Приложение
к письму Минцифры НСО
10.03.2026 № 539/32-ВН

УТВЕРЖДЕН
приказом
ГАУ НСО «Центр
«Виктория»
от 17.07.2026 № 49-од

РЕГЛАМЕНТ
УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, ОПЕРАТОРОМ КОТОРЫХ ЯВЛЯЕТСЯ
государственное автономное учреждение Новосибирской области «Социально-реабилитационный центр для несовершеннолетних «Виктория»

г. Новосибирск

2026 г.

2 Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент определяет состав и содержание работ по выявлению, анализу и устранению уязвимостей (далее – управление уязвимостями), в программных и программно-аппаратных средствах информационных систем (далее – ИС), функционирующих на основе информационно-телекоммуникационных сетей и информационно-телекоммуникационных инфраструктурах центра обработки данных Правительства Новосибирской области.

Работы по соблюдению настоящего Регламента возлагаются на должностных лиц государственного автономного учреждения Новосибирской области «Социально-реабилитационный центр для несовершеннолетних «Виктория», являющихся ответственными за информационную безопасность, специалистов государственного автономного учреждения Новосибирской области «Социально-реабилитационный центр для несовершеннолетних «Виктория» (далее – Центр), сотрудников подрядных организаций, обслуживающих государственные информационные системы (сегменты государственных информационных систем, иные информационные системы) на основании заключенных договоров с Центром (далее – подрядные организации).

1.2. Основными задачами настоящего Регламента являются:

– формирование единого подхода по организации и внедрению процессов управления уязвимостями;

– организация взаимодействия между структурными подразделениями Центра при реализации процессов управления уязвимостями.

1.3. В Регламенте используются термины и их определения, установленные 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» и иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

1.4. В Регламенте используются обозначения на схемах, приведенные в приложении № 1 к настоящему документу.

2. ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

2.1. Процесс управления уязвимостями (далее – Процесс) включает пять основных этапов (рисунок 1).

Рисунок 1 – Этапы работ по управлению уязвимостями

На этапе мониторинга уязвимостей и оценки их применимости осуществляется поиск уязвимостей на основании данных, получаемых из внешних и внутренних источников.

На этапе оценки уязвимостей определяется уровень критичности уязвимостей.

На этапе определения методов и приоритетов устранения определяется приоритетность устранения уязвимостей и осуществляется выбор методов их устранения: обновление и (или) компенсирующие меры.

На этапе устранения уязвимостей осуществляются мероприятия, направленные на нейтрализацию выявленных уязвимостей.

На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о Процессе и его результатах, а также принятие решений по улучшению Процесса.

2.2. Процесс организуется таким образом, что на каждом этапе обрабатываются сведения о новых, а также ранее выявленных уязвимостях, актуализированные по результатам мониторинга.

Рисунок 1 – Этапы работ по управлению уязвимостями

На этапе мониторинга уязвимостей и оценки их применимости осуществляется поиск уязвимостей на основании данных, получаемых из внешних и внутренних источников.

На этапе оценки уязвимостей определяется уровень критичности уязвимостей.

На этапе определения методов и приоритетов устранения определяется приоритетность устранения уязвимостей и осуществляется выбор методов их устранения: обновление и (или) компенсирующие меры.

На этапе устранения уязвимостей осуществляются мероприятия, направленные на нейтрализацию выявленных уязвимостей.

На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о Процессе и его результатах, а также принятие решений по улучшению Процесса.

2.2. Процесс организуется таким образом, что на каждом этапе обрабатываются сведения о новых, а также ранее выявленных уязвимостях, актуализированные по результатам мониторинга.

2.3. Процесс связан с другими процессами:

– мониторингом информационной безопасности (ИБ) – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей;

оценкой защищенности – экспертным анализом применимости уязвимости к инфраструктуре организации;

оценкой угроз безопасности информации (далее – угрозы) – определение угроз, реализация (возникновение) которых возможна в инфраструктуре организации;

управлением конфигурацией – управление конфигурацией информационной системы (включая изменение состава и конфигураций программного обеспечения (далее – ПО) и программно-аппаратных средств);

управлением обновлениями – приобретение, анализ и развертывание обновлений ПО;

применением компенсирующих мер защиты – 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.

Максимальная типовая схема Процесса представлена на рисунке 2.

Участники Процесса и выполняемые ими операции:

а) Центр, осуществляющие функции по обеспечению информационной безопасности: инженер - программист.

Подрядные организации, осуществляющие деятельность по обеспечению внедрения, функционирования и развития информационных систем:

По решению специалиста Центра, ответственного за обеспечение информационной безопасности в Процессе могут быть задействованы другие подразделения и организации.

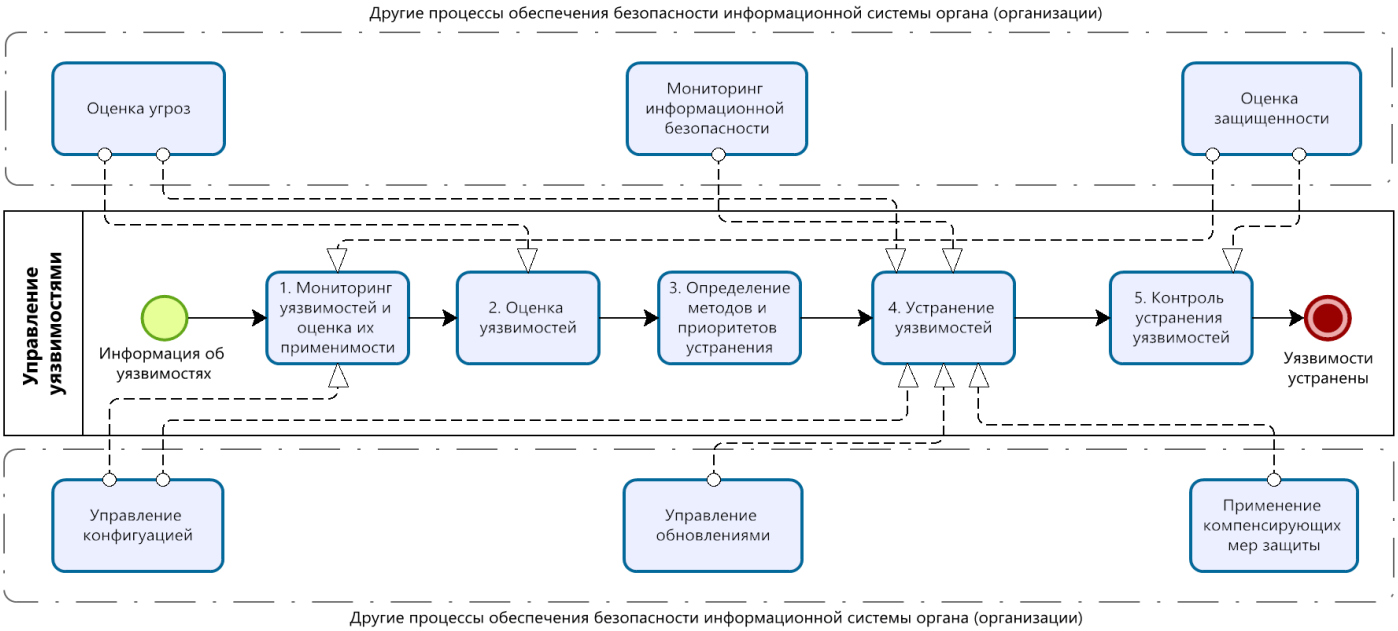


Рисунок 2 – Схема Процесса

3. МОНИТОРИНГ УЯЗВИМОСТЕЙ И ОЦЕНКА ИХ ПРИМЕНИМОСТИ

3.1. На этапе мониторинга уязвимостей и оценки их применимости осуществляется поиск уязвимостей на основании данных из следующих источников:

а) внутренние источники:

- сведения о составе и архитектуре информационной системы, полученные по результатам инвентаризации и (или) приведенные в документации;

- результаты оценки угроз;

- результаты оценки защищенности информационной системы.

б) база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации (далее – БДУ) ФСТЭК России (bdu.fstec.ru);

в) внешние источники:

- базы данных, содержащие сведения об известных уязвимостях;
- официальные информационные ресурсы разработчиков ПО и ПАС и исследователей в области информационной безопасности.

Приведенные источники данные могут уточняться или дополняться с учетом особенностей области деятельности органа (организации).

Максимальная типовая схема этапа мониторинга уязвимостей и оценки их применимости представлена на рисунке 2.

На этапе мониторинга уязвимостей и оценки их применимости выполняются операции, приведенные в таблице 2.

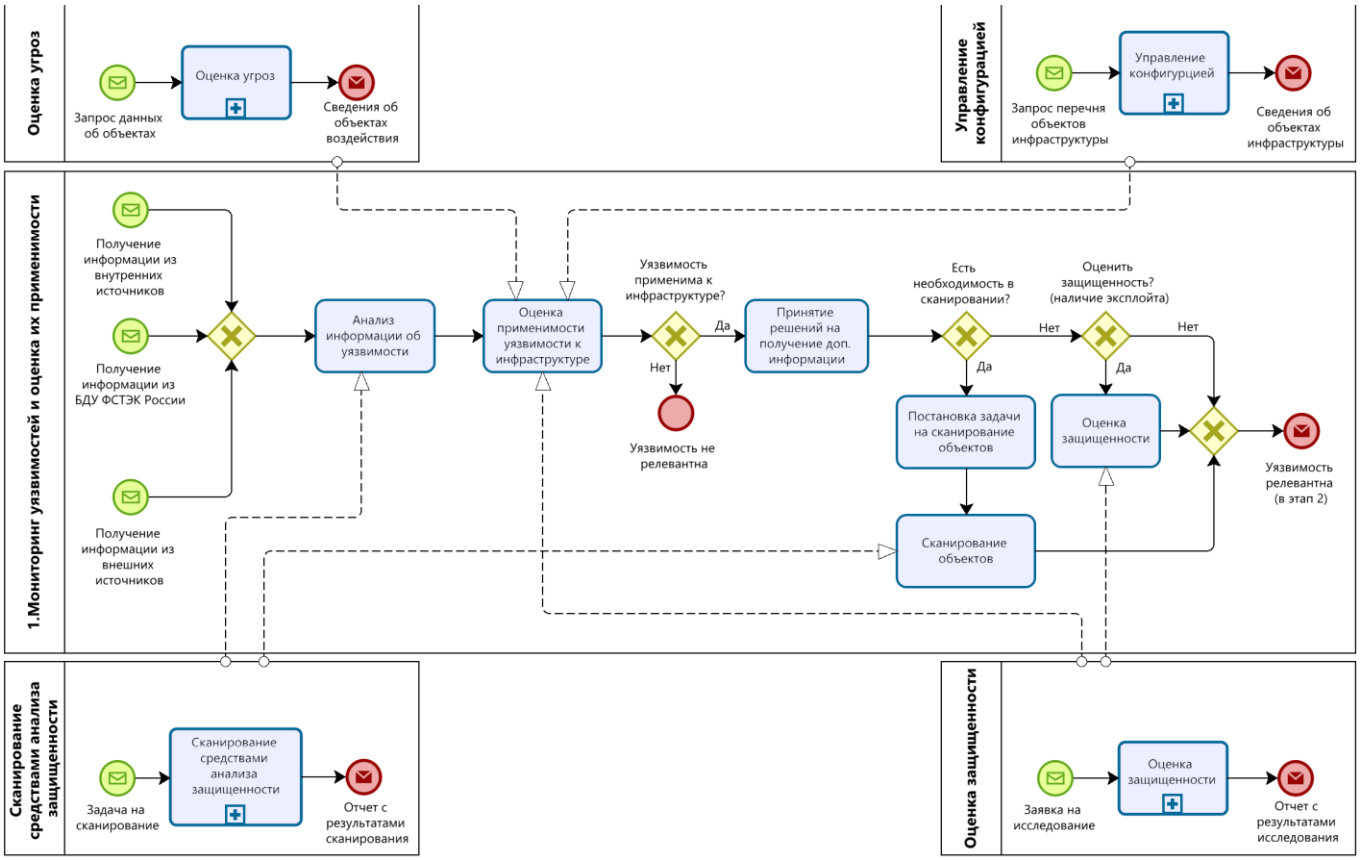


Рисунок 2 – Схема этапа мониторинга уязвимостей и оценки их применимости

Таблица 2 – операции этапа мониторинга уязвимостей и оценки их применимости

№п/п	Наименование операции	Описание операции
1.	Получение информации о новых уязвимостях	Получение информации о появлении новых уязвимостей из БДУ ФСТЭК России (bdu.fstec.ru) и/или получение информационного письма по реализации организационных и технических мер от ФСТЭК России.
2.	Создание заявки на устранение уязвимости	Заявка на выявление и дальнейшее устранение новых уязвимостей
3.	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к инфраструктуре органа (организации). Осуществляется агрегирование и корреляция собираемых данных об уязвимостях
4.	Оценка применимости уязвимости	На основе информации об объектах информационной системы и их состоянии определяется применимость уязвимости к инфраструктуре органа (организации) с целью определения уязвимостей, не требующих дальнейшей обработки. Оценка применимости уязвимостей производится:

		на основе анализа данных об инфраструктуре информационных технологий (ИТ-инфраструктуре), полученных из систем учета класса CMDB[3] 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)
5.	Принятие решений на получение дополнительной информации	Запрос дополнительной информации об уязвимости (сканирование объектов либо оценка защищенности), если имеющихся данных недостаточно для принятия решений
6.	Постановка задачи на сканирование объектов	Запрос на внеплановое сканирование объектов в случае недостаточности либо неактуальности имеющихся данных, а также в случае получения информации об уязвимости после последнего сканирования
7.	Сканирование объектов	Поиск уязвимостей и недостатков с помощью автоматизированных средств анализа защищенности. Выбор объектов и времени сканирования, уведомление заинтересованных лиц о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
8.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к объекту воздействия. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в инфраструктуре органа (организации) с использованием PoC[4] или средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия)

CMDB (англ. Configuration Management Database) – база данных управления конфигурацией4
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 инфраструктуре органа (организации).

4.2. На этапе оценки уязвимостей выполняются операции, приведенные в таблице 3.

Таблица 3 – операции этапа оценки уязвимостей

№п/п	Наименование операции	Описание операции
1.	Получение информации об объектах системы, подверженных уязвимости	Получение выборки объектов, подверженных уязвимости (автоматически или вручную)
2.	Определение уровня опасности уязвимости	Расчет базовой, контекстной и временной метрик по методике CVSS с использованием калькулятора CVSS [5]V3 или V3.1, размещенного в БДУ ФСТЭК России[6]
3.	Определение влияния на систему	Определение влияния уязвимого компонента на защищенность системы 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.
4.	Расчет критичности уязвимостей	Получение значений уровней критичности обнаруженных уязвимостей

Операции 2-4 выполняются в соответствии с Методикой оценки уровня критичности программных и программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.

4.3. Максимальная типовая схема этапа оценки уязвимостей представлена на рисунке 3.

5 CVSS (англ. Common Vulnerability Scoring System) – общая система оценки уязвимостей (адрес:https://www.first.org/cvss)6 адреса: https://bdu.fstec.ru/calc3, https://bdu.fstec.ru/calc31

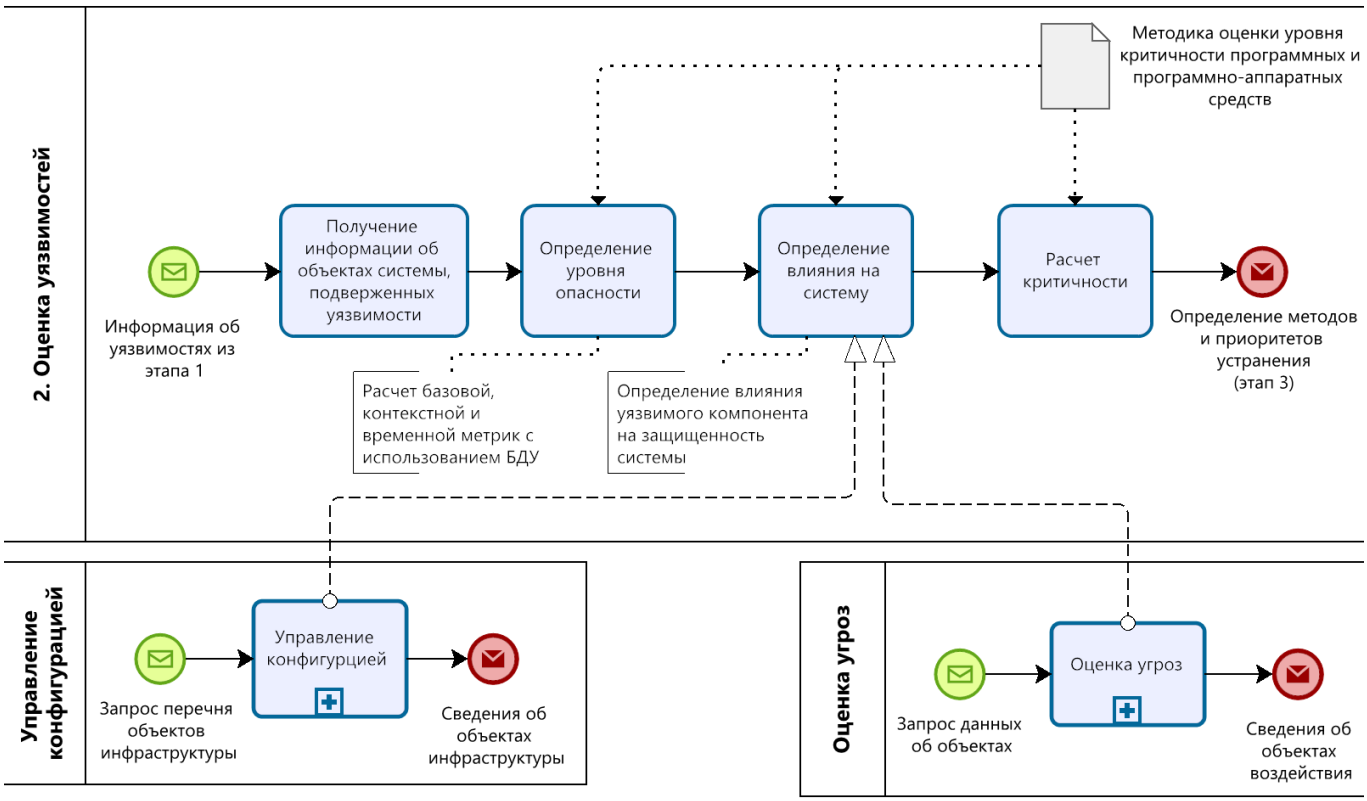


Рисунок 3 – Схема этапа оценки уязвимостей

5. ОПРЕДЕЛЕНИЕ МЕТОДОВ И ПРИОРИТЕТОВ УСТРАНЕНИЯ

5.1. На этапе определения методов и приоритетов устранения решаются задачи:

– определения приоритетности устранения уязвимостей;

– выбора методов устранения уязвимостей: обновление или компенсирующие меры (организационные меры защиты, настройка СЗИ, мониторинг событий безопасности, внесение изменений в ИТ-инфраструктуру).

На этапе определения методов и приоритетов устранения выполняются операции, приведенные в таблице 4.

Таблица 4 – операции этапа определения методов и приоритетов устранения

п/п	Наименование операции	Описание операции
	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей (этап 4)
	Определение методов устранения уязвимостей	Выбор способа устранения уязвимости: установка обновления или применение компенсирующих мер
	Принятие решения о срочной установке обновлений	При обнаружении критической уязвимости может быть принято решение о срочной установке обновления
	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование в подрядные организации
	Принятие решения о срочной реализации компенсирующих мер	При обнаружении критической уязвимости может быть принято решение о срочной реализации компенсирующих мер в качестве временного решения до установки обновления
	Создание заявки на установку обновления	Заявка создается в случае, если определено, что установка обновления для устранения данной уязвимости не запланирована
	Создание заявки на реализацию компенсирующих мер	Заявка на реализацию компенсирующих мер формируется при отсутствии возможности установки обновления, а также в случае необходимости принятия мер до устранения уязвимости

5.2. Информация для организации устранения уязвимостей направляется по электронной почте или посредством использования системы электронного документооборота и делопроизводства (СЭДД).

5.3. Максимальная типовая схема этапа определения методов и приоритетов устранения представлена на рисунке 4.

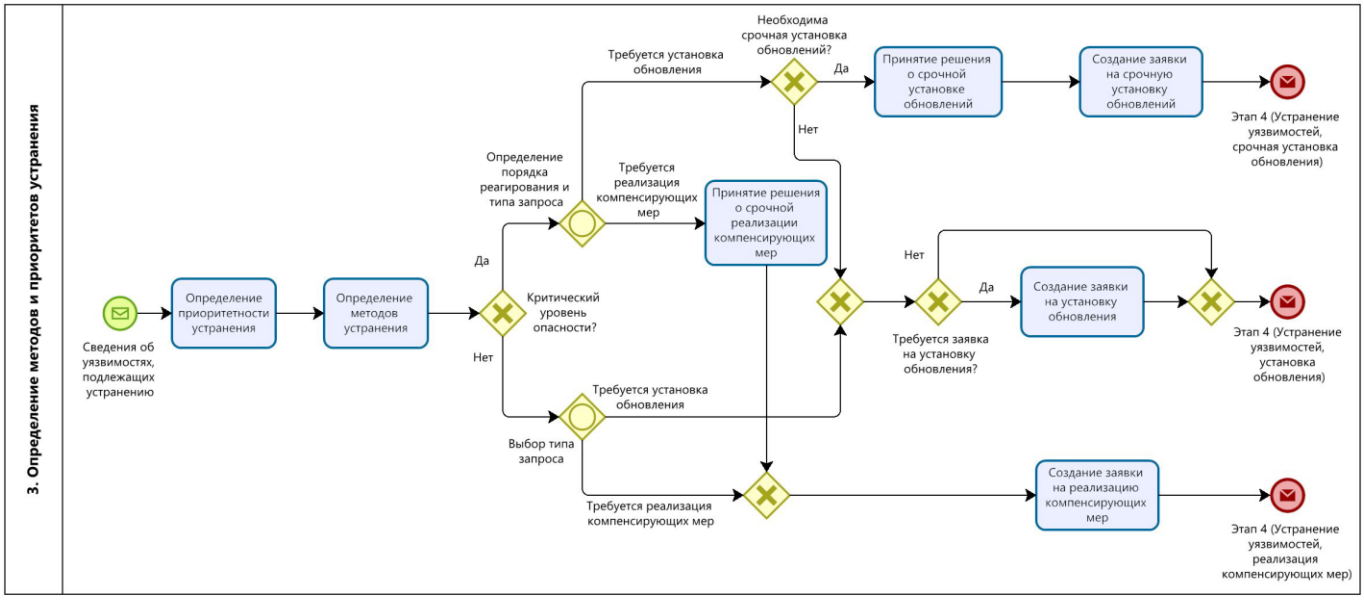


Рисунок 4 – Схема этапа определения методов и приоритетов устранения

6. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

6.1. На этапе устранения уязвимостей нейтрализуются уязвимости, выявленные на этапе мониторинга уязвимостей. При этом, выполняются операции, представленные в таблице 5.

Таблица 5 – операции этапа устранения и нейтрализации уязвимости

№п/п	Наименование операции	Описание операции
1.	Согласование установки с подрядными организациями	Срочная установка обновлений предварительно согласовывается с подрядными организациями
2.	Тестирование обновления	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недекларированные возможности)
3.	Установка обновления в тестовом сегменте	Установка обновлений на выбранном 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
5.	Установка обновления	Распространение обновления на узлы системы
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	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

6.2. Максимальная типовая схема этапа устранения уязвимостей представлена на рисунке 5.

6.3. Максимальная типовая схема подпроцесса разработки и реализация компенсирующих мер защиты на этапе устранения уязвимостей представлена на рисунке 6.

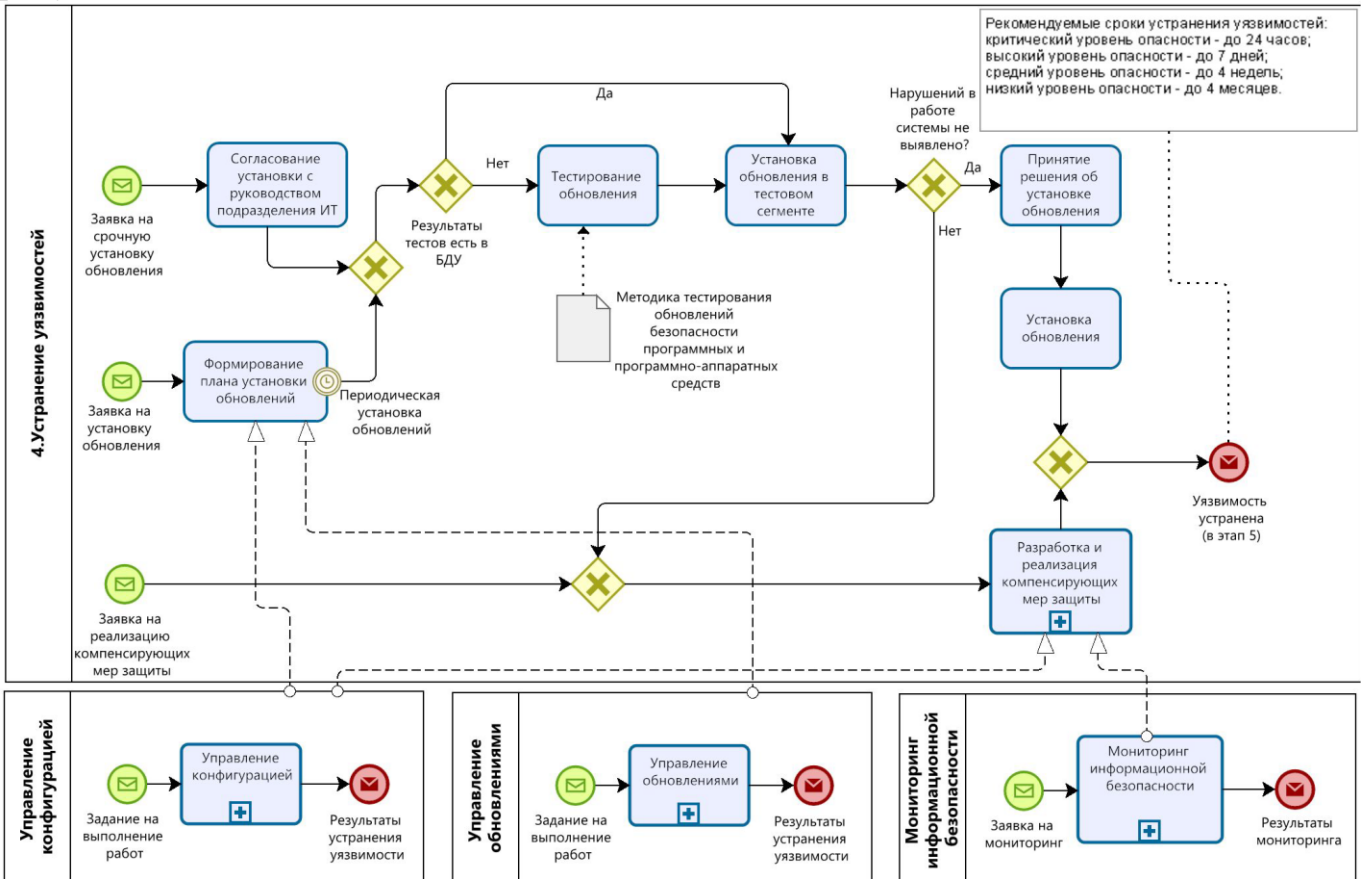


Рисунок 5 – Схема этапа устранения уязвимостей

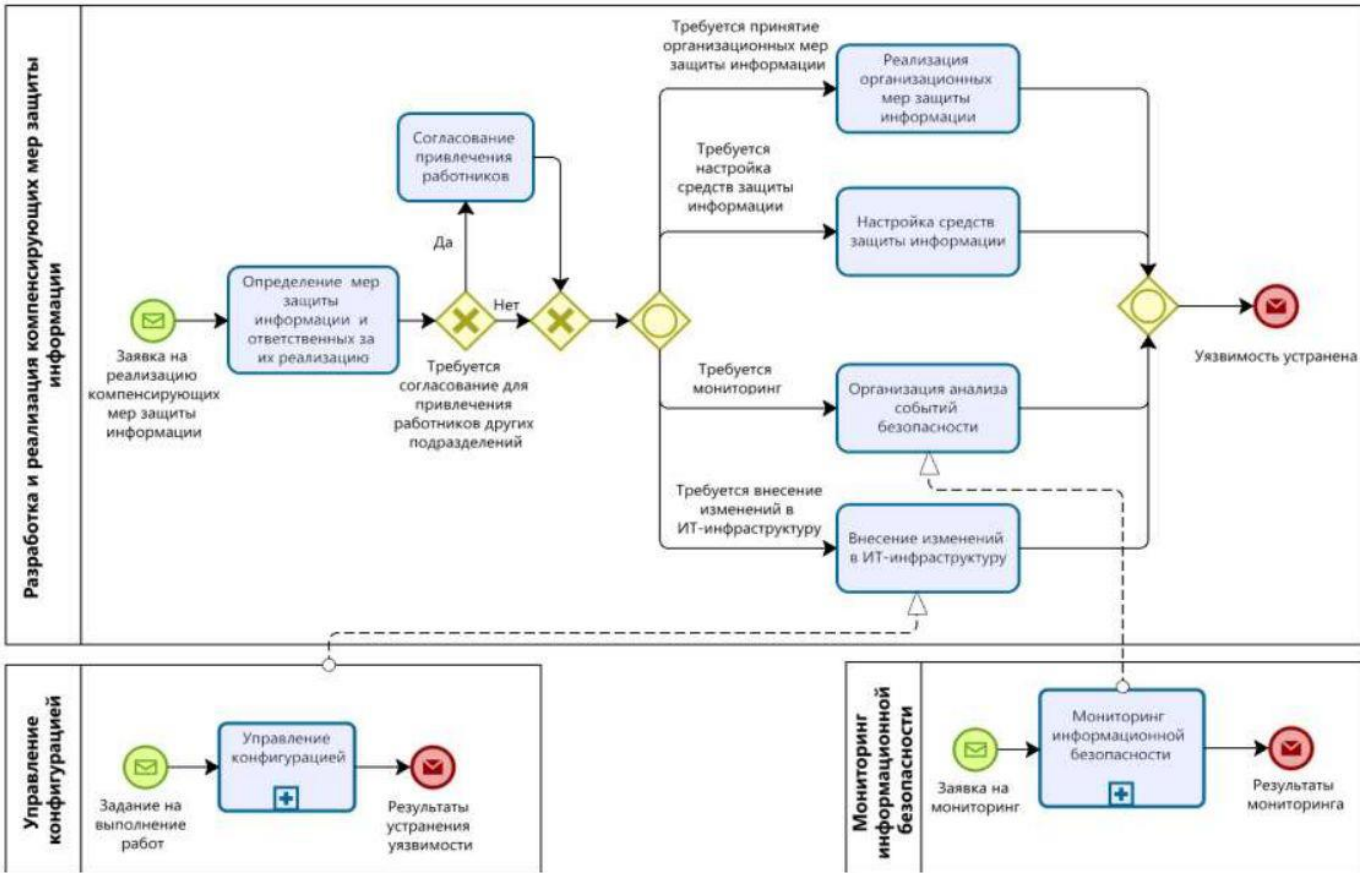


Рисунок 6 – Схема подпроцесса разработки и реализация компенсирующих мер защиты на этапе устранения уязвимостей

В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты выполняются операции, приведенные в таблице 6.

Таблица 6 – операции этапа подпроцесса разработки и реализации компенсирующих мер защиты.

№п/п	Наименование операции	Описание операции
1.	Определение мер защиты и ответственных за их реализацию	Определение компенсирующих мер, необходимых для нейтрализации уязвимости либо снижения возможных негативных последствий от ее эксплуатации. В ходе выполнения данной операции должны быть определены сотрудники, участие которых необходимо для реализации выбранных компенсирующих мер защиты
2.	Согласование привлечения сотрудников	В случае необходимости привлечения сотрудников других подразделений для реализации компенсирующих мер сотрудник Центра, ответственный за обеспечение информационной безопасности, согласует их привлечение с руководителями соответствующих подразделений
3.	Реализация организационных мер защиты	Реализация таких организационных мер защиты информации, как: ограничение использования ИТ-инфраструктуры; организация режима охраны (в частности, ограничение доступа к техническим средствам); информирование и обучение персонала органа (организации).

4.	Настройка СЗИ	Выполнение работ по настройке СЗИ
5.	Организация мониторинга 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 ПАС и ПО (в том числе, удаление ПО)

7. КОНТРОЛЬ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

7.1. На этапе контроля и устранения уязвимостей осуществляется сбор и обработка данных о Процессе и его результатах, принятие оперативных решений и их доведение до руководства для принятия управленческих решений (в том числе по улучшению Процесса).

Типовая максимальная схема этапа контроля и устранения уязвимостей представлена на рисунке 7.

На этапе контроля устранения уязвимостей выполняются операции, приведенные в таблице 7.

Таблица 7 – операции по контролю устранения уязвимостей

№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 лиц о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
3.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к объекту воздействия. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в инфраструктуре 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 информационной системе 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	Определение причин отклонений и неисполнений, разработка на их основе решений по улучшению Процесса

7.2. Типовая максимальная схема подпроцесса разработки предложений по улучшению Процесса на этапе контроля устранения уязвимостей представлена на рисунке 8[7].

[7] Представлена схема с основными причинами отклонений и неисполнений операций Процесса

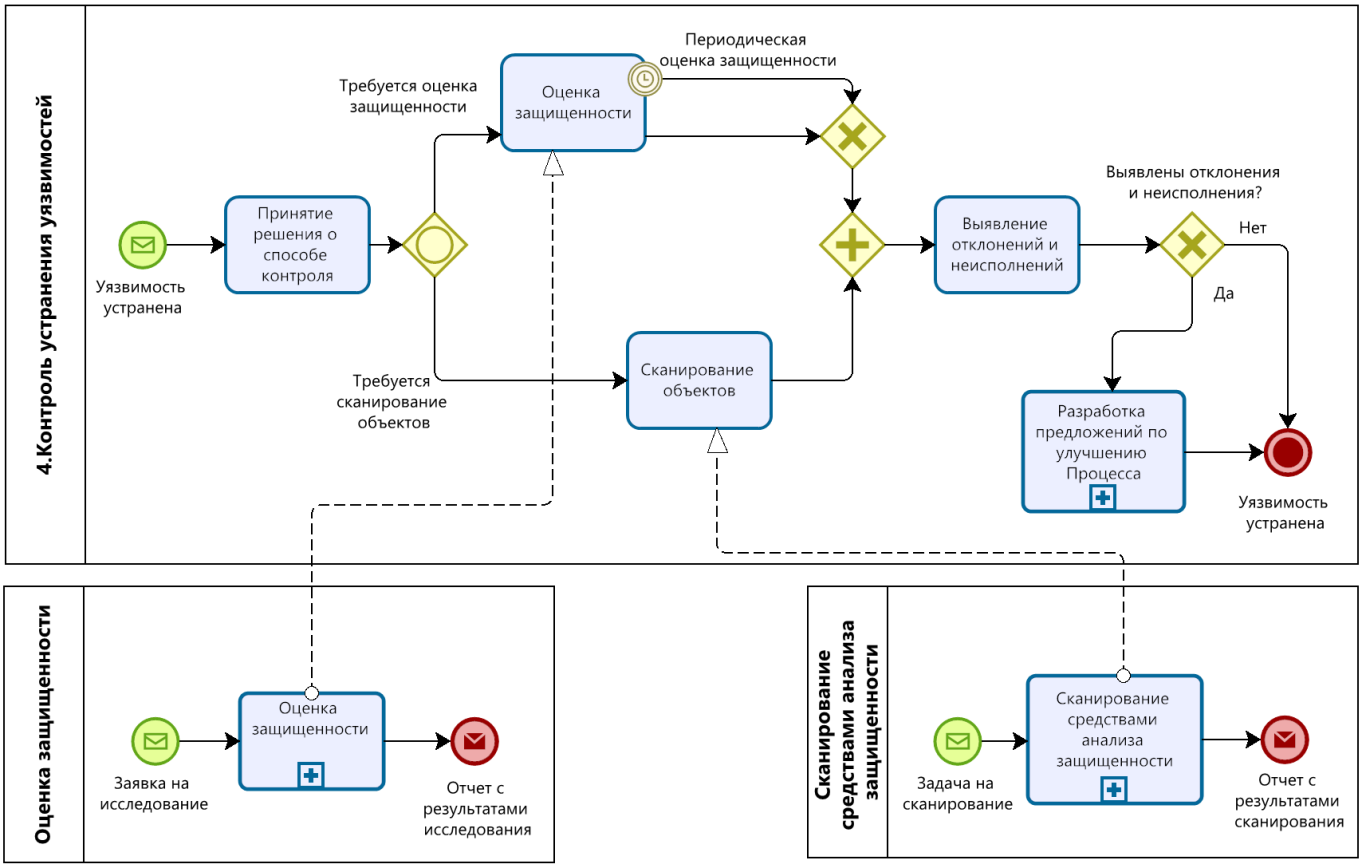


Рисунок 7 – Схема этапа контроля устранения уязвимостей

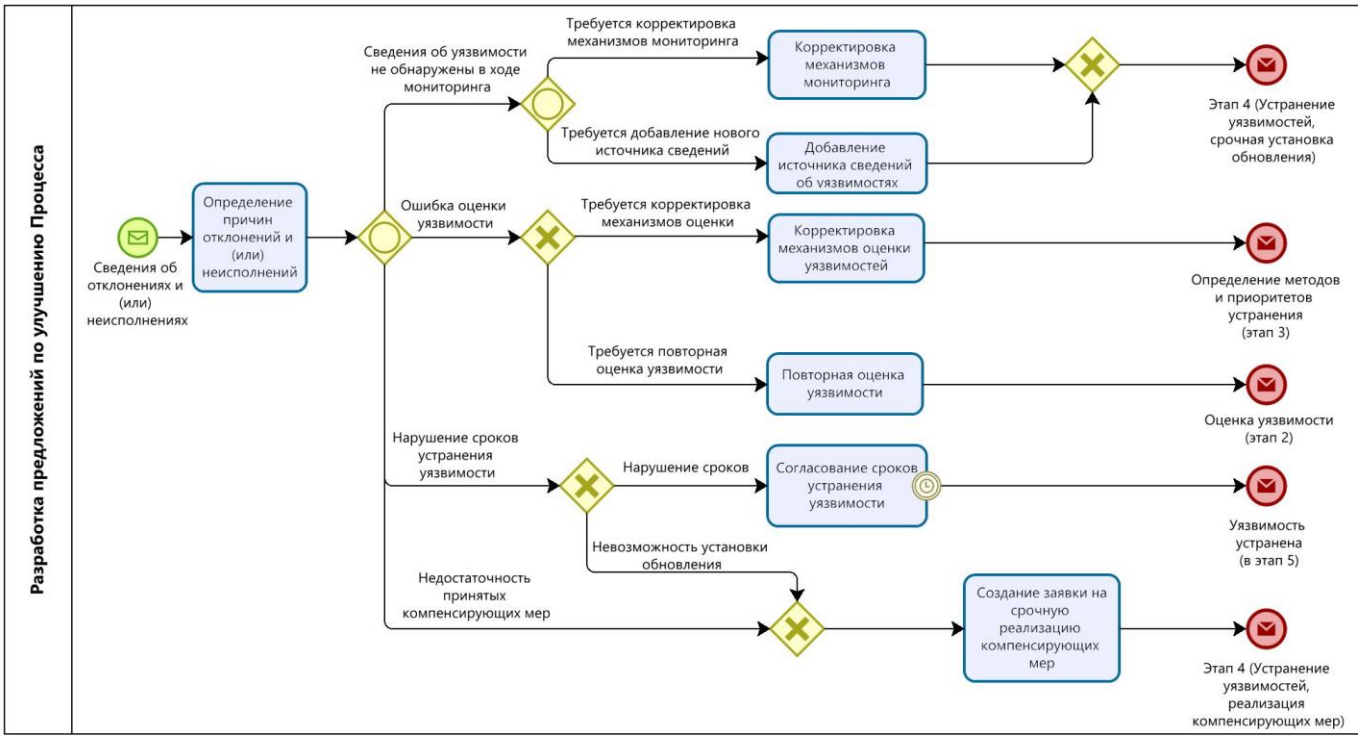


Рисунок 8 – Схема подпроцесса разработки предложений по улучшению Процесса на этапе контроля устранения уязвимостей

В рамках выполнения подпроцесса разработки предложений по улучшению Процесса выполняются операции, приведенные в таблице 8.

Таблица 8 – процесс выполнения операций

№п/п	Наименование операции	Описание операции
1.	Определение причин отклонений и (или) неисполнений	Определение причин отклонений и неисполнений операций Процесса. Возможными причинами являются: необнаружение сведений об уязвимости в ходе мониторинга; ошибки оценки уязвимостей; нарушения сроков устранения уязвимостей; недостаточность принятых компенсирующих мер.
2.	Корректировка механизмов мониторинга	Внесение изменений в конфигурацию и алгоритмы средств мониторинга уязвимостей
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 инфраструктуре органа (организации)
6.	Согласование сроков устранения уязвимости	В случае нарушения сроков устранения уязвимостей согласуются новые сроки установки обновления (согласование с подрядными организациями), либо сроки реализации компенсирующих мер защиты (согласование с ответственными лицами, определенными на этапе 4). Компенсирующие меры реализуются, как правило, в случае невозможности установки обновления
7.	Создание заявки на срочную реализацию компенсирующих мер	Заявка на реализацию компенсирующих мер формируется при отсутствии возможности установки обновления либо в случае недостаточности уже принятых компенсирующих мер защиты

Приложение № 1
к Регламенту управления
уязвимостями в государственных
информационных системах,
оператором, которых является Центр

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, показывает с чего начинается процесс;

– начальное событие, связанное с получением сообщений (данных);

– промежуточное событие, связанное с истечением определенного временного интервала;

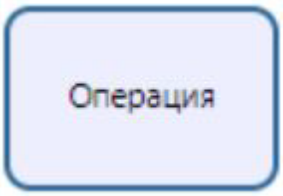
– окончание процесса или подпроцесса;

– окончание процесса или подпроцесса, связанное с отправкой сообщений (данных);

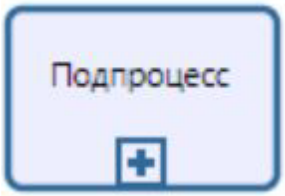
– завершение всех процессов и подпроцессов;

– развилка «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.