АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАНЕВСКОЙ РАЙОН

РАСПОРЯЖЕНИЕ

от 31.08.2023 № 75-р

ст-ца Каневская

Об утверждении регламента по выявлению анализу и устранению критических уязвимостей в информационных системах, эксплуатируемых в администрации муниципального образования Каневской район

В целях усиления обеспечения безопасности информации и повышения защищенности информационных систем в муниципальном образовании Каневской район и в соответствии с Руководством по организации процесса управления уязвимостями в органе (организации), утвержденным Федеральной службой по техническому и экспортному контролю России (далее – ФСТЭК) от 17 мая 2023 г., с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств утвержденной ФСТЭК России от 28 октября 2022 г., руководствуясь постановлением администрации муниципального образования Каневской район от 25 октября 2019 года № 1872 «О должностных полномочиях заместителей главы муниципального образования Каневской район»:

1. Утвердить Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в администрации муниципального образования Каневской район, согласно приложению к настоящему распоряжению.

2. Отделу по связям со СМИ и общественностью администрации муниципального образования Каневской район (Игнатенко Т.А.) обеспечить размещение настоящего распоряжения на официальном сайте администрации муниципального образования Каневской район в информационно-телекоммуникационной сети «Интернет».

3. Контроль за выполнением настоящего распоряжения оставляю за собой.

4. Распоряжение вступает в силу со дня его подписания.

Заместитель главы
муниципального образования,
управляющий делами администрации
муниципального образования
Каневской район В.В. Касьяненко

Приложение

УТВЕРЖДЕН
распоряжением
администрации
муниципального образования
Каневской район
от 31.08.2023 № 75-р

РЕГЛАМЕНТ
по выявлению анализу и устранению критических уязвимостей в информациониых системах, эксплуатируемых в муниципальном образовании Каневской район

1. Общее положение

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 Федеральной службой по техническому и экспортному контролю России (далее – ФСТЭК) 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

информационнойбезопасности.

Целями регламента являются:

координация деятельности администрации муниципального образования Каневской район и структурных подразделений 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 по вопросам устранения уязвимостей.

2. Порядок выявления критичных уязвимостейпрограммных, 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 администрации муниципального образования Каневской район и структурных подразделениях 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 администрации муниципального образования Каневской район и структурных подразделений:

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 администрации муниципального образования Каневской район и структурных подразделений;

оценка угроз безопасности информации – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в ИС администрацию муниципального образования Каневской район и структурные подразделения;

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

управление обновлениями – приобретение, анализ и развертывание обновлений программного обеспечения в администрации муниципального образования Каневской район и структурных подразделениях;

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 известныхуязвимостях;

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 администрации муниципального образования Каневской район и структурных подразделений, осуществляется выявление уязвимостей на основании данных из следующих источников:

а) внутренние источники:

внутренние информационные системы;

базы данных ИС;

документация на ИС.

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 администрации муниципального образования Каневской район и структурных подразделений.

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	2	3
1	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам. 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 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

1	2	3
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 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 администрации муниципального образования Каневской район и структурных подразделениях 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 администрации муниципального образования Каневской район.

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

ыполняются операции, приведенные в таблице 4.1.

Таблица 4.1

№ п/п	Наименование операции	Описание операции
1	2	3
1	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей всоответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей (этап 4)
2	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установкаобновления 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, чтоустановка 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 администрации муниципального образования Каневской район и структурных подразделениях 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.

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	2	3
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 администрации муниципального образования

Каневской район и структурных подразделений 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 под процесса разработки и реализации компенсирующих мер защиты информации выполняются операции, приведенныев таблице 4.3.

Таблица 4.3.

№ п/п	Наименование операции	Описание операции
1	2	3
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.
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 цельювыявления и блокирования попыток эксплуатации уязвимости

1	2	3
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 администрации муниципального образования Каневской район и структурных подразделениях 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.

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-аппаратныхсредств.

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.

Начальник отдела системно-технического
обеспечения управления делами
администрации муниципального образования
Каневской район А.М. Белоус