ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ
МЕНЗЕЛИНСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА
РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ
МИНЗӘЛӘ
МУНИЦИПАЛЬ РАЙОНЫ
БАШКАРМА КОМИТЕТЫ

ПОСТАНОВЛЕНИЕ 24.07.2023 г.Мензелинск **КАРАР** № 224

Об утверждении регламента по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в органах местного самоуправления Мензелинского муниципального района Республики Татарстан, регламента по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения в органах местного самоуправления Мензелинского муниципального района Республики Татарстан

В целях усиления обеспечения безопасности информации и повышения защищенности информационных систем в органах местного самоуправления Мензелинского муниципального района Республики Татарстан, в соответствии с методическими документами ФСТЭК России,

ПОСТАНОВЛЯЮ:

1. Утвердить Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в органах местного самоуправления Мензелинского муниципального района Республики Татарстан (Приложение № 1); Регламент по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения в органах местного самоуправления Мензелинского муниципального района Республики Татарстан (Приложение № 2);
2. Настоящее постановление подлежит официальному опубликованию.
3. Контроль за исполнением настоящего постановления возложить на заместителя руководителя исполнительного комитета Мензелинского муниципального района Гатину А.Г.

Руководитель М.Р. Каримов

Приложение №1
к Постановлению
Руководителя исполнительного
комитета Мензелинского
муниципального района
от 24. 07. 2023 года № 224

РЕГЛАМЕНТ ПО ВЫЯВЛЕНИЮ, АНАЛИЗУ И УСТРАНЕНИЮ КРИТИЧНЫХ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЭКСПЛУАТИРУЕМЫХ В ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ ВЕРХНЕУСЛОНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЕСПУБЛИКИ ТАТАРСТАН

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах (далее – ИС) эксплуатируемых в органе, организации (далее – 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.

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

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

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

Целями регламента являются:

– координация деятельности исполнительных органов государственной власти Республики Татарстан и органов местного самоуправления в Республике Татарстан по выявлению, анализу и устранению критичных уязвимостей в ИС;

– создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования органов (организаций);

– организация взаимодействия между структурными подразделениями органов (организаций) по вопросам устранения уязвимостей.

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

2.1. В ИС должно осуществляться выявление следующих типов уязвимостей:

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

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

– организационно-технические недостатки.

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

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

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

Процесс управления уязвимостями связан с другими процессами и процедурами деятельности 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 ИС органа (организации);

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

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

– 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 ИС взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их применения.

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

Исходными данными для определения критичности уязвимостей являются:

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

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

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

– результаты контроля защищенности информационных систем, проведенные оператором.

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

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

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

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

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

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

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

На этапе анализа уязвимостей определяется уровень критичности уязвимостей применительно к ИС органа (организации) 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 органа (организации)

На этапе анализа 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
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 системах органа (организации) с использованием средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации)

На основе таблицы 3.1. в 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 ПОРЯДОК УСТРАНЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

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

На этапе определения методов и приоритетов устранения уязвимостей решаются задачи:

– определения приоритетности устранения уязвимостей;

– выбора методов устранения уязвимостей:

– обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

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

Таблица 4.1

№ 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

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).

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

Таблица 4.2

№ 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	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 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 обновления, а также в случае необходимости принятия мер до устранения уязвимости. К компенсирующим мерам защиты информации могут относиться: организационные меры защиты информации, настройка средств защиты информации, анализ событий безопасности, внесение изменений в ИТ-инфраструктуру

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

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

Рекомендуемые сроки устранения уязвимостей:

– критический уровень опасности до 24 часов;

– высокий уровень опасности – до 7 дней;

– средний уровень опасности – до 4 недель;

– низкий уровень опасности – до 4 месяцев.

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

Таблица 4.3.

№ 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))

На основе таблиц 4.2 и 4.3. 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).

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

Выбор компенсирующих мер по защите информации осуществляется оператором с учетом архитектуры и особенностей функционирования ИС, а также

способов эксплуатации уязвимостей программных, программно-аппаратных средств.

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

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

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

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

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

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

Приложение №2
к Постановлению
Руководителя исполнительного комитета
Мензелинского муниципального района
от 24.07.2023 года № 224

РЕГЛАМЕНТ ПО АНАЛИЗУ И УСТАНОВКЕ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий регламент по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения (далее – Регламент) разработан в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств утвержденной ФСТЭК России от 28 октября 2022 г.

1.2. Регламент определяет порядок и содержание работ по тестированию программного обеспечения, в том числе с открытым исходным кодом, предназначенного для устранения уязвимостей программных, программно-аппаратных средств (далее – обновления безопасности), применяемых в информационных системах, информационно-телекоммуникационных сетях, автоматизированных системах управления, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центров обработки данных (далее – информационные системы).

Регламент может быть использован для тестирования иных обновлений программных, программно-аппаратных средств по решению оператора информационной системы.

1.3. Настоящий Регламент подлежит применению операторами информационных систем 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. Устранение уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации обеспечивается в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

1.5. Решение об установке протестированных обновлений безопасности принимается оператором информационной системы с учетом результатов тестирования и оценки рисков нарушения функционирования информационной системы от установки таких обновлений.

1.6. 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. ПОРЯДОК АНАЛИЗА ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2.1. Анализ обновлений безопасности проводится с целью своевременного выявления в них потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недекларированные возможности).

2.2. Анализу подлежат обновления безопасности, направленные на устранение уязвимостей, уровень критичности которых определен в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств утвержденной ФСТЭК России от 28 октября 2022 г.

2.3. Для целей настоящего регламента к признакам недекларированных возможностей обновлений безопасности относятся:

а) попытки обращений к файловой системе, базам данных, электронной почте и другой информации, не имеющие отношения к функционалу обновляемых программных, программно-аппаратных средств;

б) недокументированные обращения к сторонним (неизвестным оператору) сетевым адресам и доменным именам, не относящимся к оператору информационной системы;

в) системные вызовы, характерные для вредоносного программного обеспечения (например, попытки загрузки из сети «Интернет» библиотек и программных пакетов, не имеющих отношения к функционалу программного обеспечения, попытки перехвата сетевого трафика другого программного обеспечения, попытки мониторинга действий пользователей с другим программным обеспечением);

г) потенциально опасные изменения в файловой системе в результате установки обновления, в том числе загрузка и установка недокументированных программного обеспечения, драйверов и библиотек, не имеющих отношения к функционалу обновляемого программного, программно-аппаратного средства;

д) изменения конфигурации среды функционирования, не имеющие

отношения к обновляемому программному, программно-аппаратному средству (например, появление новых автоматически загружаемых программ);

е) отключение средств защиты информации и функций безопасности информации.

2.4. Анализ обновлений безопасности организуется (проводится) специалистами по защите информации (информационной безопасности) оператора информационной системы (далее – исследователь).

2.5. Анализ обновлений безопасности включает:

а) подготовку к проведению тестирования обновлений безопасности;

б) проведение тестирования обновлений безопасности;

в) оформление результатов тестирования обновлений безопасности.

2.6. Подготовка к проведению Анализа обновлений безопасности предусматривает получение обновления безопасности и подготовку среды тестирования.

Способы получения обновлений безопасности определяются исследователем, исходя из его возможностей, и не рассматриваются в данном Регламенте.

Анализ обновлений безопасности проводится в следующих средах:

а) исследовательском стенде, специально созданном для тестирования обновлений безопасности или иных целей;

б) тестовой зоне информационной системы («песочнице»);

в) информационной системе, функционирующей в штатном режиме.

Выбор среды тестирования обновлений безопасности осуществляет исследователь, исходя из его технических возможностей и угроз нарушения функционирования информационной системы.

2.7. При проведении анализа обновлений безопасности в соответствии с настоящим Регламентом должны применяться инструментальные средства анализа и контроля, функциональные возможности которых обеспечивают реализацию положений настоящего Регламента, имеющие техническую поддержку и возможность адаптации (доработки) под особенности проводимых тестирований, свободно распространяемые в исходных кодах или средства тестирования

собственной разработки. Рекомендуется применять инструментальные средства анализа и контроля, не имеющие каких-либо ограничений по их применению, адаптации (доработки) на территории Российской Федерации.

3. СОДЕРЖАНИЕ РАБОТ ПО АНАЛИЗУ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

3.1 Общие требования к проведению тестирования

3.1.1. В ходе проведения анализа обновлений безопасности должны выполняться следующие тесты:

а) сверка идентичности обновлений безопасности;

б) проверка подлинности обновлений безопасности;

в) антивирусный контроль обновлений безопасности;

г) поиск опасных конструкций в обновлениях безопасности;

д) мониторинг активности обновлений безопасности в среде функционирования;

е) ручной анализ обновлений безопасности.

3.1.2. Приведенные в пункте 3.1.1 настоящего Регламента тесты выполняются по решению исследователя, исходя из возможности получения обновлений безопасности разными способами и (или) из разных источников в распакованном (расшифрованном) виде, возможности исследователя по распаковке (расшифрованию) обновлений безопасности, а также наличия инструментальных средств анализа (контроля) и иных технических возможностей. По результатам тестирования исследователь описывает результаты каждого проведенного теста.

3.1.3. В случае выявления исследователем признаков недекларированных возможностей в ходе прохождения теста, они должны быть проанализированы путем ручного анализа обновлений безопасности.

3.2 Сверка идентичности обновлений безопасности

3.2.1. Сверка идентичности обновлений безопасности проводится в случае возможности получения обновлений безопасности разными способами и (или) из различных источников.

3.2.2. Сверка идентичности обновлений безопасности предусматривает:

1) получение обновления безопасности разными способами и (или) получение обновлений безопасности из различных источников (например, с IP-адресов, расположенных на территории Российской Федерации, а также за ее пределами);

2) расчет контрольных сумм обновлений безопасности, полученных разными способами и (или) из различных источников;

3) сравнение обновлений безопасности, полученных разными способами и (или) из разных источников, путем сравнения их контрольных сумм.

3.2.3. По результатам выполнения теста должен быть сделан вывод об идентичности обновлений безопасности, полученных разными способами и (или) из разных источников. В случае схождения контрольных сумм обновлений тест считается успешно пройденным.

3.2.4. В случае выявления несоответствий в контрольных суммах обновлений безопасности, указанные обновления безопасности должны быть проанализированы путем ручного анализа обновлений безопасности.

3.3 Проверка подлинности обновлений безопасности

3.3.1. Проверка подлинности обновлений безопасности проводится в случае наличия у исследователя возможности получить файл(ы) обновления безопасности в распакованном (расшифрованном) виде до его установки в среде функционирования, а также при наличии предоставляемых разработчиком обновления штатных средств проверки подлинности файла(ов) обновления безопасности.

3.3.2. Проверка подлинности обновлений предусматривает:

1) распаковку (расшифрование) файла(ов) обновления безопасности;

2) определение критериев проверки подлинности файла(ов) обновления

безопасности. В качестве критериев проверки подлинности файла(ов) обновления могут выступать контрольные суммы файлов, электронная цифровая подпись файлов или иные критерии проверки подлинности файла(ов) обновления безопасности, предоставляемые его разработчиком.

3.3.3. Файл считается подлинным, если критерий проверки подлинности файла(ов) обновления безопасности, определенный исследователем, идентичен критерию, предоставленному разработчиком обновления безопасности. В случае установления подлинности файла(ов) обновления безопасности тест считается успешно пройденным.

3.3.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены нарушения подлинности или подлинность которых невозможно проверить, должны быть проверены путем ручного анализа обновления безопасности.

3.4 Антивирусный контроль обновлений безопасности

3.4.1. Антивирусный контроль обновлений безопасности заключается в выявлении вредоносных компьютерных программ (вирусов) в исследуемом обновлении безопасности с использованием средств антивирусной защиты. Для проведения анализа необходимо использовать не менее двух средств антивирусной защиты разных разработчиков.

3.4.2. Антивирусный контроль обновлений безопасности предусматривает

1) проверку обновлений безопасности средствами антивирусной защиты до их установки;

2) проведение сигнатурного и эвристического анализа содержимого оперативной памяти, файловой системы и загрузочных секторов всех используемых носителей информации по завершению установки обновления безопасности.

3.4.3. Тест считается успешно пройденным в случае отсутствия признаков вредоносной активности в файлах обновлений безопасности и в самом программном обеспечении после установки обновлений безопасности.

3.4.4. В случае неуспешного прохождения теста, файл(ы) обновлений

безопасности, в которых выявлены признаки вредоносной активности, должны быть проанализированы путем ручного анализа обновлений безопасности.

3.5 Поиск опасных конструкций в обновлениях безопасности

3.5.1. Поиск опасных конструкций в обновлениях безопасности проводится в случае наличия у исследователя возможности получить файл(ы) обновления в распакованном (расшифрованном) виде до или после установки обновления в среде функционирования.

3.5.2. Поиск опасных конструкций в обновлениях безопасности предусматривает:

а) поиск опасных конструкций в обновлениях безопасности с применением индикаторов компрометации, YARA-правил и других способов;

б) контекстный поиск политических баннеров, лозунгов и другой противоправной информации в обновлениях безопасности.

3.5.3. Тест считается успешно пройденным в случае, если опасные конструкции не выявлены.

3.5.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены опасные конструкции, должны быть проанализированы путем ручного анализа обновлений безопасности.

3.5.5. При проведении ручного анализа исследователем должно быть исследовано назначение выявленных опасных конструкций, подтверждена или опровергнута их опасность.

3.6 Мониторинг активности обновлений безопасности в среде тестирования

3.6.1. Мониторинг активности обновлений безопасности в среде тестирования заключается в получении и анализе сведений о поведении обновляемого программного, программно-аппаратного средства в результате его взаимодействия со средой функционирования или другими программами, а также анализе сведений

о взаимодействии компонентов обновленного программного, программно-аппаратного средства.

3.6.2. Мониторинг активности обновлений безопасности в среде функционирования проводится при наличии возможности установки необходимых инструментов в среде тестирования обновляемого программного, программно-аппаратного средства.

3.6.3. Мониторинг активности обновлений безопасности в среде тестирования предусматривает необходимость проведения:

а) анализа результатов выполнения системных вызовов обновленного программного обеспечения;

б) анализа получаемых и отправляемых обновленным программным, программно-аппаратным средством сетевых пакетов;

в) анализа состава файловой системы до и после установки обновления программного, программно-аппаратного средства;

г) сигнатурного поиска известных уязвимостей.

3.6.4. Тест считается успешно пройденным, если в ходе мониторинга активности обновлений безопасности в среде тестирования не выявлено признаков недекларированных возможностей.

3.6.5. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены признаки недекларированных возможностей, должны быть проанализированы путем ручного анализа обновлений безопасности.

3.7 Ручной анализ обновлений безопасности

3.7.1. Ручной анализ обновлений безопасности проводится в случае, если по результатам выполнения тестов:

а) выявлены различия в обновлениях безопасности, полученных разными способами и (или) из разных источников;

б) неуспешно пройден тест подлинности файла(ов) обновления безопасности;

в) выявлены признаки вредоносной активности в файлах обновления безопасности в результате антивирусного контроля или мониторинга активности

обновления безопасности в среде функционирования;

г) обнаружены опасные конструкции.

3.7.2. Ручной анализ обновлений безопасности проводится в отношении компонентов обновлений безопасности, в которых по результатам прохождения перечисленных выше тестов выявлены указанные в пункте 3.7.1 настоящего Регламента условия.

В случае если ручной анализ провести невозможно, исследователем делается вывод о наличии в обновлении безопасности признаков недекларированных возможностей.

3.7.3. Ручной анализ обновления безопасности предусматривает:

а) анализ логики работы (в том числе дизассемблирование или декомпиляция бинарного кода при наличии соответствующих возможностей);

б) исследование компонентов обновления безопасности с помощью отладчиков и трассировщиков;

в) проверки наличия в обновлении безопасности ключевой информации (паролей, секретных ключей и другой чувствительной информации);

г) статического и динамического анализа (при наличии исходных кодов обновлений безопасности).

3.7.4. По результатам прохождения теста исследователем делается вывод о подтверждении наличия или отсутствия выявленных ранее признаков недекларированных возможностей в компоненте(ах) обновляемого программного, программно-аппаратного средства.

3.7.5. В случае если по результатам ручного тестирования в обновлении безопасности выявлены вредоносное программное обеспечение и (или) недекларированные возможности, указанная информация направляется в ФСТЭК России и Национальный координационный центр по компьютерным инцидентам (НКЦКИ) в соответствии с установленным регламентом.

4. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ

4.1. Результаты анализа обновлений безопасности оформляются в виде отчета. В отчете должны быть отражены описание тестовой среды, сведения об уязвимостях, на устранение которых направлено обновление безопасности, результаты каждого теста, проведенного в соответствии с разделом 3 настоящего Регламента.

4.2. Отчет анализа обновления безопасности включает следующие сведения:

а) наименование обновления безопасности;

б) сведения о месте размещения обновления безопасности, контрольных суммах обновления безопасности, дате выпуска обновления безопасности, разработчике обновления безопасности, версии программного обеспечения;

в) сведения об уязвимостях, на устранение которых направлено обновление безопасности;

г) наименование проведенных тестов;

д) результаты анализа (успешно/не успешно);

е) описание результатов анализа, включая средства проведения анализа, среду тестирования, выявленные признаки недекларированных возможностей, описание проведенных тестов.

4.3. Для тестов, по результатам которых выявлены признаки недекларированных возможностей, в отчет тестирования обновлений безопасности должна быть включена вся техническая информация, необходимая для пояснения выполненных в ходе исследования операций и результатов, полученных в ходе исследований (в том числе все отчеты инструментальных средств анализа и контроля).

В отношении выявленных признаков недекларированных возможностей исследователем определяются ограничения и условия, при которых установка обновления безопасности возможна. Указанные сведения включаются в отчет анализа обновлений безопасности.

5. УСТАНОВКА ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

При принятии решения о результатах тестирования обновлений безопасности программных, программно-аппаратных средств реализуется следующий порядок определения возможности установки обновлений программных, программно-аппаратных средств.

1. Вывод о возможности установки обновлений безопасности.

1.1. В отношении проприетарных программных, программно-аппаратных средств и свободно распространяемого программного обеспечения вывод о возможности установки обновления безопасности формируется на основе выполнения следующих тестов:

– сверка идентичности обновлений безопасности и (или) проверка подлинности обновлений безопасности;

– антивирусный контроль обновлений безопасности и (или) поиск опасных конструкций безопасности;

– мониторинг активности обновлений безопасности в среде функционирования.

1.2. В отношении обновлений безопасности программного обеспечения с открытым кодом вывод о возможности установки обновления безопасности формируется на основе выполнения следующих тестов:

– проверка подлинности обновлений безопасности;

– антивирусный контроль обновлений безопасности;

– мониторинг активности обновлений безопасности в среде функционирования;

– ручной анализ обновлений безопасности.

2. Оценка результатов выполненных тестов.

2.1. Если по результатам выполнения тестов результаты реализации всех тестов являются положительными, обновление безопасности является безопасным и его установка возможна.

2.2. Если по результатам выполнения тестов результаты реализации одного или более тестов являются потенциально опасными и ни один из тестов не являются опасными, обновление безопасности может быть установлено при определенных ограничениях.

Ограничения определяются исследователем по результатам тестирования и могут быть уточнены оператором информационной системы с учетом особенностей ее архитектуры и функционирования.