

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
17 мая 2023 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**РУКОВОДСТВО
ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В
ОРГАНЕ (ОРГАНИЗАЦИИ)**

СОДЕРЖАНИЕ

1. Общие положения	3
2. Процесс управления уязвимостями.....	5
3. Мониторинг уязвимостей и оценка их применимости	12
4. Оценка уязвимостей.....	16
5. Определение методов и приоритетов устранения уязвимостей.....	19
6. Устранение уязвимостей	22
7. Контроль устранения уязвимостей.....	27
Приложение	33

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее руководство по управлению уязвимостями в органе (организации) (далее – Руководство) разработано в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Руководство определяет состав и содержание работ по анализу и устранению уязвимостей (далее – управление уязвимостями), выявленных в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, информационно-телекоммуникационных инфраструктурах центров обработки данных, на базе которых функционируют эти системы и сети (далее – информационные системы).

1.3. Настоящее Руководство подлежит применению государственными органами, организациями, в том числе субъектами критической информационной инфраструктуры Российской Федерации, являющимися операторами информационных (автоматизированных) систем (далее – органы (организации)) при принятии ими мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.

1.4. Задачами Руководства являются создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования органов (организаций) и организация взаимодействия между структурными подразделениями органов (организаций) по вопросам устранения уязвимостей.

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

1.6. 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.

1.7. В Руководстве используются обозначения на схемах, приведенные в приложении 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 органа (организации).

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 органа (организации) 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 органа (организации):

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 органа (организации);

оценка угроз безопасности информации – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в информационных системах органа (организации);

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

управление обновлениями – приобретение, анализ и развертывание обновлений программного обеспечения в органе (организации);

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 уязвимостями представлена на рисунке 2.2.

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);

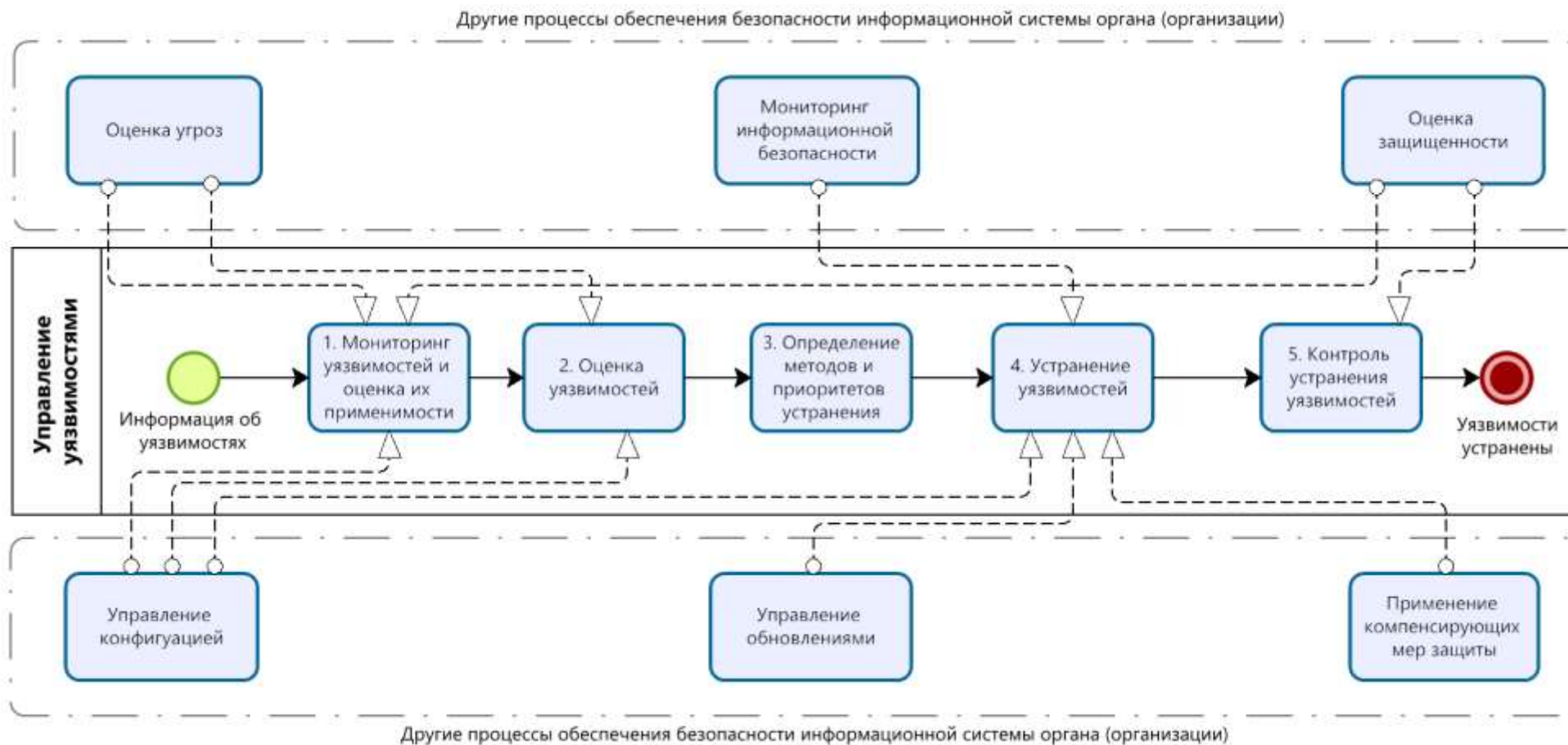


Рисунок 2.2. – Схема процесса управления уязвимостями

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 руководителя органа (организации) 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 органа (организации) ¹, представлено в таблице 2.1.

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 информации		+				
		(ОИ)				
Постановка задачи на сканирование объектов	+					
	(ОИ)					

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

1	2	3	4	5	6	7
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 компенсирующих мер защиты информации		+				
		(ОИ)				
Устранение уязвимостей						
Согласование установки с	+				+	
	(ОИ)				(У)	

1	2	3	4	5	6	7
руководством подразделения ИТ						
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)
Организация анализа событий безопасности	+			+		
	(О)			(И)		
Внесение изменений в ИТ-инфраструктуру		+			+	+
		(У)			(О)	(И)
Контроль устранения уязвимостей						
Принятие решения о способе контроля	+					
	(ОИ)					
Проверка объектов на наличие уязвимостей	+		+			
	(О)		(И)			
Оценка защищенности	+		+			
	(О)		(И)			

1	2	3	4	5	6	7
Выявление отклонений и неисполнений	+		+			
Разработка предложений по улучшению процесса управления уязвимостями	+	+			+	
Разработка предложений по улучшению процесса управления уязвимостями						
Определение причин отклонений и (или) неисполнений	+					
Корректировка механизмов мониторинга	+	+				
Добавление источника сведений об уязвимостях	+	+				
Корректировка механизмов оценки уязвимостей	+	+				
Согласование сроков устранения уязвимости	+				+	
Создание заявки на срочную реализацию компенсирующих мер защиты информации	+	+				
Обозначения: О – Ответственный – работник, ответственный за завершение выполнения задачи; И – Исполнитель – работник, непосредственно выполняющий задачу; У – Участник – работник, участие которого требуется для выполнения задачи						

3. МОНИТОРИНГ УЯЗВИМОСТЕЙ И ОЦЕНКА ИХ ПРИМЕНИМОСТИ

3.1. 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 конфигурациями²;

документация на информационные системы;

электронные базы знаний органов (организаций);

б) база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации (далее – БДУ) ФСТЭК России³;

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 органа (организации).

3.2. Схема этапа мониторинга уязвимостей и оценки их применимости представлена на рисунке 3.1⁴.

² Системы класса CMDB (англ. Configuration Management Database)

³ Адрес сайта БДУ ФСТЭК России: <https://bdu.fstec.ru>

⁴ В настоящем Руководстве представлены типовые схемы этапов процесса устранения уязвимостей

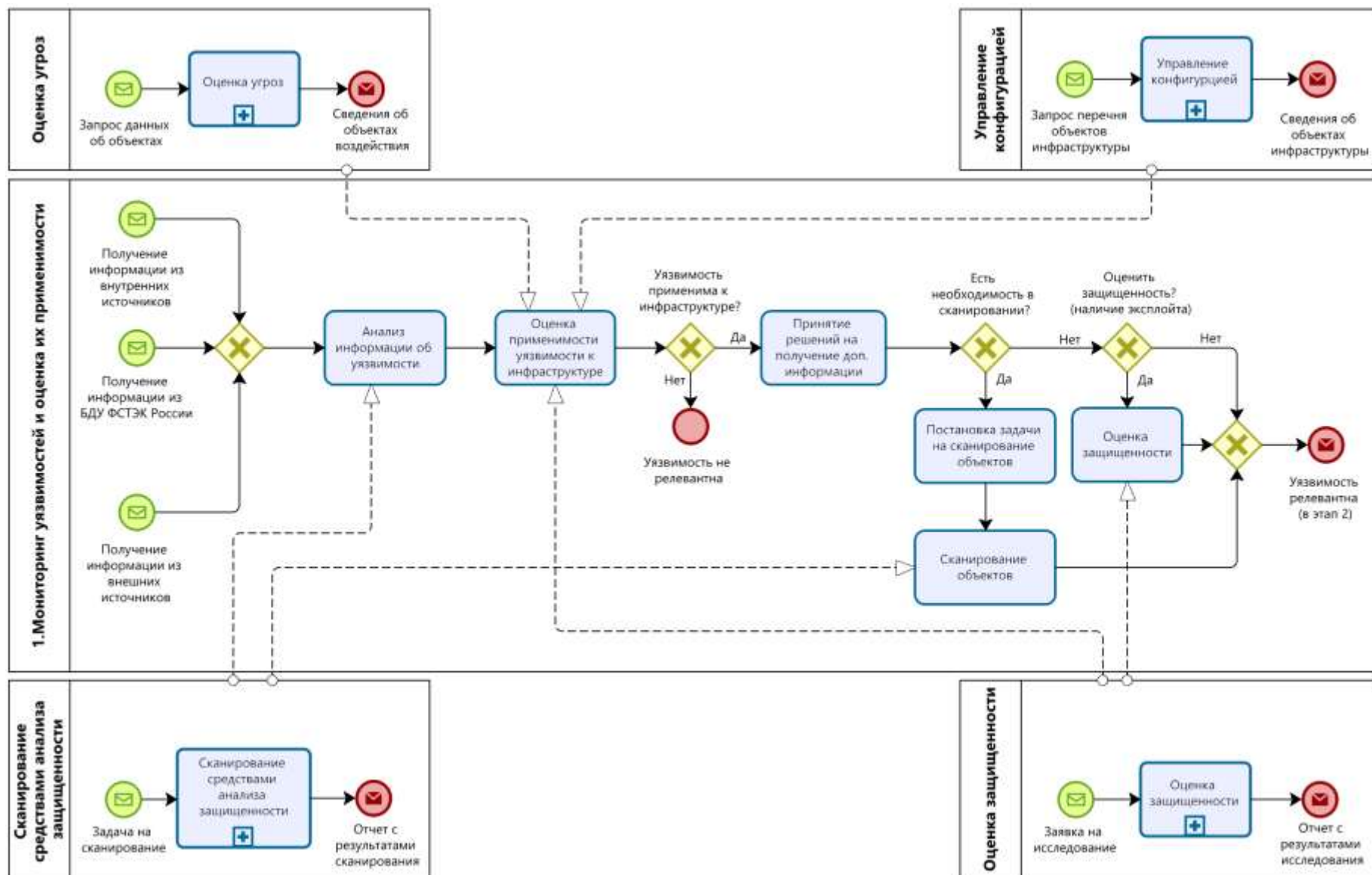


Рисунок 3.1. – Схема этапа мониторинга уязвимостей и оценки их применимости

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

Таблица 3.1.

№ п/п	Наименование операции	Описание операции
1.	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
2.	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 (п. 6)
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
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
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 сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
6.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационным системам. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных

№ п/п	Наименование операции	Описание операции
		системах органа (организации) с использованием PoC ⁵ 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)

3.3. На основе таблицы 3.1. в органе (организации) 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 органа (организации).

⁵ PoC (англ. Proof of Concept, проверка концепции) – моделирование эксплуатации уязвимости

4. ОЦЕНКА УЯЗВИМОСТЕЙ

4.1. Оценка уязвимостей производится с целью определения уровня критичности уязвимостей применительно к информационным системам органа (организации).

4.2. На этапе оценки уязвимостей выполняются операции, приведенные в таблице 4.1.

Таблица 4.1.

№ п/п	Наименование операции	Описание операции
1.	Получение информации об объектах, подверженных уязвимости	Получение выборки объектов информационных систем, подверженных уязвимости
2.	Определение уровня опасности уязвимости	Расчет базовой, контекстной и временной метрик по методике CVSS с использованием калькулятора CVSS ⁶ V3 или V3.1, размещенного в БДУ ФСТЭК России ⁷
3.	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»)
4.	Расчет критичности уязвимости	Получение значений уровней критичности обнаруженных уязвимостей

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.⁸

⁶ CVSS (англ. Common Vulnerability Scoring System) – общая система оценки уязвимостей (адрес: <https://www.first.org/cvss>)

⁷ Адреса: <https://bdu.fstec.ru/calc3>, <https://bdu.fstec.ru/calc31>

⁸ Адрес: <https://bdu.fstec.ru/documents/31>

4.3. На основе таблицы 4.1. в органе (организации) 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 органа (организации).

4.4. Схема этапа оценки уязвимостей представлена на рисунке 4.1.

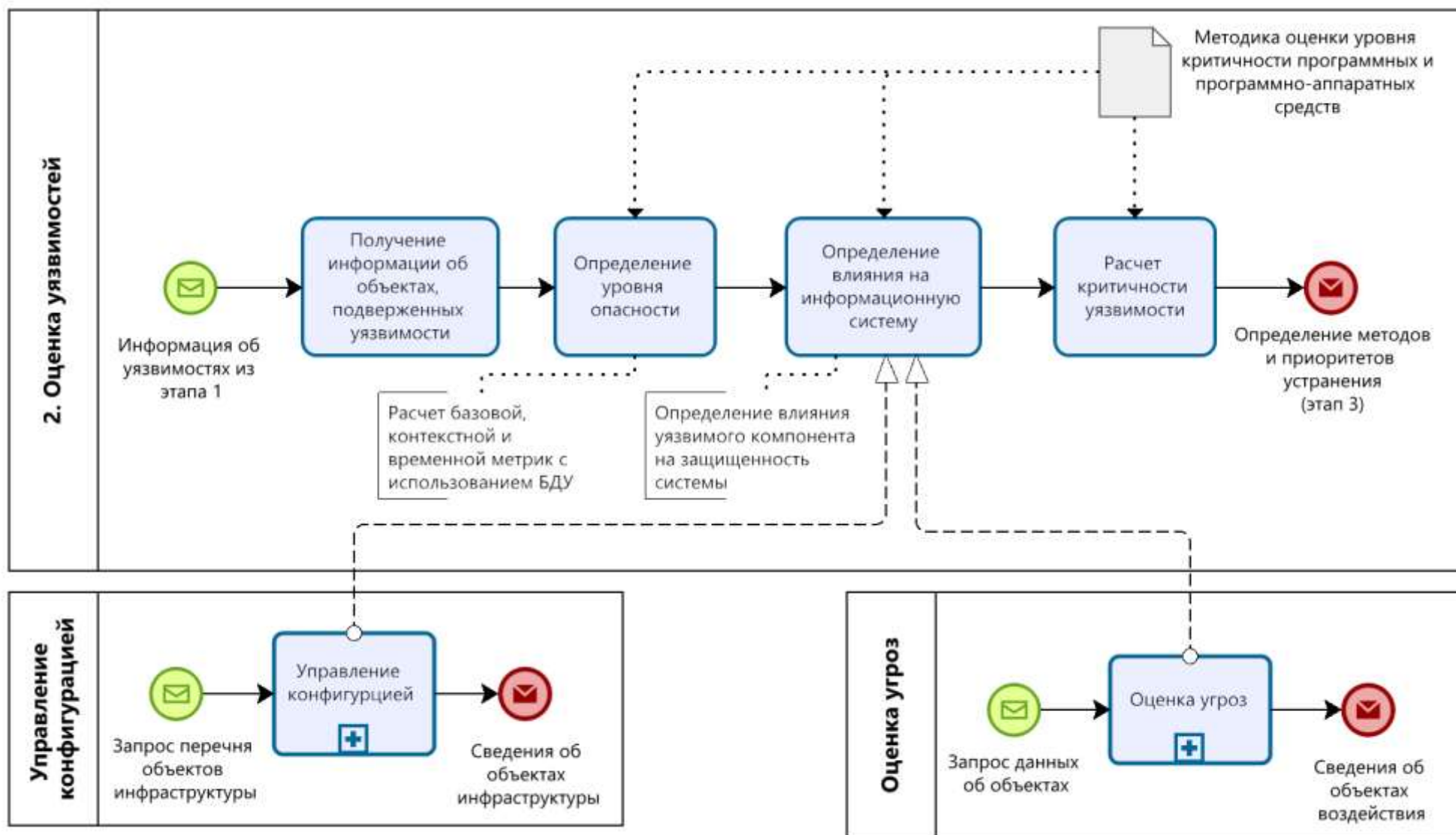


Рисунок 4.1. – Схема этапа оценки уязвимостей

5. ОПРЕДЕЛЕНИЕ МЕТОДОВ И ПРИОРИТЕТОВ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

5.1. 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.

На этапе определения методов и приоритетов устранения уязвимостей выполняются операции, приведенные в таблице 5.1.

Таблица 5.1.

№ п/п	Наименование операции	Описание операции
1.	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей (этап 4)
2.	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации
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
4.	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование руководителю подразделения ИТ
5.	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
6.	Создание заявки на установку обновления	Заявка создается в случае, если определено, что установка обновления для устранения данной уязвимости не запланирована
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

5.2. Для организации устранения уязвимостей между работниками подразделения защиты и подразделения ИТ предварительно согласовываются: сроки установки обновлений, устраняющих уязвимости; форма и способы передачи информации об уязвимостях.

5.3. На основе таблицы 5.1. в органе (организации) 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 органа (организации).

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

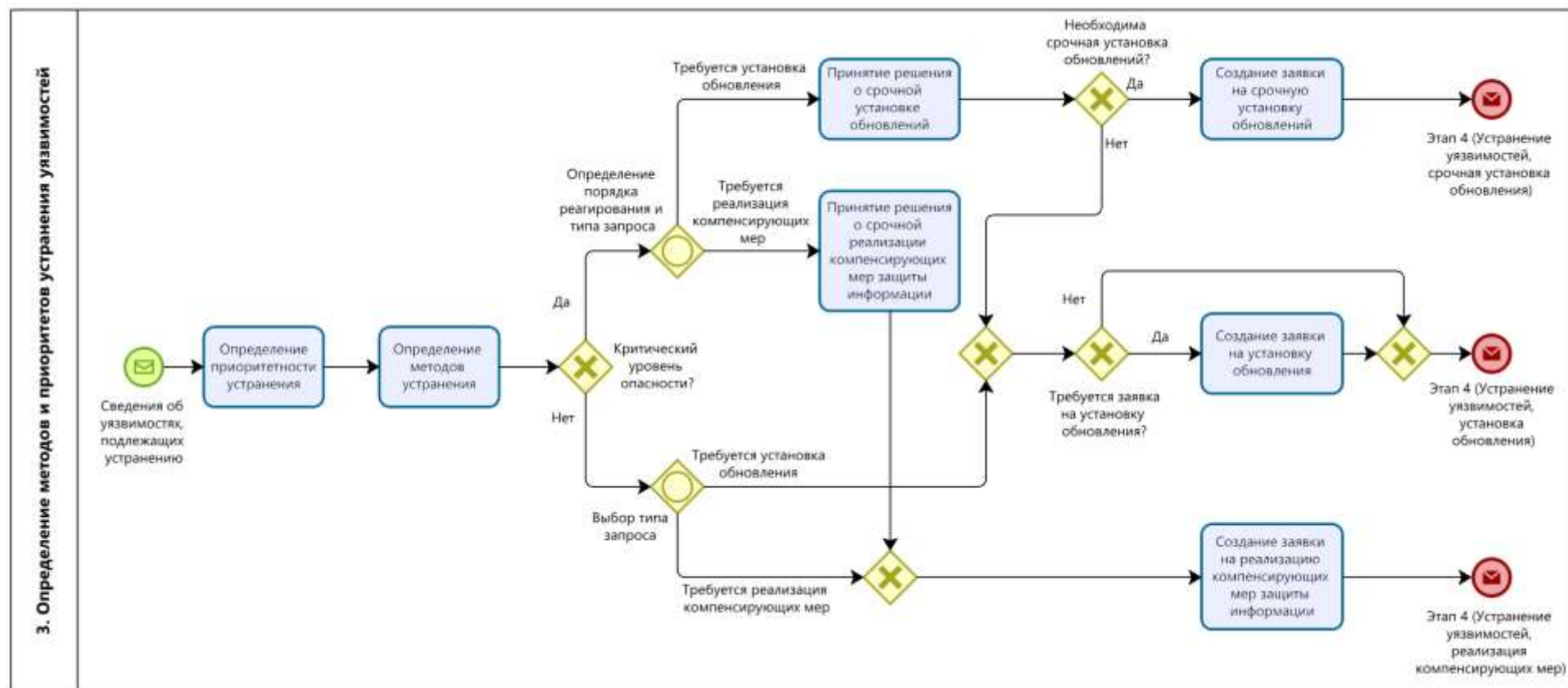


Рисунок 5.1. – Схема этапа определения методов и приоритетов устранения уязвимостей

6. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

6.1. 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 6.1.

Таблица 6.1.

№ п/п	Наименование операции	Описание операции
1.	Согласование установки с руководством подразделения ИТ	Срочная установка обновлений программного обеспечения предварительно согласовывается с руководством подразделения ИТ
2.	Тестирование обновления ⁹	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недедекларированные возможности)
3.	Установка обновления в тестовом сегменте	Установка обновлений на выбранном тестовом сегменте информационной системы в целях определения влияния их установки на ее функционирование
4.	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
5.	Установка обновления	Распространение обновления на объекты информационных систем
6.	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
7.	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

⁹ Тестирование обновлений осуществляется в отношении программного обеспечения, в том числе с открытым исходным кодом, предназначенного для устранения уязвимостей программных, программно-аппаратных средств

		<p>обновления, а также в случае необходимости принятия мер до устранения уязвимости.</p> <p>К компенсирующим мерам защиты информации могут относиться: организационные меры защиты информации, настройка средств защиты информации, анализ событий безопасности, внесение изменений в ИТ-инфраструктуру</p>
--	--	---

6.2. 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.¹⁰, по решению органа (организации) в случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России.

6.3. 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.

6.4. Рекомендуемые сроки устранения уязвимостей¹¹:

критический уровень опасности до 24 часов;

высокий уровень опасности – до 7 дней;

средний уровень опасности – до 4 недель;

низкий уровень опасности – до 4 месяцев.

6.5. Схема этапа устранения уязвимостей представлена на рисунке 6.1.

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

¹⁰ Адрес: <https://bdu.fstec.ru/documents/30>

¹¹ Рекомендуемые сроки устранения уязвимостей установлены в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.

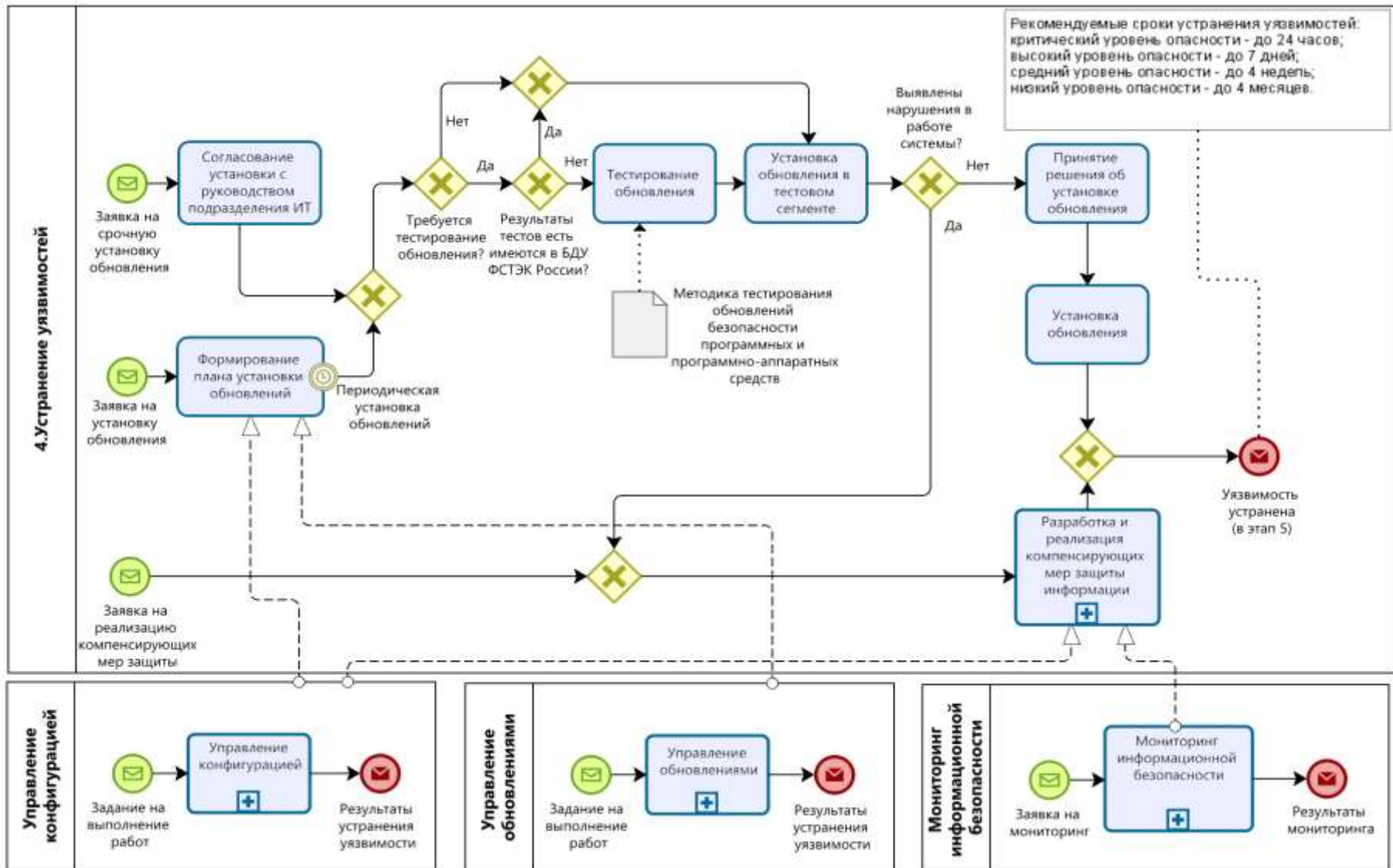


Рисунок 6.1. – Схема этапа устранения уязвимостей

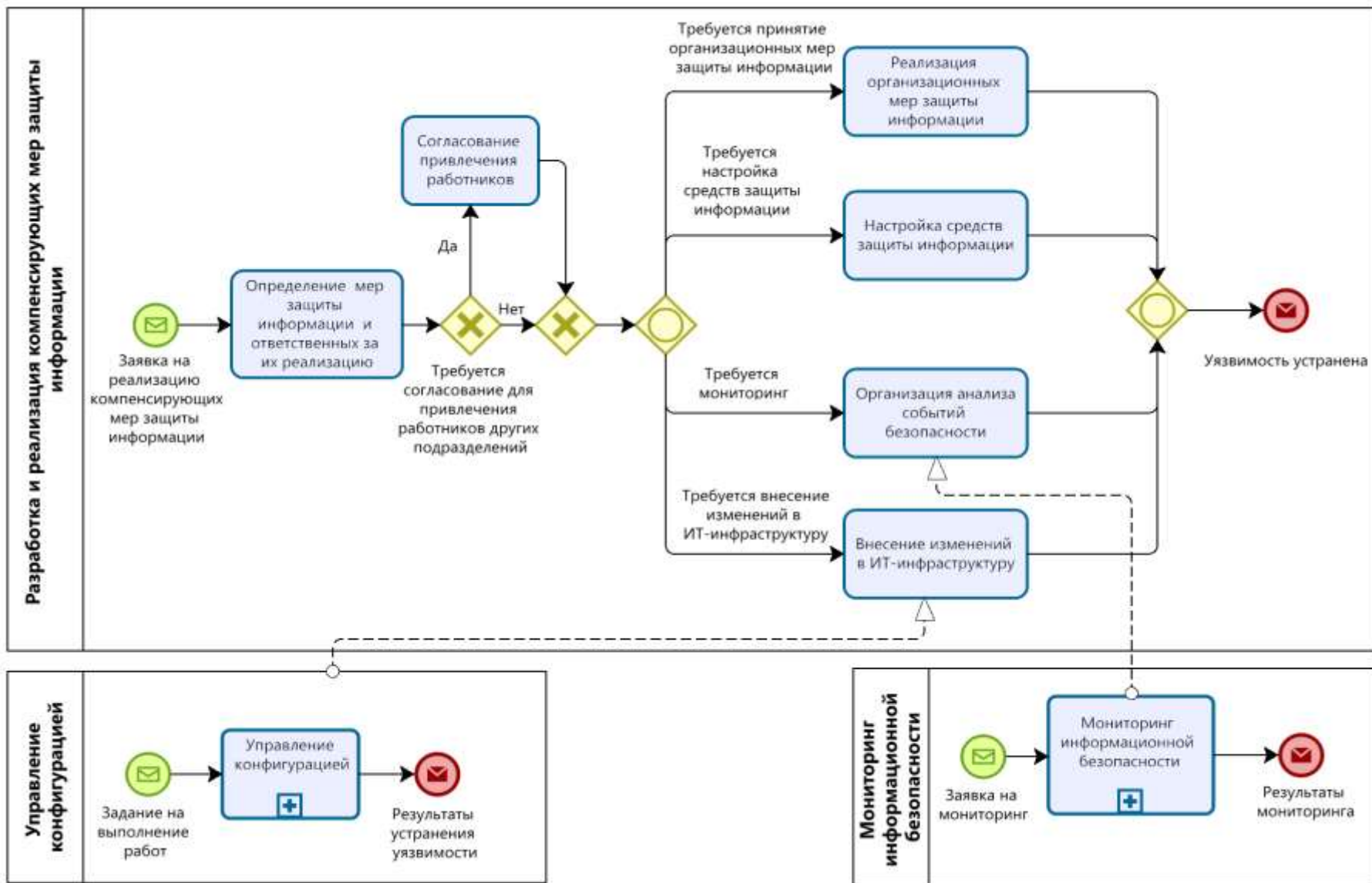


Рисунок 6.2. – Схема подпроцесса разработки и реализации компенсирующих мер защиты информации на этапе устранения уязвимостей

В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации выполняются операции, приведенные в таблице 6.2.

Таблица 6.2.

№ п/п	Наименование операции	Описание операции
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
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
3.	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)
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
5.	Организация анализа событий безопасности	Организация постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления и блокирования попыток эксплуатации уязвимости
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))

6.7. На основе таблиц 6.1 и 6.2. в органе (организации) 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 органа (организации).

7. КОНТРОЛЬ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

7.1. 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 органа (организации) для принятия решений по улучшению процесса управления уязвимостями.

На этапе контроля устранения уязвимостей выполняются операции, приведенные в таблице 7.1.

Таблица 7.1.

№ п/п	Наименование операции	Описание операции
1.	Принятие решения о способе контроля	Определение способа контроля устранения уязвимости: проверка объектов на наличие уязвимости (сканирование средствами анализа защищенности) либо оценка защищенности
2.	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
3.	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 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)
4.	Выявление отклонений и неисполнений	Анализ результатов контроля устранения уязвимостей (определение корректности устранения уязвимостей и соблюдения сроков)
5.	Разработка предложений по улучшению процесса управления уязвимостями	Определение причин отклонений и неисполнений, разработка на их основе решений по улучшению процесса управления уязвимостями

7.2. В случае выявления в ходе оценки защищенности неизвестных ранее уязвимостей (уязвимостей «нулевого дня») сведения о них рекомендуется направлять в БДУ ФСТЭК России¹².

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

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

¹² Включение неизвестных ранее уязвимостей в БДУ ФСТЭК России осуществляется в соответствии с утвержденным регламентом, размещенным по адресу <https://bdu.fstec.ru/site/regulations>

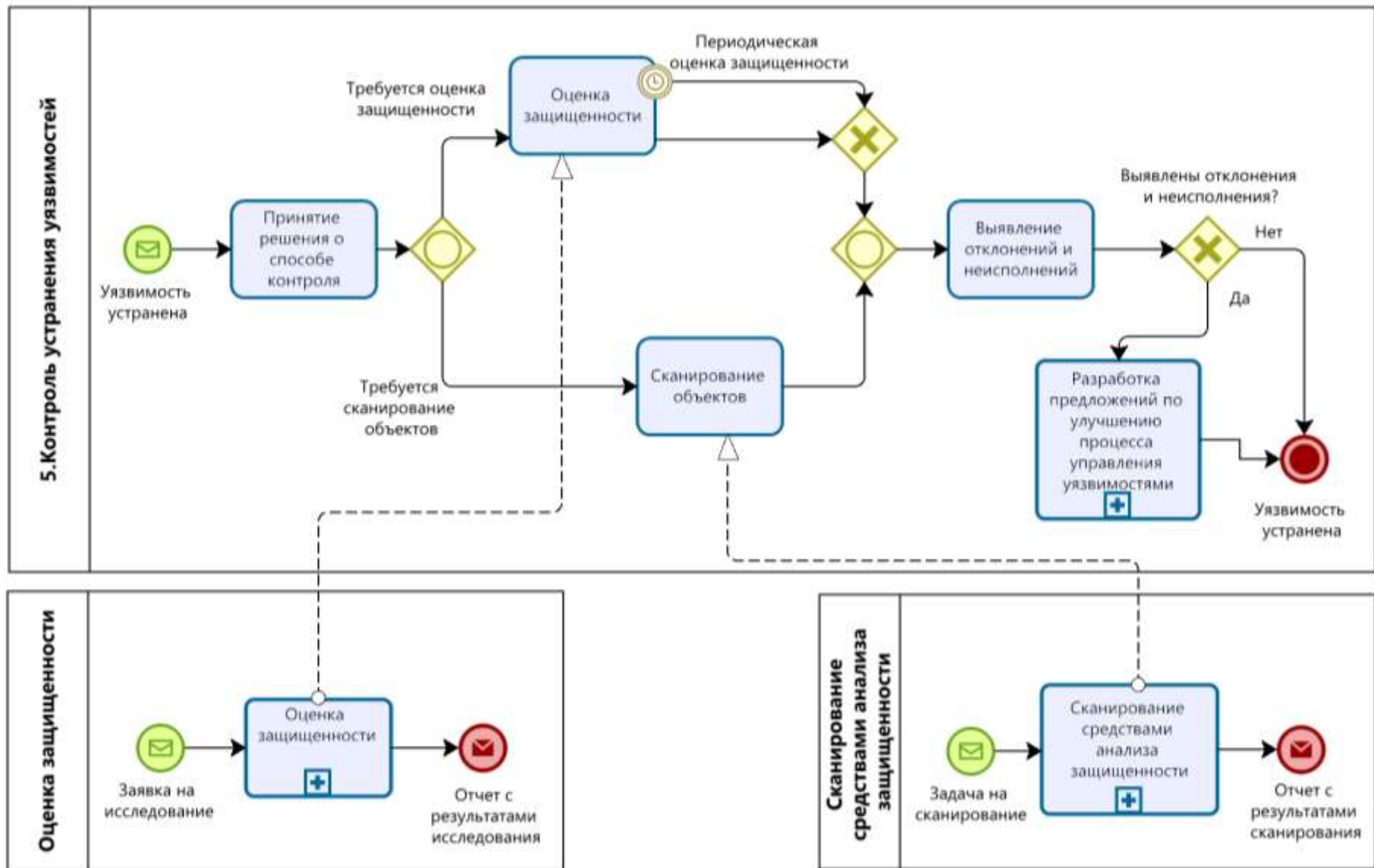


Рисунок 7.1. – Схема этапа контроля устранения уязвимостей

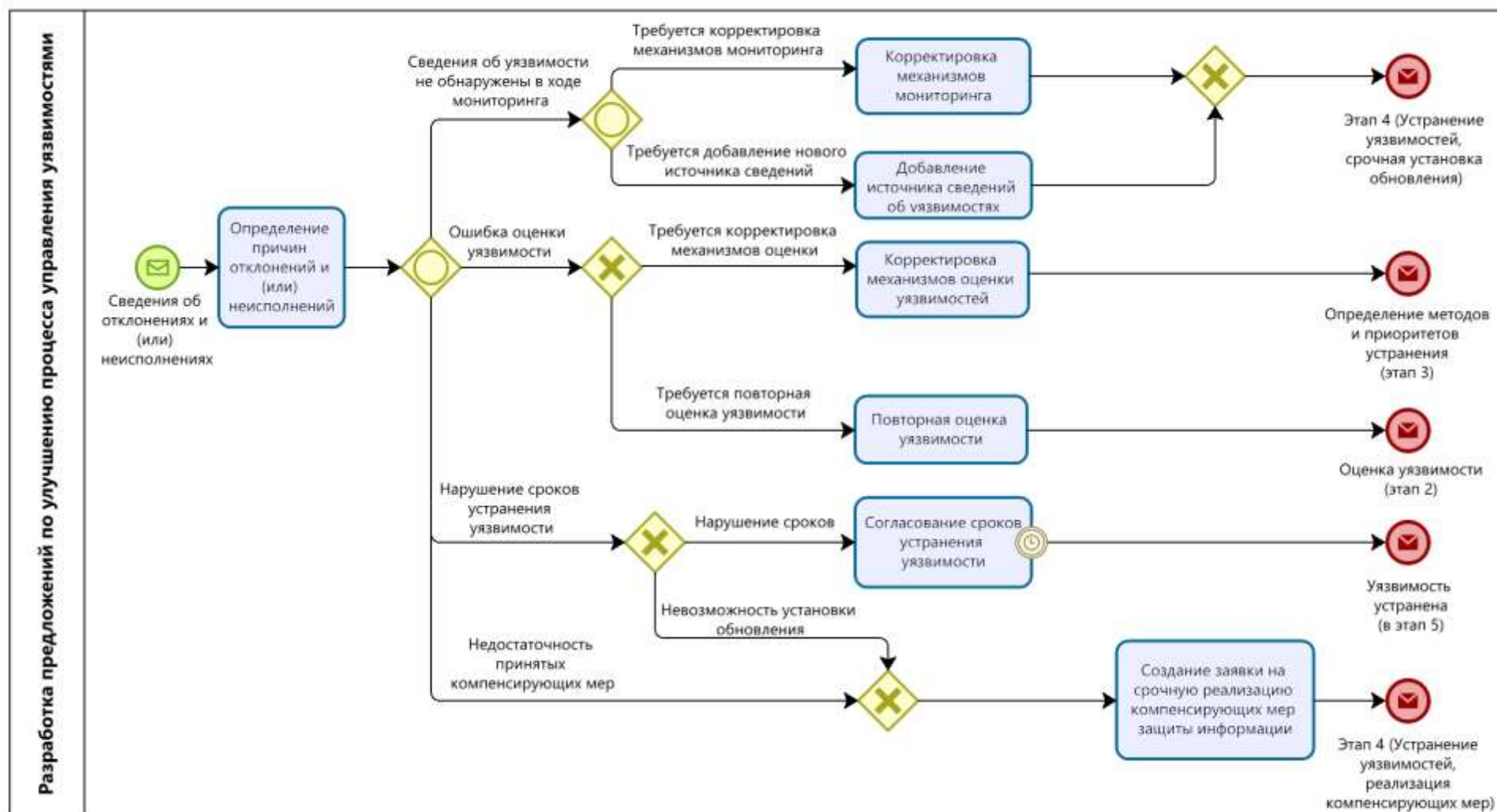


Рисунок 7.2. – Схема подпроцесса разработки предложений по улучшению процесса управления уязвимостями на этапе контроля устранения уязвимостей

В рамках выполнения подпроцесса разработки предложений по улучшению процесса управления уязвимостями выполняются операции, приведенные в таблице 7.2.

Таблица 7.2.

№ п/п	Наименование операции	Описание операции
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 органе (организации)
2.	Корректировка механизмов мониторинга	Внесение изменений в конфигурацию и алгоритмы средств сбора и обработки данных об уязвимостях
3.	Добавление источника сведений об уязвимостях	Поиск и организация мониторинга новых источников сведений об уязвимостях
4.	Корректировка механизмов оценки уязвимостей	Внесение изменений в процедуру оценки уязвимостей
5.	Повторная оценка уязвимости	Повторное определение уровня критичности уязвимости применительно к информационным системам органа (организации). Переход к этапу 2 («Оценка уязвимостей») с дальнейшим выполнением последующих этапов процесса управления уязвимостями
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 этапе 4.
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

7.5. На основе таблиц 7.1 и 7.2. в органе (организации) 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 органа (организации).

Обозначения, применяемые для целей настоящего методического документа

На схемах в настоящем руководстве 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;



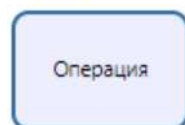
– развилка «или/или» – выбор только одного пути;



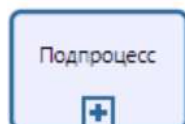
– развилка «и» – выбор всех путей;



– развилка «и/или» – выбор одного или нескольких путей;



– элементарное действие в рамках процесса;



– действие, которое может включать в себя другие действия, развилки и события.