МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

ПРИКАЗ

Карачаевск

«03» 06 2025 г. №193-ОС

Об утверждении регламента по выявлению анализу и устранению критичных уязвимостей в информационных системах

В целях усиления обеспечения безопасности информации и повышения защищенности информационных систем в федеральном государственном бюджетном образовательном учреждении высшего образования «Карачаево-Черкесский государственный университет имени У.Д. Алиева», в соответствии с методическими документами ФСТЭК России

п р и к а з ы в а ю :

1. Утвердить регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в КЧГУ (Приложение №1).

2. Контроль за исполнением настоящего постановления оставляю за собой.

И. о. ректора Т.А. Узденов

Приложение №1 к
Приказу № 193-ОС
От 03 06 2025г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Карачаево-Черкесский государственный университет имени У.Д. Алиева»
(КЧГУ)

Утверждаю
И.о. ректора КЧГУ
_____ Т.А. Узденов
«03» 06 2025 г.

РЕГЛАМЕНТ ПРОЦЕССОВ ПО ВЫЯВЛЕНИЮ, АНАЛИЗУ И УСТРАНЕНИЮ КРИТИЧНЫХ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЭКСПЛУАТИРУЕМЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах (далее - ИС) эксплуатируемых в организации (далее - Регламент) разработан в соответствии с Руководством по организации процесса управления уязвимостями в организации утвержденным ФСТЭК России от 17 мая 2023 г. и в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств утвержденной ФСТЭК России от 28 октября 2022 г.

1.2. Настоящий Регламент подлежит применению операторами информационных систем при принятии ими мер по выявлению, анализа и устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных ИС, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.

1.3. Выявление, анализ и устранение уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации обеспечивается в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

1.4. В Регламенте используются термины и определения, установленные национальными стандартами ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей», ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» и иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

Целями регламента являются:

- выявление, анализ и устранение критичных уязвимостей в ИС;

- создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования информационных систем;

- организация взаимодействия между структурными подразделениями организации по вопросам устранения уязвимостей.

2. ПОРЯДОК ВЫЯВЛЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2.1. В ИС должно осуществляться выявление следующих типов уязвимостей:

- недостатки и (или) ошибки программного обеспечения (далее ПО) ИС и ее системы защиты информации (далее - СЗИ).

- недостатки аппаратных средств ИС, в том числе аппаратных средств защиты информации.

- организационно-технические недостатки.

2.2. Непосредственными исполнителями мероприятий по выявлению, анализу и устранению уязвимостей ИС являются администратор безопасности и (или) системные администраторы ИС.

На этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников и принятие решений по их последующей обработке.

Процесс управления уязвимостями организуется для всех ИС организации и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и объектах ИС. При изменении статуса уязвимостей (применимость к ИС, наличие исправлений, критичность) должны корректироваться способы их устранения.

Процесс управления уязвимостями связан с другими процессами и процедурами деятельности организации:

- мониторинг информационной безопасности - процесс регулярного наблюдения и анализа результатов регистрации событий безопасности и иных

данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей;

- оценка защищенности - анализ возможности использования обнаруженных уязвимостей для реализации компьютерных атак на ИС организации;

- оценка угроз безопасности информации - выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в ИС организации;

- управление конфигурацией - контроль изменений, состава и настроек программного и программно-аппаратного обеспечения ИС;

- управление обновлениями - приобретение, анализ и развертывание обновлений программного обеспечения в организации;

- применение компенсирующих мер защиты информации - разработка и применение мер защиты информации, которые применяются в ИС взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их применения.

Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения администраторами безопасности о необходимости устранения уязвимостей, выявленных в программных, программно-аппаратных средствах по результатам анализа уязвимостей в ИС.

Исходными данными для определения критичности уязвимостей являются:

- база уязвимостей программного обеспечения, программно-аппаратных средств, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также иные источники, содержащие сведения об известных уязвимостях;

- официальные информационные ресурсы разработчиков программного обеспечения, программно-аппаратных средств и исследователей в области информационной безопасности;

- сведения о составе и архитектуре информационных систем,

полученные по результатам их инвентаризации и (или) приведенные в документации на информационные системы;

результаты контроля защищенности информационных систем, проведенные оператором с использованием модулей комплексного программного обеспечения Kaspersky Endpoint Security (таблица №2.2.1), в соответствии с «Регламент сканирования информационной инфраструктуры на предмет уязвимостей» (Приложение №1).

Таблица №2.2.1

№	Модуль	Описание и функции
1	**Защита от файловых угроз**	Обнаружение и блокировка вирусов, троянов, червей и других типов угроз. Автоматическое сканирование файлов при их открытии, копировании или создании. Использование облачных технологий Kaspersky Security Network для повышения точности обнаружения. Настройка уровней проверки (быстрая, полная, пользовательская). Управление карантином для изолированных угроз.
2	**Защита от веб-угроз**	Блокировка вредоносных ссылок и сайтов. Предупреждение о попытках загрузки опасных файлов. Интеграция с базами данных Kaspersky URL Advisor для категоризации сайтов. Настройка уровня контроля (высокий, средний, низкий). Добавление доверенных сайтов в исключения.
3	**Защита от почтовых угроз**	Сканирование входящих и исходящих электронных писем на наличие вредоносного содержимого. Блокировка спама и фишинговых писем. Поддержка популярных почтовых клиентов (например, Microsoft Outlook, Mozilla Thunderbird). Настройка правил для фильтрации нежелательной почты. Исключение определенных адресов из проверки.
4	**Защита от сетевых угроз**	Блокировка подозрительного сетевого трафика. Отслеживание попыток несанкционированного доступа. Настройка правил для блокировки IP-адресов. Фильтрация трафика по портам и протоколам.
5	**Сетевой экран**	Контроль входящего и исходящего сетевого трафика. Блокировка подозрительных соединений. Настройка правил для разрешения/запрещения конкретных портов и протоколов. Логирование сетевых событий.
6	**AMSI-защита**	Защита от атак, использующих механизм скриптов Windows (Windows Script Host). Обнаружение и блокировка подозрительных скриптов. Настройка политик для управления AMIS-защитой.
7	**Kaspersky Security Network**	Облачная платформа для анализа угроз и предоставления актуальных данных о безопасности. Реализация коллективного интеллекта для быстрого обнаружения новых угроз. Автоматическая передача информации о подозрительных файлах в облако. Модуль обеспечивает глобальный обмен данными о угрозах между всеми клиентами Kaspersky, что позволяет быстро реагировать на новые угрозы.

8	**Анализ поведения**	Мониторинг активности процессов и программ на устройстве. Обнаружение подозрительных действий, таких как изменение системных файлов или запуск необычных процессов. Настройка правил для различных типов поведения. Логирование результатов анализа. Модуль защиты от неизвестных (zero-day) угроз, основывается на анализе активности, а не только на сигнатурах вирусов.
9	**Защита от эксплоитов**	Обнаружение и блокировка попыток эксплуатации уязвимостей в программах. Защита критически важных процессов и системных файлов. Настройка уровня чувствительности. Возможность исключения определенных процессов из мониторинга.
10	**Предотвращение вторжений**	Защита от атак, направленных на получение несанкционированного доступа к системе. Блокировка подозрительных действий, таких как попытки взлома учетных записей или выполнения команд. Настройка политик безопасности для предотвращения вторжений. Логирование попыток вторжения. Модуль используется для защиты корпоративных систем от целевых атак, где злоумышленники пытаются получить доступ к конфиденциальной информации.
11	**Откат вредоносных действий**	Автоматическое восстановление системы после обнаружения вредоносной активности. Восстановление файлов и системных настроек до состояния до атаки. Настройка условий для автоматического отката. Логирование операций отката.
12	**Контроль приложений**	Ограничение использования программ на устройстве. Блокировка запуска нежелательных или потенциально опасных приложений. Создание "белого списка" доверенных программ. Отслеживание активности приложений. Назначение прав доступа для групп пользователей. Логирование действий приложений.
13	**Контроль устройств**	Управление подключением внешних устройств (USB-накопителей, принтеров, смартфонов и т.д.). Блокировка или ограничение использования USB-устройств. Разрешение доступа только для авторизованных устройств. Защита от утечки данных через внешние носители. Настройка политик для разных типов устройств. Возможность задания временных ограничений.
14	**Веб-контроль**	Контроль интернет-активности пользователей. Блокировка доступа к сайтам с запрещенным контентом (например, игры, мошенничество). Настройка категорий заблокированных сайтов. Добавление доверенных сайтов в исключения. Логирование посещаемых страниц.
15	**Адаптивный контроль аномалий**	Динамический анализ поведения системы и пользователей. Обнаружение нехарактерных для устройства или пользователя действий. Настройка политик для различных типов аномалий. Логирование результатов анализа.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют ИС.

Оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится администраторами безопасности информационных систем.

Оценка уровня критичности уязвимостей программных, программно-аппаратных средств применительно к конкретной ИС включает:

- определение программных, программно-аппаратных средств, подверженных уязвимостям;

- определение в информационной системе места установки программных, программно-аппаратных средств, подверженных уязвимостям (например, на периметре системы, во внутреннем сегменте системы, при реализации критических процессов (деловых процессов) и других сегментах ИС);

- расчет уровня критичности уязвимости программных, программно-аппаратных средств в ИС.

3. ПОРЯДОК АНАЛИЗА КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

На этапе анализа уязвимостей определяется уровень критичности уязвимостей применительно к ИС и осуществляется выявление уязвимостей на основании данных из следующих источников:

а) внутренние источники:

- системы управления информационной инфраструктурой (далее - ИТ - инфраструктура);

- базы данных управления конфигурациями;

- документация на ИС;

- электронные базы;

б) база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации (далее - БДУ) ФСТЭК России;

в) внешние источники:

- базы данных, содержащие сведения об известных уязвимостях;

- официальные информационные ресурсы разработчиков программных и программно-аппаратных средств и исследователей в области информационной безопасности.

Источники данных могут уточняться или дополняться с учетом

особенностей функционирования информационных систем.

На этапе анализа уязвимостей и оценки их применимости выполняются операции, приведенные в таблице 3.1.

Таблица 3.1

Наименование операции	**Описание операции**
Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам органа (организации). Агрегирование и корреляция собираемых данных об уязвимостях
Оценка применимости уязвимости	На основе информации об объектах информационных систем и их состоянии определяется применимость уязвимости к информационным системам органа (организации) с целью определения уязвимостей, не требующих дальнейшей обработки (не релевантных уязвимостей). Оценка применимости уязвимостей производится: на основе анализа данных об ИТ-инфраструктуре, полученных из баз данных управления конфигурациями в рамках процесса «Управление конфигурацией»; на основе анализа данных о возможных объектах воздействия, полученных в результате моделирования угроз в рамках процесса «Оценка угроз»; по результатам оценки защищенности
Принятие решений на получение дополнительной информации	Запрос дополнительной информации об уязвимости (сканирование объектов, оценка защищенности), если имеющихся данных недостаточно для принятия решений по управлению уязвимостями
Постановка задачи на сканирование объектов	Запрос на внеплановое сканирование объектов информационных систем в случае недостаточности либо неактуальности имеющихся данных, а также в случае получения информации об уязвимости после последнего сканирования
Сканирование объектов	Поиск уязвимостей и недостатков с помощью автоматизированных систем анализа защищенности. Выбор объектов и времени сканирования, уведомление заинтересованных подразделений (например, ситуационного центра, подразделения ИТ) о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационным системам. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах органа (организации) с использованием средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации)

На основе таблицы 3.1. в должно разрабатываться детальное описание

операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные. Детальное описание операций включается в организационно-распорядительные документы по защите информации организации.

4. ПОРЯДОК УСТРАНЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

4.1. На этапе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации, также принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

На этапе определения методов и приоритетов устранения уязвимостей решаются задачи:

- определения приоритетности устранения уязвимостей;
- выбора методов устранения уязвимостей:
- обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

На этапе определения методов и приоритетов устранения уязвимостей выполняются операции, приведенные в таблице 4.1.

Таблица 4.1

Наименование операции	Описание операции
Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей (этап 4)
Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации
Принятие решения о срочной установке обновлений	При обнаружении критической уязвимости может быть принято решение о срочной установке обновления программного обеспечения объектов информационных систем, подверженных уязвимости
Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование руководителю подразделения ИТ

Принятие решения о срочной реализации компенсирующих мер защиты информации	При обнаружении критической уязвимости может быть принято решение о срочной реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления

На основе таблицы 4.1. должно разрабатываться детальное описание операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные. Детальное описание операций включается в организационно-распорядительные документы по защите информации в информационной системе.

4.2. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга. При этом выполняются операции, представленные в таблице 4.2.

Таблица 4.2

Наименование операции	**Описание операции**
Согласование установки с руководством подразделения ИТ	Срочная установка обновлений программного обеспечения предварительно согласовывается с руководством подразделения ИТ
Тестирование обновления	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее - недекларированные возможности)
Установка обновления в тестовом сегменте	Установка обновлений на выбранном тестовом сегменте информационной системы в целях определения влияния их установки на ее функционирование
Принятие решения об установке обновления	В случае, если негативного влияния от установки обновления на выбранном сегменте системы не выявлено, принимается решение о его распространении в системе. В случае обнаружения негативного влияния от установки обновления на выбранном сегменте системы дальнейшее распространение обновления не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации
Установка обновления	Распространение обновления на объекты информационных систем
Формирование плана установки обновлений	Уязвимости, для устранения которых не была определена необходимость срочной установки обновлений, устраняются в ходе плановой установки обновлений. Формирование плана обновлений осуществляется с учетом заявок на установку обновлений

Разработка и реализация компенсирующих мер защиты информации	Разработка и применение мер защиты информации, которые применяются в информационных системах взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их установки, обнаружением негативного влияния от установки обновления, а также в случае необходимости принятия мер до устранения уязвимости. К компенсирующим мерам защиты информации могут относиться: организационные меры защиты информации, настройка средств защиты информации, анализ событий безопасности, внесение изменений в ИТ- инфраструктуру

Тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с Регламентом по выявлению, анализу и устранению критичных уязвимостей в эксплуатируемых ИС, по решению организации в случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России.

При наличии соответствующих сведений могут быть использованы компенсирующие меры защиты информации, представленные в бюллетенях безопасности разработчиков программных, программно-аппаратных средств, а также в описаниях уязвимостей, опубликованных в БДУ ФСТЭК России.

Рекомендуемые сроки устранения уязвимостей:

- критический уровень опасности до 24 часов;
- высокий уровень опасности - до 7 дней;
- средний уровень опасности - до 4 недель;
- низкий уровень опасности - до 4 месяцев.

В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации выполняются операции, приведенные в таблице 4.3.

Таблица 4.3

Наименование операции	Описание операции
Определение мер защиты информации и ответственных за их реализацию	Определение компенсирующих мер защиты информации, необходимых для нейтрализации уязвимости либо снижения возможных негативных последствий от ее эксплуатации. В ходе выполнения данной операции должны быть определены работники, участие которых необходимо для реализации выбранных компенсирующих мер защиты информации

Согласование привлечения работников	В случае необходимости привлечения работников других подразделений для реализации компенсирующих мер защиты информации руководитель подразделения защиты согласует их привлечение с руководителями соответствующих подразделений
Реализация организационных мер защиты информации	Реализация организационных мер защиты информации предусматривает: ограничение использования ИТ-инфраструктуры; организация режима охраны (в частности, ограничение доступа к техническим средствам); информирование и обучение персонала органа (организации)
Настройка средств защиты информации	Оценка возможности реализации компенсирующих мер с использованием средств защиты информации, выбор средств защиты информации (при необходимости). Выполнение работ по настройке средств защиты информации
Организация анализа событий безопасности	Организация постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления и блокирования попыток эксплуатации уязвимости
Внесение изменений в ИТ-инфраструктуру	Внесение изменений в ИТ-инфраструктуру включает действия по внесению изменений в конфигурации программных и программно-аппаратных средств (в том числе, удаление (выведение из эксплуатации))

На основе таблиц 4.2 и 4.3. должно разрабатываться детальное описание операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные.

Детальное описание операций включается в организационно-распорядительные документы по защите информации в организации.

В случае невозможности получения, установки и тестирования обновлений программных, программно-аппаратных средств принимаются компенсирующие меры защиты информации.

Выбор компенсирующих мер по защите информации осуществляется оператором с учетом архитектуры и особенностей функционирования ИС, а также способов эксплуатации уязвимостей программных, программно-аппаратных средств.

Компенсирующими организационными и техническими мерами, направленными на предотвращение возможности эксплуатации уязвимостей, могут являться:

- изменение конфигурации уязвимых компонентов ИС, в том числе в части предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;

- ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей (например, отключение уязвимых служб и сетевых протоколов);

- установка дополнительных средств защиты как программных так программно-аппаратных;

- резервирование компонентов ИС, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

- использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление в ИС признаков эксплуатации уязвимостей;

- мониторинг информационной безопасности и выявление событий безопасности информации в ИС, связанных с возможностью эксплуатации уязвимостей.

Приложение №1

Регламент сканирования информационной инфраструктуры на предмет уязвимостей

1. Общие положения

1.1. Настоящий регламент регулирует порядок проведения сканирования информационной инфраструктуры для выявления уязвимостей, включая критические.

1.2. Цели:

- Обеспечение соответствия требованиям ФСТЭК России (Руководство от 17.05.2023).
- Снижение рисков нарушения конфиденциальности, целостности и доступности информации.

1.3. Область применения: все информационные системы, серверы, рабочие станции, сетевые устройства и ПО организации.

2. Ответственные лица

2.1. **Ответственный за обеспечение информационной безопасности в организации**:

- Организует процесс сканирования.
- Контролирует устранение уязвимостей.
- Формирует итоговые отчеты.

2.2. **Центр информационных технологий**:

- Проводит техническое сканирование.
- Внедряет меры по устранению уязвимостей.

2.3. **Руководители подразделений**:

- Обеспечивают доступ к инфраструктуре для сканирования.

3. Периодичность и методы сканирования

3.1. **Периодичность**:

- Полное сканирование инфраструктуры: **ежемесячно в автоматическом порядке**.
- Проверка критических систем (серверы, БД): **еженедельно в автоматическом порядке**.
- Внеплановое сканирование: при изменении конфигурации сети/ПО или после инцидентов.

3.2. **Инструменты**:

- Kaspersky Endpoint Security (с актуальными базами уязвимостей) в соответствии с пунктом 2.2 «Регламента процессов по выявлению, анализу и устранению критичных уязвимостей в информационных системах эксплуатируемых в КЧГУ имени У.Д. Алиева».
- Ручная проверка конфигураций (по чек-листам ФСТЭК).

4. Процедура проведения сканирования

4.1. **Подготовка**:

- Утверждение графика сканирования (в соответствии с пунктом 3.1).
- Уведомление подразделений о времени проведения работ.
- Резервное копирование критических систем (при необходимости).

4.2. **Выполнение**:

- Запуск автоматизированных инструментов.
- Фиксация результатов в **Журнале сканирования** (Таблица №1.1) и **Форме плана устранения** (Таблица №1.2).

4.3. **Ограничения**:

- Сканирование вне рабочих часов для минимизации нагрузки.
- Запрет на использование агрессивных методов (например, нагрузочное тестирование).

5. Обработка результатов

5.1. **Классификация уязвимостей**:

- **Критическая** (CVSS ≥ 9.0): Устранение в течение **24 часов**.
- **Высокая** (CVSS 7.0–8.9): Устранение в течение **72 часов**.
- **Средняя/Низкая** (CVSS < 7.0): Устранение в плановом порядке (до 14 дней).

5.2. **Действия при критических уязвимостях**:

- Изоляция системы от сети.
- Немедленное уведомление ответственного за ИБ.
- Внесение данных в **Акт о критической уязвимости** (Таблица №2).

6. Отчётность

6.1. **Отчёт о сканировании** (формируется в течение 3 рабочих дней, при выявлении уязвимостей):

- Перечень выявленных уязвимостей.
- Рекомендации по устранению.
- Сроки выполнения (Таблица №3).

6.2. **Итоговый отчёт**:

- Предоставляется руководству ежеквартально.
- Содержит статистику, динамику устранения уязвимостей и план улучшений.

Таблица №1.1. Журнал сканирования

Дата	Объект	Тип уязвимости	Уровень риска	Ответственный за устранение	Срок	Статус
02.04.2024	Сервер БД	CVE-2024-1234 (SQLi)	Критический	Сидоров П.К.	04.04.2025	Устранено

Таблица №1.2. Форма плана устранения

Уязвимость	Срок устранения	Ответственный	Статус	Примечания
CVE-2024-1234 (SQLi)	04.04.2025	Сидоров П.К.	Выполнено	Патч применён

Таблица №2. Акт о критической уязвимости

Акт № ___ от «___» _____ 202_ г.

1. Объект: [название информационной системы].
2. Описание уязвимости: [CVE-ID, CVSS-оценка, краткое описание].
3. Принятые меры:
   - Изоляция системы: Да/Нет.
   - Временные решения: [например, блокировка порта].
4. Срок полного устранения: _____.
5. Подписи:
   - Ответственный за ИБ: _____
   - Администратор безопасности: _____

Таблица №3. Отчёт о сканировании

Отчёт № ___ от «___» _____ 202_ г.

1. Объект проверки: [название информационной системы].
2. Количество выявленных уязвимостей:
   - Критических: ___
   - Высоких: ___
   - Средних/Низких: ___
3. Рекомендации:
   - Установить патч/обновление для CVE-2024-5678.
   - Обновить правила межсетевого экрана.
4. Подпись ответственного за ИБ: _____

Примечания:

- Все журналы и отчёты хранятся в течение **3 лет**.
- Документы должны быть доступны для проверки регулирующих органов (Роскомнадзор, ФСТЭК).
- Изменения в регламент вносятся приказом руководителя организации.