Глава Горьковского муниципального района Омской области

ПОСТАНОВЛЕНИЕ

от 29.07.2024 № 238

р.п. Горьковское

Об утверждении регламента «Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

В целях обеспечения безопасности сведений ограниченного доступа, не составляющих государственную тайну, и во исполнение руководящих документов ФСТЭК России, руководствуясь Уставом Горьковского муниципального района Омской области постановляю:

1. Утвердить прилагаемый регламент «Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области».
2. Управлению строительства и ЖКХ Администрации Горьковского муниципального района Омской области разместить настоящее постановление на официальном сайте Горьковского муниципального района Омской области в сети Интернет и на информационном стенде Администрации Горьковского муниципального района Омской области, расположенном по адресу: Омская область, Горьковский район, р.п. Горьковское, ул. Красный Путь, д. 2.
3. Контроль за исполнением настоящего постановления оставляю за собой.

Глава муниципального района М.Ю. Болтрик

Приложение
к постановлению Главы Горьковского
муниципального района Омской области
от 29.07.2024 г. № 238

РЕГЛАМЕНТ
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий регламент по управлению уязвимостями в Администрации Горьковского муниципального района Омской области (далее – Регламент) разработан в соответствии с методическим документом «Руководство по организации процесса управления уязвимостями в органе (организации)», утвержденном ФСТЭК России от 17.05.2023.

1.2. Регламент определяет состав и содержание работ по анализу и устранению уязвимостей (далее – управление уязвимостями), выявленных в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей (далее – информационные системы).

1.3. Управление уязвимостями сертифицированных программных, программно-аппаратных средств защиты информации обеспечивается с учетом эксплуатационной документации на них, а также рекомендаций разработчиков.

1.4. В Руководстве 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», ГОСТ Р 59547-2021 «Мониторинг информационной безопасности», ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» и иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

1.5. В Руководстве используются обозначения на схемах, приведенные в приложении №1 к настоящему документу.

2. ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

2.1. Процесс управления уязвимостями включает пять основных этапов (рисунок 2.1).

Рисунок 2.1. – Этапы работ по управлению уязвимостями

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.

На этапе оценки уязвимостей определяется уровень критичности уязвимостей применительно к информационным системам Администрации Горьковского муниципального района Омской области.

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.

На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса.

2.2. Процесс управления уязвимостями организуется для всех информационных систем Администрации Горьковского муниципального района Омской области и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и объектах информационной системы. При изменении статуса уязвимостей

(применимость к информационным системам, наличие исправлений, критичность) должны корректироваться способы их устранения.

2.3. Процесс управления уязвимостями связан с другими процессами и процедурами деятельности Администрации Горьковского муниципального района Омской области:

– мониторинг информационной безопасности – процесс постоянного 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 информационные системы Администрации Горьковского муниципального района Омской области;

– оценка угроз безопасности информации – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в информационных системах Администрации Горьковского муниципального района Омской области;

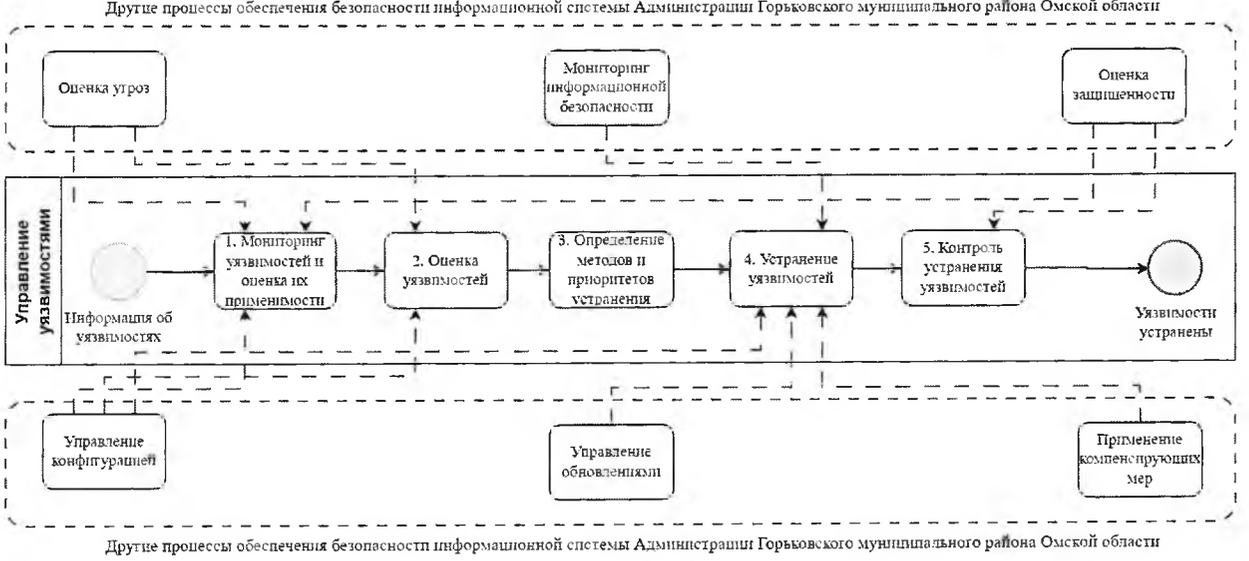
– управление конфигурацией – контроль изменений, состава и настроек программного и программно-аппаратного обеспечения информационных систем;

– управление обновлениями – приобретение, анализ и развертывание обновлений программного обеспечения в Администрации Горьковского муниципального района Омской области;

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

Схема процесса управления уязвимости предоставлена на рисунке 2.2.

Рисунок 2.2. – Схема процесса управления уязвимостями



2.4. Участниками процесса управления уязвимостями являются:

а) подразделение, осуществляющие функции по обеспечению информационной безопасности (далее – подразделение по защите):

– руководитель;

– специалист, ответственный за проведение оценки угроз безопасности информации (далее – аналитик угроз);

– специалист, ответственный за проведение оценки защищенности;

– специалист, ответственный за внедрение мер защиты информации;

б) подразделение, ответственное за внедрение информационных технологий (далее – подразделение ИТ):

– руководитель;

– специалист.

По решению Главы Администрации Горьковского муниципального района Омской области, в процессе управления уязвимостями, могут быть задействованы другие подразделения и специалисты, в частности, подразделение, ответственное за организацию закупок программных и программно-аппаратных средств, подразделение, ответственное за эксплуатацию инженерных систем.

Распределение операций, реализуемых в рамках процесса управления уязвимостями, по ролям работников подразделений ИТ и подразделения по защите Администрации Горьковского муниципального района Омской области, представлено в таблице 2.1[1].

Таблица 2.1

Операции	Подразделение по защите				Подразделение ИТ	
	Руководитель	Аналитик угроз	Специалист по проведению оценки защищенности	Специалист по внедрению мер защиты информации	Руководитель	Специалист
1	2	3	4	5	6	7
Мониторинг уязвимостей и оценка их применимости						
Анализ информации об уязвимостях	+ (О)	+ (И)				
Оценка применимости уязвимости	+ (О)	+ (И)				
Принятие решений на получение дополнительной		+ (ОИ)				

[1] Роли могут распределяться и (или) совмещаться в зависимости от укомплектованности подразделений

информации						
Постановка задачи на сканирование объектов	+ (ОИ)					
Сканирование объектов	+ (О)		+ (И)			
Оценка защищенности	+ (О)		+ (И)			
Оценка уязвимостей						
Получение информации об объектах, подверженных уязвимости		+ (ОИ)				
Определение уровня опасности		+ (ОИ)				
Определение влияния на информационные системы		+ (ОИ)				
Расчет критичности уязвимости	+ (О)	+ (И)				
Определение методов и приоритетов устранения уязвимостей						
Определение приоритетности устранения уязвимостей	+ (О)	+ (И)				
Определение методов устранения уязвимостей	+ (О)	+ (И)				
Принятие решения о срочной установке обновлений	+ (ОИ)					
Создание заявки на срочную установку обновления	+ (ОИ)					
Создание задания на установку обновлений		+ (ОИ)				
Принятие решения о срочной реализации компенсирующих мер защиты информации	+ (ОИ)					
Создание задания на реализацию		+ (О				

компенсирующих мер защиты информации		И)				
Устранение уязвимостей						
Согласование установки с руководством подразделения ИТ	+ (ОИ)				+ (У)	
Тестирование обновления					+ (О)	+ (И)
Установка обновления в тестовом сегменте					+ (О)	+ (И)
Принятие решения об установке обновления					+ (ОИ)	
Установка обновления					+ (О)	+ (И)
Формирование плана установки обновлений					+ (ОИ)	
Разработка и реализация компенсирующих мер защиты информации	+ (О)	+ (И)		+ (И)		+ (У)
Разработка и реализация компенсирующих мер защиты информации						
Определение мер защиты информации и ответственных за их реализацию	+ (О)	+ (И)				
Согласование привлечения работников	+ (ОИ)				+ (У)	
Реализация организационных мер защиты информации	+ (ОИ)				+ (У)	
Настройка средств защиты информации	+ (О)			+ (И)		+ (У)
Администрация Горьковского муниципального района Омской области анализа событий безопасности	+ (О)			+ (И)		
Внесение изменений в ИТ-инфраструктуру		+ (У)			+ (О)	+ (И)

Контроль устранения уязвимостей						
Принятие решения о способе контроля	+ (О И)					
Проверка объектов на наличие уязвимостей	+ (О)		+ (И)			
Оценка защищенности	+ (О)		+ (И)			
Выявление отклонений и неисполнений	+ (О)		+ (И)			
Разработка предложений по улучшению процесса управления уязвимостями	+ (О И)	+ (И)			+ (У)	
Разработка предложений по улучшению процесса управления уязвимостями						
Определение причин отклонений и (или) неисполнений	+ (О И)					
Корректировка механизмов мониторинга	+ (О)	+ (И)				
Добавление источника сведений об уязвимостях	+ (О)	+ (И)				
Корректировка механизмов оценки уязвимостей	+ (О)	+ (И)				
Согласование сроков устранения уязвимости	+ (О И)				+ (У)	
Создание заявки на срочную реализацию компенсирующих мер защиты информации	+ (О)	+ (И)				
Обозначения:						
О – Ответственный – работник, ответственный за завершение выполнения задачи;						
И – Исполнитель – работник, непосредственно выполняющий задачу;						
У – Участник – работник, участие которого требуется для выполнения задачи						

2.МОНИТОРИНГ УЯЗВИМОСТЕЙ И ОЦЕНКА ИХ ПРИМЕНИМОСТИ

2.5. На этапе мониторинга уязвимостей и оценки их применимости 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 информационные системы;

– электронные базы знаний Администрации Горьковского муниципального района Омской области;

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 Администрации Горьковского муниципального района Омской области.

2.6. Схема этапа мониторинга уязвимостей и оценки их применимости представлена на рисунке 3.1[2].

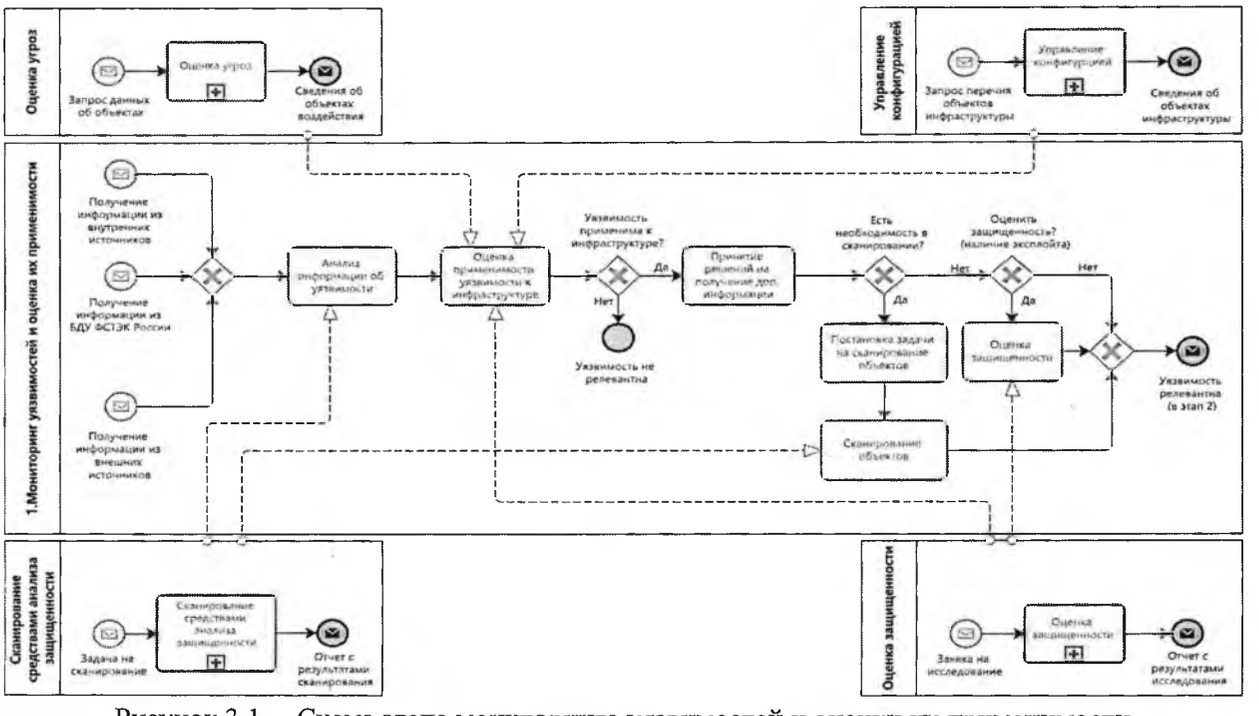


Рисунок 3.1. – Схема этапа мониторинга уязвимостей и оценки их применимости

[2] В настоящем Руководстве представлены типовые схемы этапов процесса устранения уязвимостей

2.7. Описание операций, выполняемых на этапе мониторинга уязвимостей и оценки их применимости, включающее наименование операций, описание операций, исполнителей операции, приведено в таблице 3.1.

Таблица 3.1

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
1.	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам Администрации Горьковского муниципального района Омской области. Агрегирование и корреляция собираемых данных об уязвимостях	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
2.	Оценка применимости уязвимости	На основе информации об объектах информационных систем и их состоянии определяется применимость уязвимости к информационным системам Администрации Горьковского муниципального района Омской области 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 (п. 6)	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
3.	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	Ответственный: - Аналитик угроз Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
4.	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	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Руководитель Подразделения ИБ
5.	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	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Специалист по проведению оценки защищенности

		сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости	Подразделения ИБ
6.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационных системах. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах Администрации Горьковского муниципального района Омской области с использованием PoC[3] или 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)	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Специалист по проведению оценки защищенности Подразделения ИБ

2.8. Анализ информации об уязвимостях, определенных в соответствии с таблицей 3.1, продолжительность, выходные данные и результат анализа оценки применимости уязвимости отражается в таблице 3.2.

Таблица 3.2

№ уязвимости	Название уязвимости	Источник информации об уязвимости	Анализ информации об уязвимости	Исполнители	Продолжительность	Оценка применимости уязвимости к инфраструктуре	Решение о применимости уязвимости к инфраструктуре (релевантности) (да/нет)	Принятие решений на получение дополнительной информации
1	2	3	4	5	6	7	8	9
								сканирование объектов
								оценка защищенности
								Не требуется

2.9. Для уязвимостей, в отношении которых в принято решение об их применимости к инфраструктуре, если имеющихся данных недостаточно для принятия решений по управлению уязвимостями, принимается решений на получение дополнительной информации (сканирование объектов, оценка защищенности).

2.10. Для уязвимостей, в отношении которых в принято решение о постановке задачи на сканирование объектов:

– руководителем подразделения ИБ утверждается заявка на сканирование, содержащая перечень выбранных объектов, их расположение и время сканирования (Приложение №3 к настоящему регламенту);

[3] PoC (англ. Proof of Concept, проверка концепции) – моделирование эксплуатации уязвимости

– уведомляются заинтересованные подразделения (например, функциональные отделы, подразделения ИТ) о проведении сканирования;

– проводится сканирование.

2.11. По результатам сканирования выбранных объектов на наличие уязвимости оформляется отчет, содержащий перечень уязвимостей с указанием их критичности.

2.12. Вывод о релевантности уязвимости по результатам сканирования отражается в таблице 3.3.

2.13. Для уязвимостей, в отношении которых в принято решение об оценке защищенности, выполняется экспертная оценка возможности применения уязвимости в информационных системах.

2.14. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах Администрации Горьковского муниципального района Омской области с использованием PoC или 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)

2.15. Результат оценки защищенности, включающей оценку возможности эксплуатации уязвимости в информационных системах Администрации Горьковского муниципального района Омской области, отражается в таблице 3.3.

Таблица 3.3

язви-мости	Назв ание уязвимости	Резуль тат сканирования объектов	Результат оценки защищенности при наличии эксплойтов	П родол-житель-ность работ	Вывод о релевантности уязвимости (да/нет)
	2	3	4	5	6

2.16. Вывод о релевантности уязвимости по результатам анализа полученной дополнительной информации, отражается в таблице 3.3.

2.17. По результатам мониторинга уязвимостей и оценки их применимости, формируется отчет по форме, представленной в Приложении №2 к настоящему регламенту, содержащий перечень выявленных уязвимостей и принятие решений по их последующей обработке.

3. ОЦЕНКА УЯЗВИМОСТЕЙ

3.1. Оценка уязвимостей производится с целью определения уровня критичности уязвимостей применительно к информационным системам Администрации Горьковского муниципального района Омской области.

3.2. Исходными (входящими) данными при оценке уязвимостей, является информация, полученная на этапе мониторинга уязвимостей и оценки их применимости.

3.3. Операции по определению уровня опасности уязвимости, ее влияния на информационные системы и расчету критичности уязвимости выполняются в соответствии с Методикой оценки уровня критичности уязвимостей программных и программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.

3.4. Схема этапа оценки уязвимостей представлена на рисунке 4.1.

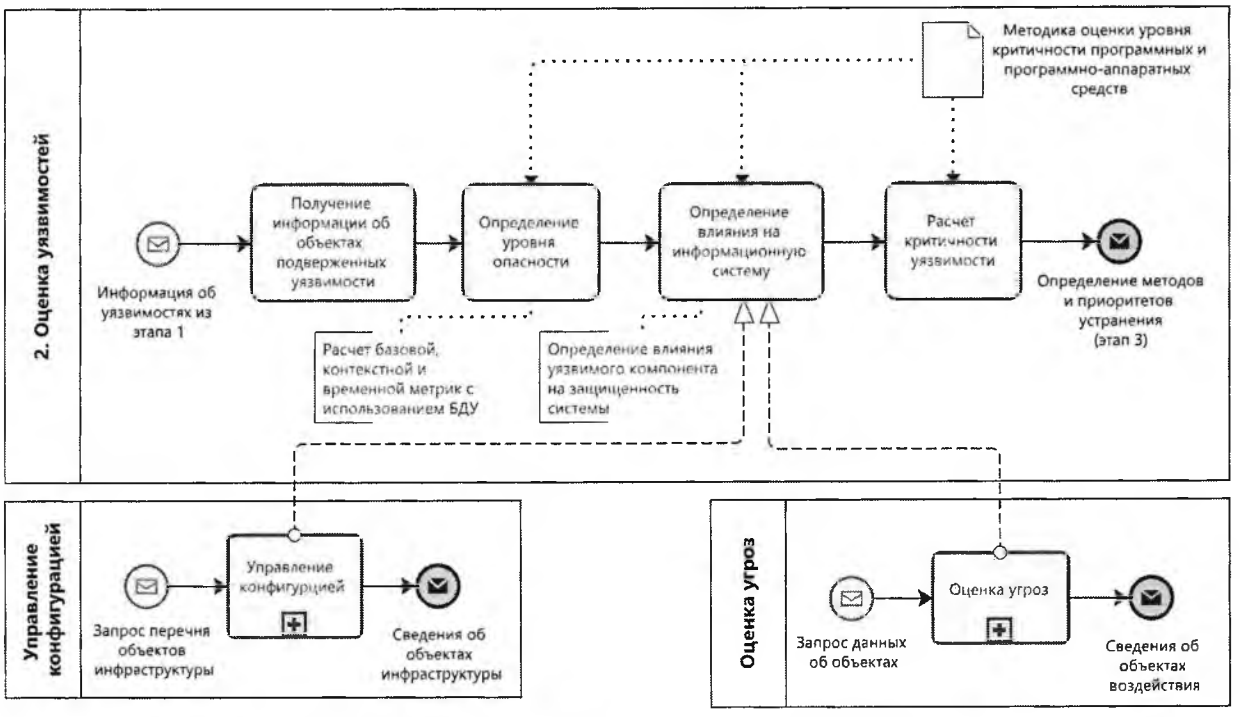


Рисунок 4.1. – Схема этапа оценки уязвимостей

3.5. Описание операций, выполняемых на этапе оценки уязвимостей, включающее наименование операций, описание операций, исполнителей операции, приведено в таблице 4.1.

Таблица 4.1.

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
	Получение информации об объектах, подверженных уязвимости	Получение выборки объектов информационных систем, подверженных уязвимости	Ответственный: - Аналитик угроз Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
	Определение уровня опасности уязвимости	Расчет базовой, контекстной и временной метрик по методике CVSS с использованием калькулятора CVSS V3 или V3.1, размещенного в банке данных угроз безопасности информации федеральной службы по техническому и экспортному контролю	Ответственный: - Аналитик угроз Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ

	Определение влияния на информационные системы	Определение влияния уязвимого компонента на защищенность информационных систем выполняется с использованием результатов процесса «Оценка угроз» (в части сведений о недопустимых негативных последствиях и возможных объектах воздействий), при этом могут быть использованы данные об ИТ-инфраструктуре, полученные из баз данных управления конфигурациями (отдельные результаты из процесса «Управление конфигурацией»)	Ответственный: - Аналитик угроз Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
	Расчет критичности уязвимости	Получение значений уровней критичности обнаруженных уязвимостей	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ

3.6. Анализ информации об уязвимостях, определенных на этапе мониторинга уязвимостей и оценки их применимости, продолжительность, выходные данные и результат определения уровня критичности уязвимостей применительно к информационным системам Администрации Горьковского муниципального района Омской области отражается в таблице 4.2.

Таблица 4.2

№ уязвимости	Название уязвимости	Исполнители	Продолжительность	Получение информации об объектах, подверженных уязвимости	Определение уровня опасности уязвимости	Определение влияния на информационные системы	Расчет критичности уязвимости

3.7. По результатам анализа уязвимостей формируется отчет по форме, представленной в Приложении №4 к настоящему регламенту, содержащий расчет критичности выявленных уязвимостей.

4. ОПРЕДЕЛЕНИЕ МЕТОДОВ И ПРИОРИТЕТОВ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

4.1. 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.

4.2. Входными данными для определения приоритетности устранения уязвимостей являются результаты расчета критичности уязвимостей на этапе оценки уязвимостей (п. 4 настоящего регламента).

4.3. Схема этапа определения методов и приоритетов устранения уязвимостей представлена на рисунке 5.1.

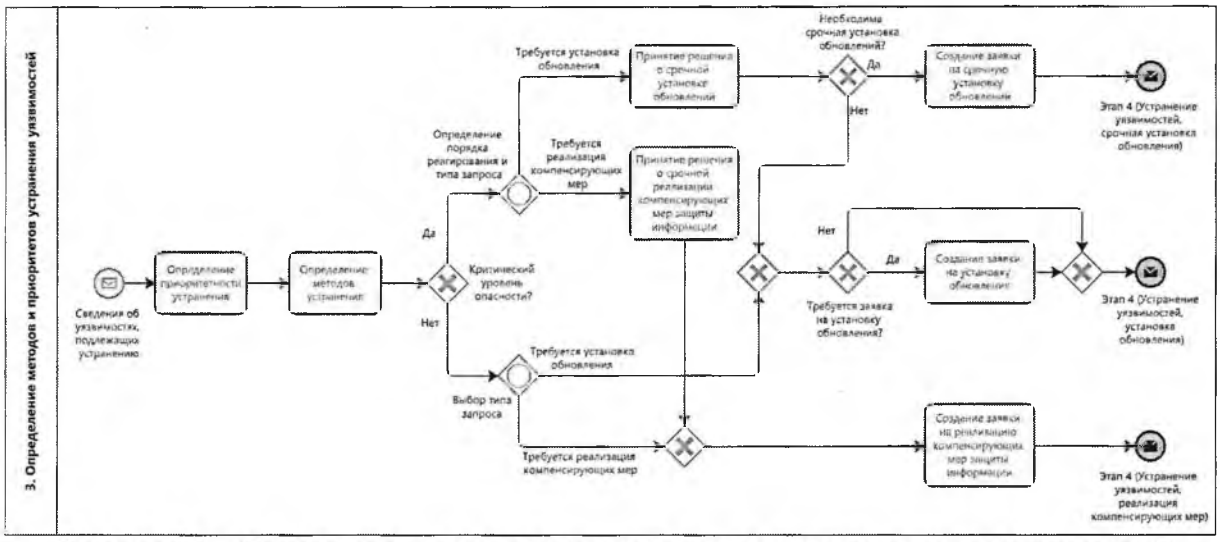


Рисунок 5.1. – Схема этапа определения методов и приоритетов устранения уязвимостей

4.4. Описание операций, выполняемых на этапе определения методов и приоритетов устранения уязвимостей, включающее наименование операций, описание операций, исполнителей операции, приведено в таблице 5.1

Таблица 5.1.

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
1.	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей (п. 4 настоящего регламента)	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
2.	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
3.	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	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Руководитель Подразделения ИБ
4.	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование руководителю подразделения ИТ (Приложение 7)	Ответственный: - Руководитель Подразделения ИБ Исполнитель: - Руководитель Подразделения ИБ
5.	Принятие решения о	При обнаружении критической уязвимости может быть принято решение о срочной	Ответственный: - Руководитель

	срочной реализации компенсирующих мер защиты информации	реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления	Подразделения ИБ Исполнитель: - Руководитель Подразделения ИБ
6.	Создание заявки на установку обновления	Заявка создается в случае, если определено, что установка обновления для устранения данной уязвимости не запланирована (Приложение 6)	Ответственный: - Аналитик угроз Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ
7.	Создание заявки на реализацию компенсирующих мер защиты информации	Заявка на реализацию компенсирующих мер защиты информации формируется при отсутствии возможности установки обновления, а также в случае необходимости принятия мер до устранения уязвимости (Приложение 8)	Ответственный: - Аналитик угроз Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ

4.5. На основании определения приоритетности и метода устранения уязвимостей, принятия решения о срочной установке обновления или реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления, создается заявки на срочную/плановую установку обновления или реализацию компенсирующих мер защиты информации (Приложения 6, 7, 8 к настоящему регламенту).

4.6. Для организации устранения уязвимостей между работниками подразделения ИБ и подразделения ИТ предварительно согласовываются:

– сроки установки обновлений, устраняющих уязвимости;

– форма и способы передачи информации об уязвимостях.

4.7. Анализ информации об приоритетности и методах устранения уязвимостей, продолжительность, выходные данные и результат определения приоритетности и метода устранения уязвимостей применительно к информационным системам Администрации Горьковского муниципального района Омской области отражается в таблице 5.2.

Таблица 5.2

№ уязви-мости	Название уязви-мости	Определение приоритетности устранения уязвимостей (срочная/плановая)	Определение метода устранения уязвимости (установка обновлений/ применение компенсирующих мер)	Принятие решения о срочной установке обновлений или применению компенсирующих мер для критичных уязвимостей (да/нет)	Продолжи-тельность/ срок устранения уязвимостей	Исполни-тели
1	2	3	4	5	6	7

4.8. По результатам определения приоритетности и метода устранения уязвимостей формируется отчет по форме, представленной в Приложении № 5 к настоящему регламенту.

5. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

5.1. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга.

5.2. Исходными (входящими) данными при устранении уязвимостей, является информация, полученная на этапе определения методов и приоритетов устранения уязвимостей.

5.3. Схема этапа устранения уязвимостей представлена на рисунке 6.1.

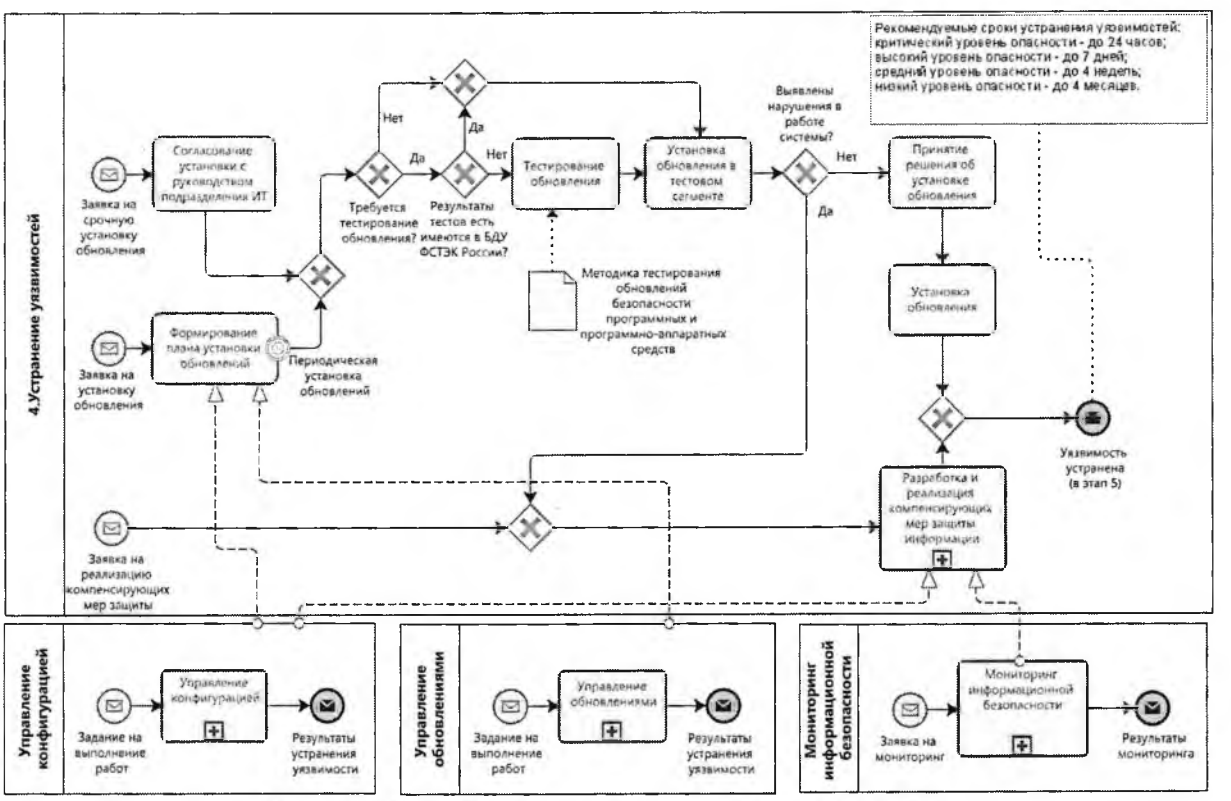


Рисунок 6.1. – Схема этапа устранения уязвимостей

5.4. Описание операций, выполняемых на этапе устранения уязвимостей, включающее наименование операций, описание операций, исполнителей операции, приведено в таблице 6.1

Таблица 6.1.

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
	Согласование установки с руководством подразделения ИТ	Срочная установка обновлений программного обеспечения предварительно согласовывается с руководством подразделения ИТ	Ответственный: Руководитель Подразделения ИБ Исполнитель: Руководитель Подразделения ИБ Участник: Руководитель Подразделения ИТ

	Тестирование обновления[4]	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)	Ответственный: Руководитель Подразделения ИТ Исполнитель: Специалист Подразделения ИТ
	Установка обновления в тестовом сегменте	Установка обновлений на выбранном тестовом сегменте информационной системы в целях определения влияния их установки на ее функционирование	Ответственный: Руководитель Подразделения ИТ Исполнитель: Специалист Подразделения ИТ
	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	Ответственный: Руководитель Подразделения ИТ Исполнитель: Руководитель Подразделения ИТ
	Установка обновления	Распространение обновления на объекты информационных систем	Ответственный: Руководитель Подразделения ИТ Исполнитель: Специалист Подразделения ИТ
	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	Ответственный: Руководитель Подразделения ИТ Исполнитель: Руководитель Подразделения ИТ
	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	Ответственный: Руководитель Подразделения ИБ Исполнитель: - Аналитик угроз Подразделения ИБ - Специалист по внедрению мер ЗИ подразделения ИБ Участник: Специалист подразделения ИТ

[4] Тестирование обновлений осуществляется в отношении программного обеспечения, в том числе с открытым исходным кодом, предназначенного для устранения уязвимостей программных, программно-аппаратных средств

		безопасности, внесение изменений в ИТ-инфраструктуру	

5.5. Установка обновления выполняется после осуществления проверок, перечисленных в таблице 6.2:

Таблица 6.2.

№ уязвимости	Название уязвимости	Требуется тестирование обновления? (да/нет)	Результат тестирования обновления имеется в банке данных угроз безопасности	Продолжительность/ срок установки обновлений в тестовом сегменте[6]	Исполнители тестирования обновления	установка обновлений вызвала нарушение работы системы? (да/нет)	Дата установки обновлений в рабочей	Исполнитель установки обновлений	Уязвимость устранена? (да/нет)
1	2	3	4	5	6	7	8	9	10

5.6. В случае если уязвимость найдена в информационной системе, которая не введена в эксплуатацию, то установка в тестовом сегменте не производится. Установка обновления производится непосредственно на информационной системе.

5.7. Тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с Методикой тестирования обновлений программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.[8], по решению органа (организации) в случае отсутствия соответствующих результатов тестирования в банке данных угроз безопасности информации федеральной службы по техническому и экспортному контролю.

5.8. Установка обновления на действующую информационную систему выполняется только в случае успешного проведения тестирования и принятия решения на установку обновлений. Данное действие выполняется специалистом подразделения ИТ. Определяются исполнители и сроки исполнения установки обновлений.

5.9. При обнаружении нарушений в работе тестового сегмента информационной системы во время проведения тестирования обновления разрабатывается заявка на разработку и реализацию компенсирующих мер защиты по форме, приведенной в Приложении 8.

5.10. 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

[5] Заполняется только для уязвимостей, для которых в п. 3 ответ «Да»
[6] Заполняется только для уязвимостей, для которых в п. 4 ответ «Нет»
[7] Заполняется в случае, если анализ проводился на тестовой системе при наличии рабочей
[8] Адрес: https://bdu.fstec.ru/documents/30

банке данных угроз безопасности информации федеральной службы по техническому и экспортному контролю.

5.11. Рекомендуемые сроки устранения уязвимостей[9]:

– критический уровень опасности до 24 часов;

– высокий уровень опасности – до 7 дней;

– средний уровень опасности – до 4 недель;

– низкий уровень опасности – до 4 месяцев.

5.12. Разработка и применение компенсирующих мер применяется в случае:

– неуспешного проведения тестирования обновления;

– поступления заявки на реализацию компенсирующих мер.

5.13. При разработке и реализации компенсирующих мер следует руководствоваться организационно-распорядительной документацией Администрации Горьковского муниципального района Омской области по информационной безопасности, а именно документами, регламентирующие управление конфигурацией и мониторинг информационной безопасности.

5.14. Описание операций, выполняемых выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации, включающее наименование операций, описание операций, исполнителей операции, приведено в таблице 6.3

Таблица 6.3.

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
1.	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	Ответственный: Руководитель Подразделения ИБ Исполнитель: Аналитик угроз Подразделения ИБ
2.	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	Ответственный: Руководитель Подразделения ИБ Исполнитель: Руководитель Подразделения ИБ Участник: Руководитель Подразделения ИТ
3.	Реализация организационных мер защиты	Реализация организационных мер защиты информации предусматривает:	Ответственный: Руководитель Подразделения ИБ Исполнитель: Руководитель

[9] Рекомендуемые сроки устранения уязвимостей установлены в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.

	информации	ограничение использования ИТ-инфраструктуры; организация режима охраны (в частности, ограничение доступа к техническим средствам); информирование и обучение персонала Администрации Горьковского муниципального района Омской области	Подразделения ИБ Участник: Руководитель Подразделения ИТ
4.	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	Ответственный: Руководитель Подразделения ИБ Исполнитель: - Специалист по внедрению мер ЗИ подразделения ИБ Участник: Специалист подразделения ИТ
5.	Администрация Горьковского муниципального района Омской области анализа событий безопасности	Администрация Горьковского муниципального района Омской области постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления и блокирования попыток эксплуатации уязвимости	Ответственный: Руководитель Подразделения ИБ Исполнитель: - Специалист по внедрению мер ЗИ подразделения ИБ
6.	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))	Ответственный: Руководитель Подразделения ИТ Исполнитель: - Специалист подразделения ИТ Участник: Аналитик угроз Подразделения ИБ

5.15. Схема подпроцесса разработки и реализации компенсирующих мер защиты информации на этапе устранения уязвимостей представлена на рисунке 6.2.

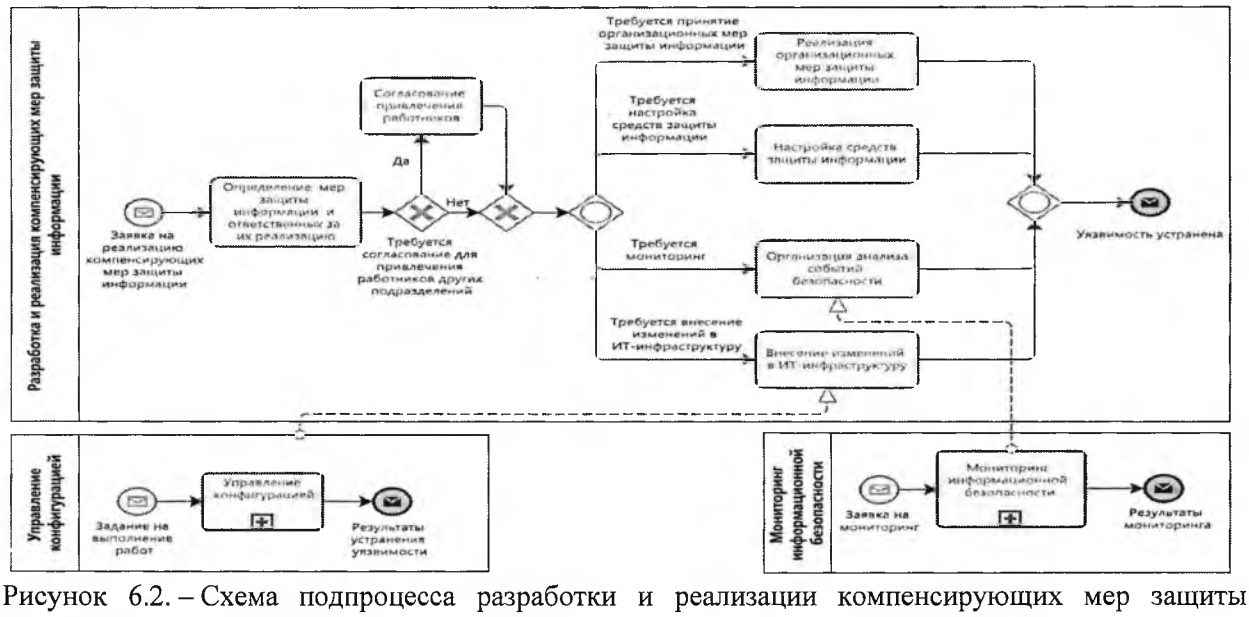


Рисунок 6.2. – Схема подпроцесса разработки и реализации компенсирующих мер защиты информации на этапе устранения уязвимостей

5.16. Разработка и реализация компенсирующих мер осуществляется в соответствии с таблицей 6.4:

Таблица 6.4

№ уязвимости	Название уязвимости	Определение компенсирующих мер	Описание компенсирующих мер	Срок реализации компенсирующих мер	Исполнитель
1	2	3	4	5	6

5.17. Для определения мер ЗИ могут привлекаться сотрудники других подразделений при согласовании руководителя данного подразделения.

5.18. В качестве компенсирующих мер могут быть выбраны:

- Организационные меры ЗИ;
- Дополнительные настройки средств защиты информации;
- Дополнительный анализ событий безопасности;
- Изменение ИТ-инфраструктуры.

5.19. По результатам этапа устранения уязвимостей формируется отчет по форме, представленной в Приложении №9 к настоящему регламенту.

6. КОНТРОЛЬ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

6.1. На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, принятие оперативных решений и их доведение до руководства Администрации Горьковского муниципального района Омской области для принятия решений по улучшению процесса управления уязвимостями.

6.2. Исходными (входящими) данными при контроле устранения уязвимостей, является информация, полученная на этапе устранения уязвимостей.

6.3. Схема этапа контроля устранения уязвимостей представлена на рисунке 7.1.

Рисунок 7.1. – Схема этапа контроля устранения уязвимостей

6.4. Описание операций, выполняемых на этапе контроля устранения уязвимостей, включающее наименование операций, описание операций, исполнителей операции, приведено в таблице 7.1

Таблица 7.1.

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
	Принятие решения о способе контроля	Определение способа контроля устранения уязвимости: проверка объектов на наличие уязвимости (сканирование средствами анализа защищенности) либо оценка защищенности	Ответственный: Руководитель Подразделения ИБ Исполнитель: Руководитель Подразделения ИБ
	Проверка объектов на наличие уязвимостей	Выбор объектов и времени сканирования, уведомление заинтересованных подразделений (например, ситуационного центра, подразделения ИТ) о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости	Ответственный: Руководитель Подразделения ИБ Исполнитель: Специалист по оценке защищенности Подразделения ИБ
	Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационным системам. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах Администрации Горьковского муниципального района Омской области с использованием PoC или средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационным системам в обход ее системы защиты информации)	Ответственный: Руководитель Подразделения ИБ Исполнитель: Специалист по оценке защищенности Подразделения ИБ
	Выявление отклонений и неисполнений	Анализ результатов контроля устранения уязвимостей (определение корректности устранения уязвимостей и соблюдения сроков)	Ответственный: Руководитель Подразделения ИБ Исполнитель: Специалист по оценке защищенности Подразделения ИБ
	Разработка предложений по улучшению процесса управления уязвимостями	Определение причин отклонений и неисполнений, разработка на их основе решений по улучшению процесса управления уязвимостями	Ответственный: Руководитель Подразделения ИБ Исполнитель: аналитик угроз Подразделения ИБ Участник: Руководитель Подразделения ИТ

6.5. Контроль устранения уязвимостей осуществления при проведении проверок, перечисленных в таблице 7.3:

Таблица 7.3.

№ уязвимости	Название уязвимости	Способ контроля[10]	Дата проведения оценки защищенности[11]	Дата сканирования объектов[12]	Применяемое средство анализа защищенности[4]	Исполнитель ОЗ или сканирования объектов	Срок проведения ОЗ или сканирования объектов	Выявлены отклонения или неисполнения?
1	2	3	4	5		6	7	8

6.6. Оценка защищенности проводится на основании согласованной заявки на исследовании в указанные в этой заявке сроки.

6.7. В случае выявления в ходе оценки защищенности неизвестных ранее уязвимостей (уязвимостей «нулевого дня») сведения о них рекомендуется направлять в банк данных угроз безопасности информации федеральной службы по техническому и экспортному контролю[13].

6.8. Сканирование объектов осуществляется средствами анализа защищенности.

6.9. Для проведения сканирования объектов допускается использование свободно распространяемого программного обеспечения, например, ScanOVAL ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

6.10. По результатам проведения оценки защищенности / сканирования объектов формируется отчет (приложение 10).

6.11. При выявлении отклонений или нарушений работы информационной системы проводится разработка предложений по улучшению процесса управления уязвимостей.

6.12. Схема подпроцесса разработки предложений по улучшению процесса управления уязвимостями на этапе контроля устранения уязвимостей представлена на рисунке 7.2.

---

[10] Способы контроля устранения уязвимости: сканирование средствами анализа защищенности либо оценка защищенности

[11] Заполняется только для уязвимостей, для которых в п. 3 ответ «Оценка защищенности»

[12] Заполняется только для уязвимостей, для которых в п. 3 ответ «Сканирование объектов»

[13] Включение неизвестных ранее уязвимостей в БДУ ФСТЭК России осуществляется в соответствии с утвержденным регламентом, размещенным по адресу https://bdu.fstec.ru/site/regulations

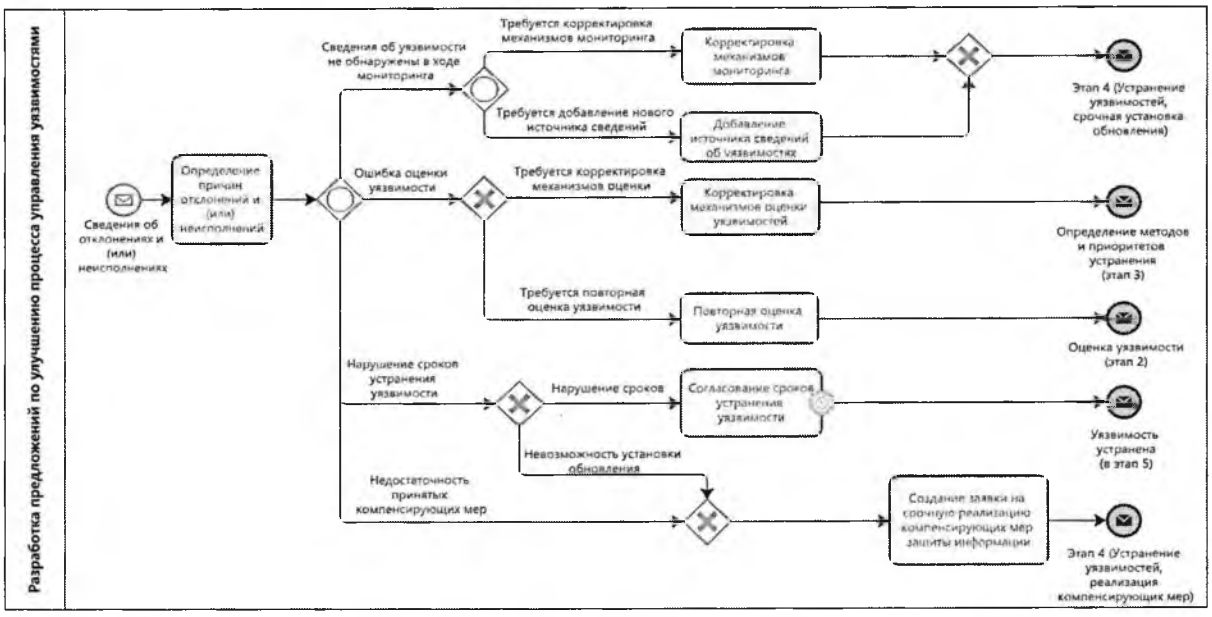


Рисунок 7.2. – Схема подпроцесса разработки предложений по улучшению процесса управления уязвимостями на этапе контроля устранения уязвимостей

6.13. В рамках выполнения подпроцесса разработки предложений по улучшению процесса управления уязвимостями выполняются операции, приведенные в таблице 7.4.

Таблица 7.4.

№ п/п	Наименование операции	Описание операции	Участники процесса мониторинга уязвимостей
1.	Определение причин отклонений и (или) неисполнений	Определение причин отклонений и неисполнений операций процесса управления уязвимостями. Возможными причинами являются: пропуск уязвимости в ходе мониторинга; ошибки оценки уязвимостей; нарушения сроков устранения уязвимостей; недостаточность принятых компенсирующих мер. Причины отклонений и неисполнений операций процесса управления уязвимостями могут быть дополнены по результатам анализа процесса управления уязвимостями в Администрации Горьковского муниципального района Омской области	Ответственный: Руководитель Подразделения ИБ Исполнитель: Руководитель Подразделения ИБ
2.	Корректировка механизмов мониторинга	Внесение изменений в конфигурацию и алгоритмы средств сбора и обработки данных об уязвимостях	Ответственный: Руководитель Подразделения ИБ Исполнитель: аналитик угроз Подразделения ИБ
3.	Добавление источника сведений об уязвимостях	Поиск и организация мониторинга новых источников сведений об уязвимостях	Ответственный: Руководитель Подразделения ИБ Исполнитель: аналитик угроз

			Подразделения ИБ
4.	Корректировка механизмов оценки уязвимостей	Внесение изменений в процедуру оценки уязвимостей	Ответственный: Руководитель Подразделения ИБ Исполнитель: аналитик угроз Подразделения ИБ
5.	Повторная оценка уязвимости	Повторное определение уровня критичности уязвимости применительно к информационным системам Администрации Горьковского муниципального района Омской области в соответствии с п. 4 настоящего регламента с дальнейшим выполнением последующих этапов процесса управления уязвимостями	Ответственный: Руководитель Подразделения ИБ Исполнитель: аналитик угроз Подразделения ИБ
6.	Согласование сроков устранения уязвимости	В случае нарушения сроков устранения уязвимостей новые сроки установки обновления согласуются с подразделением ИТ, сроки реализации компенсирующих мер защиты информации – с ответственными лицами, определенными на п. 4 настоящего регламента.	Ответственный: Руководитель Подразделения ИБ Исполнитель: Руководитель Подразделения ИБ
7.	Создание заявки на срочную реализацию компенсирующих мер защиты информации	Заявка на реализацию компенсирующих мер формируется при отсутствии возможности установки обновления либо в случае недостаточности уже принятых компенсирующих мер защиты информации	Ответственный: Руководитель Подразделения ИБ Исполнитель: аналитик угроз Подразделения ИБ Участник: Руководитель подразделения ИТ

6.14. Ответственное лицо определяет причины отклонений и (или) неисполнения.

6.15. Возможными причинами отклонений могут являться:

- Ошибка оценки уязвимости;
- Нарушение сроков устранения уязвимостей;
- Недостаточность принятых компенсирующих мер;
- Сведения об уязвимости не обнаружены в ходе мониторинга.

6.16.Ошибка оценки уязвимости.

6.16.1. В случае выявления ошибки оценки уязвимостей необходимо провести повторную оценку в соответствии с этапом оценки уязвимостей.

6.16.2. Ошибка оценки уязвимости может являться следствием некорректного определения механизмов оценки. Выполняется корректировка механизмов оценки уязвимостей в соответствии с этапом определения методов и приоритетов устранения уязвимостей.

6.17.Нарушение сроков устранения уязвимостей.

6.17.1. В случае нарушения сроков устранения уязвимостей выполняется повторное согласование устранения уязвимостей на основании заявки и выполняются работы по разработке и реализации компенсирующих мер согласно п. 6 настоящего регламента.

6.17.2. При нарушении сроков вследствие невозможности установки обновления создается заявка на срочную реализацию компенсирующих мер защиты информации согласно Приложению 8 к настоящему регламенту и выполняются работы по разработке и реализации компенсирующих мер согласно п. 6 настоящего регламента.

6.18.При недостаточности принятых компенсирующих мер создается заявка на срочную реализацию компенсирующих мер защиты информации согласно Приложению 8 к настоящему регламенту и выполняются работы по разработке и реализации компенсирующих мер согласно п. 6 настоящего регламента.

6.19.Сведения об уязвимости не были обнаружены в ходе мониторинга.

6.19.1. При неверно выбранных механизмов мониторинга необходимо провести корректировку выбора и выполнить устранение уязвимости в соответствии с Приложением 4 к настоящему регламенту.

6.19.2. Уязвимость могла быть необнаруженной в случае неиспользования дополнительных источников. В данном случае необходимо добавить источник сведений об уязвимостях и провести устранение уязвимости в соответствии с Приложением 4 к настоящему регламенту.

6.19.3.

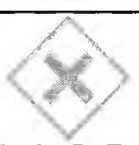
Таблица 7.5.

№ уязвимости	Название уязвимости	Причина отклонения и (или) неисполнения	Применяемые меры для устранения отклонения и (или) неисполнения	Исполнитель
1	2	3	4	5

Приложение № 1 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Условные обозначения, применяемые в Регламенте по управлению уязвимостями в Администрации Горьковского муниципального района Омской области

На схемах в настоящем регламенте используются следующие элементы из системы условных обозначений для моделирования бизнес-процессов BPMN 2.0 (англ. Business Process Management Notation, нотация моделирования бизнес-процессов):

	– начальное событие, показывает с чего начинается процесс;
	– начальное событие, связанное с получением сообщений (данных);
	– промежуточное событие, связанное с истечением определенного временного интервала;
	– окончание процесса или подпроцесса;
	– окончание процесса или подпроцесса, связанное с отправкой сообщений (данных);
	– завершение всех процессов и подпроцессов;
	– развилка «или/или» – выбор только одного пути;
	– развилка «и» – выбор всех путей;
	– развилка «и/или» – выбор одного или нескольких путей;
	– элементарное действие в рамках процесса;
	– действие, которое может включать в себя другие действия, развилки и события.

Приложение № 2 к регламенту «Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»Отчет о проведении мониторинга уязвимостей и оценки

их применимости в информационной системе Администрации Горьковского муниципального района Омской области

Был выполнен анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационной системе Администрации Горьковского муниципального района Омской области.

Выявление уязвимостей было проведено на основании данных из следующих источников:

– документация на информационные системы;

– база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России.

Результат анализа оценки применимости уязвимостей отражен в таблице 1.

Таблица 1.

№ уязвимости	Название уязвимости	Источник информации об уязвимости	Анализ информации об уязвимости	Исполнители	Продолжительность	Оценка применимости уязвимости к инфраструктуре	Решение о применимости уязвимости к инфраструктуре (релевантности) (да/нет)	Принятие решений на получение дополнительной информации
1	2	3	4	5	6	7	8	9
								сканирование объектов
								оценка защищенности
								Не требуется

Для определения релевантности уязвимостей, в отношении которых принято решение на получение дополнительной информации, методом сканирования объектов, проведено сканирование объектов.

Сканирование объектов осуществлено на основании заявки на сканирование №____ от «___» _____г., содержащей перечень выбранных объектов, их расположение и время сканирования.

О проведении сканирования уведомляются заинтересованные

подразделения:

- функциональные отделы;
- подразделения ИТ.

Сканирование объектов выполнено с помощью средств анализа защищенности «___» _____г. (сертификат ФСТЭК России № ___, действителен до «___» _____г.).

Отчет о сканировании уязвимостей, выполненный с помощью средства анализа защищенности, содержащий перечень уязвимостей с указанием их критичности, приведен в приложении 1 к настоящему отчету.

Для определения релевантности уязвимостей, в отношении которых принято решение на получение дополнительной информации, методом оценки защищенности объектов, проведена оценка защищенности объектов.

В ходе оценки защищенности осуществлена проверка возможности эксплуатации уязвимости в информационных системах Администрации Горьковского муниципального района Омской области с использованием PoC или 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)

Отчет по результатам оценки защищенности, включающий оценку возможности эксплуатации уязвимости в информационных системах Администрации Горьковского муниципального района Омской области, приведен в приложении 2 к настоящему отчету.

По результатам анализа полученной дополнительной информации был сделан вывод о релевантности уязвимости по отношению к информационной системе. Результат отражен в таблице 2.

Таблица 2

№ уязвимости	Название уязвимости	Вывод о релевантности уязвимости (да/нет)
1	2	3

Для релевантных уязвимостей необходимо провести оценку уровня критичности применительно к информационной системе в соответствии с Регламентом по оценке уязвимостей в Администрации Горьковского муниципального района Омской области.

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Приложение №3 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Наименование должности руководителя подразделения ИТ
От Наименование должности руководителя подразделения ИБ

ЗАЯВКА
на проведение сканирования объектов информационных систем

От «___» _____20__ г. №_____

Прошу согласовать проведение сканирования объектов информационных систем _____ на наличие уязвимостей в срок с _____ по _____. Перечень объектов для проведения сканирования прилагаю в таблице 1.

Таблица 1

Объект сканирования	Расположение объекта сканирования	IP-адрес / DNS-имя объекта сканирования

_____ _____ _____
(должность) (подпись) (И.О. Фамилия)

Согласовано

_____ _____ _____
(должность) (подпись) (И.О. Фамилия)

Приложение № 4 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Отчет об анализе уязвимостей
в информационной системе Администрации Горьковского муниципального района Омской области

На основании отчета о проведении мониторинга уязвимостей и оценки их применимости в информационной системе _____ (далее – Система) от «___» _____ 202___ г. №_____ проведена оценка уровня критичности выявленных уязвимостей.

Исполнитель: _____
Продолжительность оценки – _____ часов.

Результаты оценки приведены в таблице 1.

Таблица 1

№ уязвимости	Название уязвимости	Объекты, подверженные уязвимости	Уровень опасности уязвимости (I_{cvss})	Тип компонента информационной системы (K)	Количество уязвимых компонентов информационной системы (L)	Влияние уязвимого компонента на защищенность периметра информационной системы (P)	Показатель влияния уязвимости на информационные системы (I_{infr}) *	Уровень критичности уязвимости (V) **

Приложение № 5 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Отчёт об определении методов и приоритетов устранения уязвимостей

От «___» _____ 20___ г. №_____

На основании:

– Отчета о выявлении потенциальных уязвимостей и оценке их применимости в информационной системе от «___» _____ 20__ г. №_____;

– Отчета о проведении оценки уязвимостей от «___» _____ 20___ г. №_____, определены методы и приоритеты устранения выявленных уязвимостей информационной системы _____ (далее – Система).

Исполнитель: _____.

Продолжительность определения – _____ час.

Результаты приведены в таблице 1.

Таблица 1

№ уязвимости	Название уязвимости	Приоритетность устранения уязвимостей (срочная/плановая)	Метод устранения уязвимости (установка обновлений/применение компенсирующих мер)	Необходимость срочной установки обновлений или применение компенсирующих мер (да/нет)	Срок устранения уязвимостей	Исполнитель

_____ _____ _____

(должность) (подпись) (И.О. Фамилия)

Приложение № 6 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Наименование должности руководителя подразделения ИТ
Наименование организации
От Наименование должности руководителя подразделения ИБ

Заявка на установку обновления программного обеспечения объектов информационных систем

Для устранения уязвимостей, выявленных в (программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей), прошу согласовать сроки и выполнить установку обновления программного обеспечения объектов информационных систем, подверженных уязвимости.

Название программного обеспечения	№ уязви-мости	Название уязвимости	Определение приоритетности устранения уязвимостей (срочная/плановая)	Сроки установки обновлений, устраняющих уязвимости	Форма и способы передачи информации об уязвимостях
1	2	3	4	5	6

Ответственным от отдела ИБ за взаимодействие с Ответственным от отдела ИТ назначен (ФИО и должность, номер телефона или другие контактные данные)

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Согласовано

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Приложение № 7 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Наименование должности руководителя подразделения ИТ
Наименование организации
От Наименование должности руководителя подразделения ИБ

Заявка на срочную установку обновления программного обеспечения объектов информационных систем

Для устранения уязвимостей, выявленных в (программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей), прошу согласовать сроки и выполнить установку обновления программного обеспечения объектов информационных систем, подверженных уязвимости.

Название программное обеспечение	№ уязви-мости	Название уязвимости	Определение приоритетности устранения уязвимостей (срочная/плановая)	Сроки установки обновлений, устраняющих уязвимости	Форма и способы передачи информации об уязвимостях
1	2	3	4	5	6

Ответственным от отдела ИБ за взаимодействие с Ответственным от отдела ИТ назначен (ФИО и должность, номер телефона или другие контактные данные)

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Согласовано

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Приложение № 8 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Наименование должности руководителя подразделения ИТ
Наименование организации
От Наименование должности руководителя подразделения ИБ

Заявка на реализацию компенсирующих мер защиты информации

Для устранения уязвимостей, выявленных в (программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей), прошу согласовать перечень компенсирующих мер защиты информации, сроки и ответственных за их реализацию.

№ уязви-мости	Название уязвимости	Название программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, подверженных уязвимости	Определение приоритетности и устранения уязвимостей (срочная/плановая)	содержание компенсирующих мер защиты информации	Ответственное за реализацию компенсирующих мер защиты информации подразделение	форма и способы передачи информации об уязвимостях
1	2	3	4	5	6	7

Ответственным от отдела ИБ за взаимодействие при реализации компенсирующих мер защиты информации назначен (ФИО и должность, номер телефона или другие контактные данные)

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Согласовано

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Приложение № 9 к Регламенту «Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Форма 9.1

Наименование должности
руководителя подразделения ИТ
Наименование организации
От Наименование должности
руководителя подразделения ИБ

Отчет
об устранении уязвимостей

Срочное устранение уязвимостей согласовано __.__.20___ с руководителем подразделения ИТ (заявка №____ от __.__.20___).[14]

Входными данными для устранения уязвимостей является заявка на установку обновления.

На основании заявки на установку обновления проводились мероприятия по устранению уязвимостей.

Таблица 1

№ уязвимости	Название уязвимости	Требуется тестирование обновления? (да/нет)	Результат тестирования обновления имеется в банке данных угроз безопасности	Продолжительность/ срок установки обновлений в тестовом сегменте	Исполнители тестирования обновления	установка обновлений вызвала нарушение работы системы? (да/нет)	Дата установки обновлений	Исполнитель установки обновлений	Уязвимость устранена? (да/нет)
1	2	3	4	5	6	7	8	9	10

При попытке установки обновления с целью устранения уязвимостей №_____ было выявлено негативное влияние на информационную систему, в связи с чем принято решение разработать и реализовать компенсирующие меры для устранения этих уязвимостей:

Таблица 2

№ уязвимости	Название уязвимости	Определение компенсирующих мер	Описание компенсирующих мер	Срок реализации компенсирующих мер	Исполнитель
1	2	3	4	5	6

[14] Актуально только при принятии решения о срочной установки обновления.

В результате проведения мероприятий, перечисленных в таблицах 1 и 2 было выполнено устранение уязвимостей.

_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Форма 9.2

Наименование должности
руководителя подразделения ИТ
Наименование организации
От Наименование должности
руководителя подразделения ИБ

Отчет
об устранении уязвимостей

На основании заявки на реализацию компенсирующих мер защиты специалистом подразделения ИБ были разработаны и выполнены следующие компенсирующие меры:

№ уязвимости	Название уязвимости	Определение компенсирующих мер	Описание компенсирующих мер	Срок реализации компенсирующих мер	Исполнитель
1	2	3	4	5	6

_____ _____ _____
(должность) (подпись) (И.О. Фамилия)

Приложение №10 к регламенту
«Управление уязвимости в информационных системах, эксплуатируемых Администрацией Горьковского муниципального района Омской области»

Отчет контроля устранения уязвимостей информационной системы

От «___» _____ 2023 г. №_____

В срок с _____ по _____ проведен контроль устранения уязвимостей в информационной системе _____ (далее – Система).

Исполнитель: _____.

Продолжительность анализа – _____ часов.

Результаты контроля приведены в таблице 1.

Таблица 1

№ уязвимости	Название уязвимости	Способ контроля	Дата сканирования объектов	Применяемое средство анализа защищенности	Исполнитель сканирования объектов	Срок проведения сканирования объектов	Выявлены отклонения или неисполнения?
1	2	3	5		6	7	8

При проведении контроля выявлено, что все уязвимости, перечисленные таблице 1, устранены. Дополнительные мероприятия для устранения этих уязвимостей не требуются.

_____ _____ _____

(должность) (подпись) (И.О. Фамилия)