АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ТБИЛИССКИЙ РАЙОН

ПОСТАНОВЛЕНИЕ

от 12.09.2023 № 1041

ст-ца Тбилисская

Об утверждении Регламента по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в администрации муниципального образования Тбилисский район и подведомственных им организациях

В целях усиления обеспечения безопасности информации и повышения защищенности информационных систем, эксплуатируемых в органах местного самоуправления муниципального образования Тбилисский район и подведомственных им организациях, в соответствии с методическими документами ФСТЭК России, руководствуясь статьями 31, 60, 66 Устава муниципального образования Тбилисский район, п о с т а н о в л я ю :

1. Утвердить регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в органах местного самоуправления муниципального образования Тбилисский район и подведомственных им организациях (приложение).

2. Отделу информатизации организационно-правового управления администрации муниципального образования Тбилисский район (Свиридов Д.И.) обеспечить размещение настоящего постановления на официальном сайте администрации муниципального образования Тбилисский район в информационно-телекоммуникационной сети «Интернет».

3. Контроль за выполнением настоящего распоряжения возложить на заместителя главы муниципального образования Тбилисский район Кириченко Т.В.

4. Постановление вступает в силу со дня его подписания.

Глава муниципального образования Тбилисский район Е.Г. Ильин

Администрация муниципального образования Тбилисский район Краснодарского края
Отдел делопроизводства и организационной работы организационно-правового управления

Приложение

УТВЕРЖДЕН
постановлением администрации
муниципального образования
Тбилисский район
от 12.09.2023 № 1041

РЕГЛАМЕНТ
по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в администрации муниципального образования Тбилисский район и подведомственных им организациях

1. Общие положения

1.1. Настоящий регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах (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 определяет порядок выявления, анализа и устранения уязвимостей, недостатков программного обеспечения, программно-аппаратных средств, организационно-технических недостатков и порядок действий ответственных лиц органов местного самоуправления муниципального образования Тбилисский район и подведомственных им организациях (далее – ОМСУ МО МГО), при контроле защищенности информации, обрабатываемой в информационных системах (далее – ИС) ОМСУ МО МГО, в соответствии с требованиями о защите информации, содержащейся в ИС, а также иными нормативными правовыми актами и методическими документами ФСТЭК России

1.3. Целью регламента является повышение уровня информационной безопасности ОМСУ МО МГО посредством повышения защищенности информационной инфраструктуры и информационных систем ОМСУ МО МГО, обеспечение взаимодействия между структурными подразделениями ОМСУ МО МГО по вопросам устранения уязвимостей.

1.4. 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.

1.5. Результат проведенных мероприятий по выявлению, анализу и устранению уязвимостей отражается в акте проверки (Приложение).

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.

1.7. Действие настоящего положения распространяется на всех сотрудников ОМСУ МО МГО и третью сторону в части их касающейся.

2. Порядок выявления критичных уязвимостей программных, программно-аппаратных средств, организационно-технических недостатков

2.1. Уязвимость – это недостаток ИС или системы защиты, который может привести к реализации угрозы безопасности информации.

2.2. Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации ИС.

2.3. Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИС составляет 1 год. Внеплановые процедуры выявления, анализа и устранения уязвимостей ИС проводят по распоряжению руководителя ОМСУ МО МГО в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет администратор безопасности на основе фактов, которые свидетельствуют о возможной угрозе. В обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИС.

2.4. В ИС должно осуществляться выявление следующих типов уязвимостей:

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

2) недостатки аппаратных средств ИС, в том числе аппаратных средств защиты информации.

3) организационно-технические недостатки.

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

2.6. 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.

2.7. Процесс управления уязвимостями организуется для всех ИС ОМСУ МО МГО 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.

3. Порядок анализа критичных уязвимостей программных, программно-аппаратных средств

3.1. На этапе анализа уязвимостей определяется уровень критичности уязвимостей применительно к ИС ОМСУ МО МГО.

3.1.1. Выявление уязвимостей осуществляется на основании данных из следующих источников:

1) внутренние источники:

- системы управления информационной инфраструктурой (далее – ИТ-инфраструктура);
- базы данных управления конфигурациями;
- документация на ИС;
- электронные базы знаний ОМСУ МО МГО;

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

3) внешние источники:

- базы данных, содержащие сведения об известных уязвимостях;
- официальные информационные ресурсы разработчиков программных и программно-аппаратных средств и исследователей в области информационной безопасности.

3.1.2. Источники данных могут уточняться или дополняться с учетом особенностей функционирования ОМСУ МО МГО.

3.2. 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
2	Оценка применимости уязвимости	На основе информации об объектах ИС и их состоянии определяется применимость уязвимости к информационным системам ОМСУ МО МГО 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 ОМСУ МО МГО 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)

3.3. Выявление недостатков программного обеспечения

3.3.1. При выявлении недостатков программного обеспечения проверяют:

1) конфигурации и настройки программно-технических средств ИС и ее системы защиты информации на соответствие требованиям эксплуатационной документации и требований к защите информации;

2) наличие и сроки действия лицензий на установленное программное обеспечение ИС;

3) наличие последних обновлений используемого программного обеспечения ИС;

4) соответствие обновлений версиям программного обеспечения, установленного в ИС и системе защиты информации;

5) проверка обновлений вирусных баз;

6) проводят анализ сообщений об уязвимостях из специальных источников для ИС.

3.3.2. При наличии в ИС сканеров безопасности администратор безопасности осуществляет процесс сканирования и анализ отчетов об обнаруженных уязвимостях.

3.3.3. Результаты сканирования ИС должны быть отсортированы администратором безопасности по степени критичности (опасности реализации известных угроз безопасности) обнаруженных уязвимостей.

3.4. Выявление недостатков аппаратных средств

3.4.1. К недостаткам аппаратных средств, используемых в ИС, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

3.4.2. При выявлении недостатков аппаратных средств проверяют:

1) Техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств ИС за период контроля защищенности.

2) Наличие сертификатов соответствия на примененные в ИС и ее системе защиты информации аппаратные средства.

3) Наличие у поставщиков обновленных версий аппаратных средств, примененных в ИС и системе защиты информации.

4) Перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств.

5) Конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

3.5. Выявление организационно-технических недостатков

3.5.1. При выявлении недостатков организационно-технических мероприятий проверяют:

1) состояние и актуальности организационно-распорядительной документации (далее ОРД) по защите информации, обрабатываемой в ИС;

2) заполнение рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД);

3) Соответствие выполнения правил генерации и смены паролей пользователей принятым требованиям;

4) Соответствие выполнения правил заведения и удаления учетных записей пользователей принятым требованиям;

5) Соответствие выполнения правил разграничения доступа к информации и ресурсам ИС принятым требованиям;

6) Соответствие полномочий пользователей принятым требованиям;

7) Наличие документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;

8) Состояние физической защиты ИС (средства охраны и физического доступа в контролируемых зонах ИС);

9) Знаний и соблюдения пользователями ИС основных нормативно-правовых актов в области защиты информации и требований ОРД.

3.5.2. В проверке обязательно непосредственно участвует администратор безопасности.

4. Оценка уровня критичности выявленных уязвимостей.

4.1.1. 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.

4.1.2. Исходными данными для определения критичности уязвимостей являются:

1) 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;

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

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

4) результаты контроля защищенности информационных систем, проведенные оператором.

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

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

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

1) определение программных, программно-аппаратных средств, подверженных уязвимостям;

2) 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);

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

4.1.5. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в ИС осуществляется в соответствии с разделом 2 Методики оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 г.

5. Порядок устранения критичных уязвимостей программных, программно-аппаратных средств, организационно-технических недостатков

5.1. Устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор безопасности и системные администраторы ИС, каждый в своей части.

5.2. 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.

5.3. 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.

5.4. 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

5.5. 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 5.2.

Таблица 5.2

№ 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	В случае, если негативного влияния от установки обновления на выбранном сегменте системы не выявлено, принимается решение о его распространении

№ п/п	Наименование операции	Описание операции
	обновления	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
8.	Разработка и реализация мероприятий организационно-технического характера	Обновление либо разработка новых (недостающих) организационно-распорядительных документов, подлежащих применению в ОМСУ МО МГО, согласно особенностям их функционирования, назначение должностных лиц, ответственных за работу в области информационной безопасности, создание коллегиальных органов (комиссий). В случае выявление уязвимости технического характера (состояние помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) принимается решение о реализация мероприятий по устранению выявленных недостатков, приведению объектов в нормативное состояние.

5.6. В случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России тестирование обновлений программных и

программно-аппаратных средств осуществляется в соответствии с настоящим Регламентом по решению ОМСУ МО МГО

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.

5.7. Рекомендуемые сроки устранения уязвимостей:

1) критический уровень опасности до 24 часов;

2) высокий уровень опасности – до 7 дней;

3) средний уровень опасности – до 4 недель;

4) низкий уровень опасности – до 4 месяцев.

5.8. В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации выполняются операции, приведенные в таблице 5.3.

Таблица 5.3

№ 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 ОМСУ МО МГО
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

№ п/п	Наименование операции	Описание операции
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))

5.9. На основе таблиц 5.2 и 5.3 в ОМСУ МО МГО 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 ОМСУ МО МГО.

5.10. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

5.11. 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 ИС с учетом архитектуры и особенностей функционирования ИС, а также способов эксплуатации уязвимостей программных, программно-аппаратных средств.

5.12. Компенсирующими организационными и техническими мерами, направленными на предотвращение возможности эксплуатации уязвимостей, являются:

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

2) 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);

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

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

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

6. Заключительные положения

6.1. Сотрудники ОМСУ МО МГО должны быть предупреждены об ответственности за действия, нарушающие требования настоящего Регламента.

6.2. Сотрудники ОМСУ МО МГО, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим положением, в пределах, определенных действующим законодательством Российской Федерации, муниципальными правовыми актами и локальными актами ОМСУ МО МГО.

Заместитель главы муниципального образования Тбилисский район Т.В. Кириченко

Приложение

к Регламенту по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в администрации муниципального образования Тбилисский район и подведомственных им организациях

АКТ
проведенной проверки информационной безопасности

В ходе проверки объекта защиты информации «[указать наименование объекта]»
Расположенного по адресу «[указать адрес объекта]»

Было установлено:

Объект:	Имеет уязвимости | Не имеет уязвимостей (Нужное подчеркнуть)

Уязвимости программного обеспечения

Уязвимости аппаратных средств

Организационно - технические уязвимости

Предпринятые действия для устранения уязвимостей

Дополнительные пояснения по процессу проверки

Администратор безопасности _____

Дата: _____ МП

Заместитель главы муниципального образования Тбилисский район Т.В. Кириченко