ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ
(РОСТЕХНАДЗОР)

П Р И К А З

05 сентября 2023 г. № 325

Москва

Об утверждении регламента по выявлению, анализу и устранению уязвимостей в информационных системах, эксплуатируемых в Федеральной службе по экологическому, технологическому и атомному надзору

В целях усиления обеспечения безопасности информации и повышения защищенности информационных систем в Федеральной службе по экологическому, технологическому и атомному надзору п р и к а з ы в а ю:

1. Утвердить Регламент по выявлению, анализу и устранению уязвимостей в информационных системах, эксплуатируемых в Федеральной службе по экологическому, технологическому и атомному надзору, согласно приложению к настоящему приказу.

2. Возложить реализацию работ по управлению уязвимостями в информационных системах, эксплуатируемых в Федеральной службе по экологическому, технологическому и атомному надзору, на Управление информатизации (С.А. Корчивой).

3. Координацию деятельности по управлению уязвимостями в информационных системах, эксплуатируемых в Федеральной службе по экологическому, технологическому и атомному надзору и контроль за исполнением настоящего приказа возложить на заместителя руководителя А.В. Ферапонтова.

Руководитель А.В. Трембицкий

Приложение
к приказу Федеральной службы
по экологическому, технологическому
и атомному надзору
от 05 сентября 2023 г. № 325

РЕГЛАМЕНТ ПО ВЫЯВЛЕНИЮ, АНАЛИЗУ И УСТРАНЕНИЮ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, ЭКСПЛУАТИРУЕМЫХ В ФЕДЕРАЛЬНОЙ СЛУЖБЕ ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Регламент по выявлению, анализу и устранению уязвимостей в информационных системах, эксплуатируемых в Федеральной службе по экологическому, технологическому и атомному надзору (далее – Регламент), регулирует порядок организации работ по выявлению, анализу и устранению уязвимостей (далее – управление уязвимостями) в Ростехнадзоре.

1.1. Регламент определяет состав и содержание работ по управлению уязвимостями, выявленными 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).

1.2. Целью организации процесса управления уязвимостями в Ростехнадзоре является снижение рисков информационной безопасности от реализации угроз, обусловленных уязвимостями в информационных системах (далее – ИС) Ростехнадзора, с приоритетом предотвращения уязвимостей на периметре сетей Ростехнадзора.

1.3. Настоящий Регламент разработан в соответствии с Руководством по организации процесса управления уязвимостями в органе (организации), утвержденным ФСТЭК России от 17 мая 2023 г., и в соответствии

с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 г.

1.4. Настоящий Регламент устанавливает принципы и механизмы поиска, оценки, классификации уязвимостей, а также их устранения или минимизации последствий, определяет относящиеся к процессу функции, роли, полномочия и ответственность подразделений в Ростехнадзоре.

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

2. ЭТАПЫ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

2.1. В ИС должно осуществляться выявление следующих типов уязвимостей:

– недостатки и(или) ошибки программного обеспечения (далее – ПО) ИС и ее системы защиты информации;

– недостатки аппаратных средств ИС, в том числе аппаратных средств защиты информации;

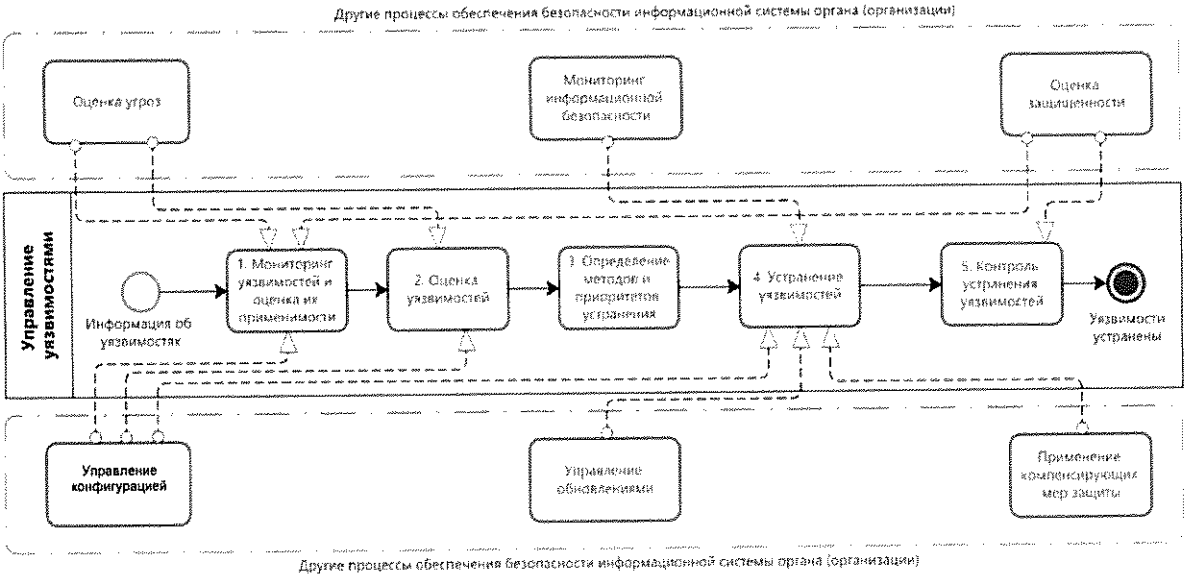
– организационно-технические недостатки.

2.2. Непосредственными участниками процесса управления уязвимостями ИС являются администратор безопасности и системные администраторы ИС.

2.3. Процесс управления уязвимостями состоит из пяти основных этапов, которые обеспечивают решение задач процесса, контроль за процессом, его результатами (рис. 1).

2.4. На основе таблиц Регламента по этапам процесса управления уязвимостями в Ростехнадзоре должны разрабатываться детальные описания операций, включающие наименования операций, описание операций, исполнителей, продолжительность, входные и выходные данные. Детальное описание операций включается в организационно-распорядительные документы по защите информации Ростехнадзора.

2.5. Процесс управления уязвимостями связан с процессами управления конфигурацией, управления обновлениями, оценки угроз. Данные процессы в Регламенте не рассматриваются.



Этапы процесса управления уязвимостями Рис. 1

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

Процесс управления уязвимостями организуется для всех ИС Ростехнадзора и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и объектах ИС. При изменении

статуса уязвимостей (применимость к ИС, наличие исправлений, критичность) должны корректироваться способы их устранения.

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

– 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 ИС Ростехнадзора;

– оценка угроз – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в ИС Ростехнадзора;

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

– управление обновлениями – приобретение, анализ и развертывание обновлений ПО в Ростехнадзоре;

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

3. МОНИТОРИНГ, АНАЛИЗ УЯЗВИМОСТЕЙ И ОЦЕНКИ ИХ ПРИМЕНИМОСТИ

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

а) внутренние источники:

– системы управления информационной инфраструктурой

(далее – ИТ-инфраструктура);

– базы данных управления конфигурациями;

– документация на ИС;

– электронные базы знаний органов (организаций);

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 Ростехнадзора.

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

Таблица 3.1

№	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 ИС Ростехнадзора. Агрегирование и корреляция собираемых данных об уязвимостях.
2	Оценка применимости уязвимости	На основе информации об объектах ИС и их состоянии определяется применимость уязвимости к ИС Ростехнадзора с целью определения уязвимостей, не требующих дальнейшей обработки (нерелевантных 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 «Оценка угроз»; по результатам оценки защищенности
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 ИС 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 ИС. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в ИС Ростехнадзора с использованием средства эксплуатации уязвимости, в том числе в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к ИС в обход ее системы защиты информации

4. ОЦЕНКА УЯЗВИМОСТЕЙ

4.1. На этапе оценки уязвимостей определяется уровень критичности уязвимостей применительно к ИС Ростехнадзора. Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения администраторами безопасности о необходимости устранения уязвимостей, выявленных в программных, программно-аппаратных средствах по результатам анализа уязвимостей в ИС.

Исходными данными для определения критичности уязвимостей являются:

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

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

– сведения о составе и архитектуре ИС, полученные по результатам их инвентаризации и (или) приведенные в документации на ИС;

– результаты контроля защищенности ИС, проведенные оператором.

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

4.2. Оценка уровня критичности уязвимостей программных,

программно-аппаратных средств проводится администраторами безопасности.

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

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

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

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

Для расчета итогового уровня критичности применяется Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденная ФСТЭК России от 28 октября 2022 г.

5. ОПРЕДЕЛЕНИЕ МЕТОДОВ И ПРИОРИТЕТОВ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

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

На этапе определения методов и приоритетов устранения уязвимостей решаются следующие задачи:

– определение приоритетности устранения уязвимостей;

– выбор методов устранения уязвимостей:

– обновление ПО 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

№	Наименование операции	Описание операции
1	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей
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 ИС, подверженных уязвимости
4	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование начальнику Управления информатизации
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

6. УСТРАНЕНИЕ УЯЗВИМОМОСТЕЙ

6.1. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленных на этапе мониторинга. При этом выполняются операции, представленные в таблице 6.1.

Таблица 6.1

№	Наименование операции	Описание операции
1	Согласование установки с руководством Управления информатизации	Срочная установка обновлений ПО предварительно согласовывается с руководством Управления информатизации

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

Тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с данным Регламентом по решению Ростехнадзора в случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России.

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

Рекомендуемые сроки устранения уязвимостей:

– критический уровень опасности – до 24 часов;

– высокий уровень опасности – до 7 дней;

– средний уровень опасности – до 4 недель;

– низкий уровень опасности – до 4 месяцев.

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

Таблица 6.2

№	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)

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

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

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

могут являться:

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

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

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

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

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

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 Ростехнадзора для принятия решений по улучшению процесса управления уязвимостями. На этапе контроля устранения уязвимостей выполняются операции, приведенные в таблице 7.1.

Таблица 7.1

№	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 России.

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

Таблица 7.2

№	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 Ростехнадзоре
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 ИС Ростехнадзора. Переход к «Оценке 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
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