	8
5.2.3. Исследование вопросов обеспечения безопасности информации, обрабатываемой с использованием веб-технологий	8
5.2.4. Исследование вопросов обеспечения безопасности информации при использовании в ИР технологий беспроводной передачи данных	10
5.3. Подготовка отчетной документации.....	10

1. Термины и определения

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Информационные ресурсы Российской Федерации (далее по тексту – информационные ресурсы) – информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

Владельцы информационных ресурсов – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные ресурсы.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой им информации.

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования информационного ресурса и (или) нарушения безопасности обрабатываемой им информации, в том числе произошедший в результате компьютерной атаки.

Элементы информационного ресурса – составляющие комплекса программно-аппаратных средств информационного ресурса (серверы, рабочие станции пользователей, телекоммуникационное оборудование и т.д.).

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уязвимость – недостаток программной составляющей элемента информационного ресурса, который может использоваться для реализации угроз безопасности информации.

Средство анализа защищенности – программное или программно-аппаратное средство, предназначенное для выявления уязвимостей элементов информационного ресурса.

2. Обозначения и сокращения

ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

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.

3. Общие положения

Настоящие «Методические рекомендации...» разработаны в соответствии с п.п. в) п. 3 Указа Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и предназначены для использования силами ГосСОПКА.

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

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.

4. Порядок проведения МОЗ

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

Внеплановые МОЗ рекомендуется проводить в следующих случаях:

- 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;
- 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.

5. Этапы проведения МОЗ

МОЗ включают в себя следующие этапы:

- изучение исходных данных;
- определение возможностей злоумышленника по проведению КА на исследуемый ИР;
- подготовка отчетной документации.

5.1. 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.

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.

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.

5.2. 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.

Указанный перечень мероприятий может быть расширен (сокращен) по результатам изучения исходных данных исходя из архитектурных особенностей исследуемого ИР. Также допускается сократить указанный перечень мероприятий в случае проведения повторных МОЗ, например, с целью оценки эффективности мер, принятых владельцем ИР и направленных на устранение ранее выявленных недостатков.

5.2.1. 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.

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». В случае необходимости проведения тестирования, направленного на выявление уязвимостей к КА типа «отказ в обслуживании», указанное тестирование целесообразно проводить на тестовых стендах³ (при их наличии) или во время технологических перерывов, когда нарушение штатного режима функционирования элементов ИР не будет иметь негативных последствий.

При исследовании элементов автоматизированных систем управления, к которым предъявляются требования по недопущению нарушения их штатного режима функционирования, целесообразно отказаться от применения САЗ. В данном случае поиск известных уязвимостей элементов автоматизированных систем управления следует осуществлять по версиям используемого на них программного обеспечения в специализированных информационных базах

¹ Если исследуемый ИР состоит из нескольких сегментов, сетевое взаимодействие между которыми ограничено, или имеет сопряжение с внешними по отношению к нему ИР или сетью Интернет, используется несколько точек подключения. Выбор точек подключения и конфигурационных параметров САЗ должны обеспечивать максимальную полноту анализа возможностей предполагаемого злоумышленника по влиянию на исследуемый ИР.

² Для получения достоверных сведений об уровне защищенности ИР необходимо исследовать максимально возможное количество его элементов, доступных из каждой точки подключения.

³ Идентичных элементам исследуемого ИР.

данных⁴. Применение САЗ допустимо только на тестовых стендах⁵ (при их наличии) или во время технологических перерывов, когда нарушение штатного режима функционирования автоматизированных систем управления не будет иметь негативных последствий.

При наличии сопряжения автоматизированных систем управления с другими сегментами ИР или внешними по отношению к ним ИР допустимо использование САЗ в отношении оборудования, установленного на их границе.

5.2.2. 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:

- 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 доступа⁶;
- 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).

5.2.3. 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:

⁴ База данных Common Vulnerabilities and Exposures (CVE), бюллетени по безопасности Microsoft Security Bulletins (MS), база данных уязвимостей ФСТЭК России (BDU) и т.д.

⁵ Идентичных элементам исследуемых автоматизированных систем управления.

⁶ В случае отсутствия документов, регламентирующих вопросы разграничения сетевого доступа, при анализе конфигураций ТКО следует руководствоваться принципом предоставления минимально достаточного доступа, а также правилом «все, что не разрешено, то запрещено».

- сбор информации о веб-приложении;
- проверка возможности получения расширенной информации о веб-приложении («раскрытие информации о веб-приложении»);
- проверка механизмов обработки веб-приложением входных данных;
- проверка механизмов аутентификации пользователей веб-приложения.

В рамках сбора информации о веб-приложении осуществляется сбор информации об элементах, входящих в состав веб-приложения, на основании которой строятся все последующие проверки. В эти данные входят:

- ссылочная структура веб-приложения;
- структура каталогов;
- множество точек «входа» веб-приложения.

В рамках проверки возможности получения расширенной информации о веб-приложении осуществляются попытки поиска информации о наличии файлов на веб-сервере, которые недоступны при навигации по веб-ресурсу, комментариев разработчиков, сообщений об ошибках, а также другой информации, которая может быть использована для проведения КА в отношении исследуемого элемента ИР.

В рамках проверки механизмов обработки входных данных веб-приложения для всех точек «входа» проводится оценка возможности проведения КА, направленных на средства динамического формирования HTML-страниц.

В рамках проверки механизмов аутентификации пользователей веб-приложения 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 (САРТСНА, блокировка пользователя после

нескольких попыток неудачного перебора и т.п.).

5.2.4. 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.

При этом проводятся (с использованием программных или программно-аппаратных 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 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.

5.3. Подготовка отчетной документации

По результатам МОЗ проводится итоговый анализ полученных данных и подготавливаются отчетные материалы.

В общем случае отчетные материалы должны содержать:

- описание предмета МОЗ;
- результаты МОЗ;
- заключение.

Описание предмета МОЗ составляется по результатам анализа исходных

данных об исследуемом ИР и включает:

- сведения о владельце ИР;
- сведения об ИР. При этом должны быть отражены:
 - назначение ИР;
 - структура и принципы функционирования ИР;
 - порядок обработки информации;
 - порядок обмена данными с внешними (по отношению к исследуемому) ИР;
 - порядок администрирования ИР;
 - описание применяемых мер по защите информации;
 - наличие организационно-распорядительной документации в области обеспечения ИБ⁷;
- другие сведения, полученные в ходе проведения МОЗ, характеризующие порядок эксплуатации ИР и меры по обеспечению его ИБ.

Результаты МОЗ должны отражать полный перечень мероприятий, проведенных в рамках работ, направленных на определение возможностей злоумышленника по проведению КА на исследуемый ИР, с указанием их качественных результатов, а также краткое описание технических средств, использованных при проведении указанных мероприятий.

Заключение должно содержать:

- выводы о состоянии защищенности исследованного ИР;
- перечень выявленных недостатков в области обеспечения ИБ и обусловленных ими угроз безопасности информации;
- возможные сценарии действий злоумышленника (с учетом типа злоумышленника и уровня его квалификации, а также применяемых владельцем ИР организационных и технических мер по защите информации);
- рекомендации по устранению выявленных недостатков в области обеспечения ИБ.

⁷ Перечень документов целесообразно оформить в виде приложения к отчету.