ПРАВИТЕЛЬСТВО
АМУРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

17.10.2023 № 879

г. Благовещенск

Об утверждении Регламента
выявления, анализа и устранения уязвимостей в информационных системах, эксплуатируемых в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях

В целях усиления обеспечения безопасности информации и повышения защищенности информационных систем, эксплуатируемых в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях, в соответствии с Руководством по организации процесса управления уязвимостями в органе (организации), утвержденным Федеральной службой по техническому и экспортному контролю 17.05.2023, Правительство Амурской области

п о с т а н о в л я е т:

1. Утвердить прилагаемый Регламент выявления, анализа и устранения уязвимостей в информационных системах, эксплуатируемых в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях.

2. Контроль за исполнением настоящего постановления возложить на заместителя председателя Правительства Амурской области Пузанова П.И.

3. Настоящее постановление подлежит официальному опубликованию на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) и размещению на Портале Правительства Амурской области в информационно-телекоммуникационной сети Интернет (www.amurobl.ru).

Губернатор Амурской области В.А. Орлов

ПРАВИТЕЛЬСТВО АМУРСКОЙ ОБЛАСТИ
АППАРАТ ГУБЕРНАТОРА ОБЛАСТИ И ПРАВИТЕЛЬСТВА ОБЛАСТИ
Отдел регистрации и сопровождения правовых актов

Приложение
УТВЕРЖДЕН
постановлением Правительства
Амурской области
от 17.10.2023 № 879

Регламент
выявления, анализа и устранения уязвимостей в информационных системах, эксплуатируемых в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок действий по организации процесса выявления, анализа и устранения уязвимостей в информационных системах (далее – ИС), эксплуатируемых в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях (далее – органы (организации), и определяет порядок работы органов (организаций) в части управления уязвимостями.

1.2. В настоящем Регламенте используются следующие понятия:

1) уязвимость – это свойство ИС, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации;

2) управление уязвимостью – это деятельность по анализу и устранению уязвимостей, выявленных в программных, программно-аппаратных средствах ИС, информационно-телекоммуникационных сетях, автоматизированных системах управления, информационно-телекоммуникационных инфраструктурах центров обработки данных, на базе которых функционируют эти системы и сети.

1.3. Процесс управления уязвимостями взаимосвязан со следующими процессами и процедурами в деятельности органов (организаций):

1) мониторинг информационной безопасности (далее – ИБ) – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей, устанавливаемый Регламентом мониторинга (просмотра, анализа) результатов регистрации событий безопасности и реагирования на них, утверждаемым органом (организацией);

2) оценка защищенности – анализ возможности использования обнаруженных уязвимостей для реализации компьютерных атак на ИС органа

(организации), устанавливаемый порядком контроля (анализа) защищенности информации в ИС, утверждаемым органом (организацией);

3) оценка угроз безопасности информации – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в ИС органа (организации) и осуществляется в процессе моделирования угроз безопасности информации, результаты которой отражаются в Модели угроз безопасности информации в ИС органа (организации), представляющей собой описание систем, сетей и актуальных угроз безопасности информации в соответствии с Методикой оценки угроз безопасности информации, утвержденной Федеральной службой по техническому и экспортному контролю 05.02.2021;

4) управление конфигурацией – контроль изменений, состава и настроек программного и программно-аппаратного обеспечения ИС, устанавливаемый Регламентом внесения изменений в конфигурацию ИС и системы защиты информации, утверждаемым органом (организацией);

5) управление обновлениями – приобретение, анализ и развертывание обновлений программного обеспечения в органе (организации), устанавливаемые порядком контроля (анализа) защищенности информации в ИС, утверждаемым органом (организацией);

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

1.4. Настоящий Регламент предназначен для следующих сотрудников органа (организации) (далее – Участники процесса):

1) назначенных ответственными за обеспечение безопасности персональных данных;

2) назначенных ответственными за защиту информации в государственных ИС;

3) выполняющих функции по управлению (администрированию) системой защиты информации;

4) выполняющих функции по управлению конфигурацией ИС и ее системы защиты информации.

1.5. Ответственным за организацию процесса управления уязвимостями в органе (организации) является сотрудник органа (организации), ответственный за обеспечение безопасности персональных данных и защиту информации, не содержащей сведения, составляющие государственную тайну, в ИС органа (организации) (далее – Ответственный сотрудник).

1.6. Ответственный сотрудник организует и контролирует своевременное и квалифицированное выполнение Участниками процесса положений нормативных правовых актов Российской Федерации в области ИБ, нормативных и методических документов уполномоченных органов в области защиты информации и локальных актов органа (организации) в области управления уязвимостями ИБ.

1.7. В органе (организации) осуществляются следующие роли исполнителей процесса управления уязвимостями:

1) управление уязвимостями – при наличии в органе (организации) подразделения, осуществляющего функции по защите информации в органе (организации) (далее – подразделение ИБ), осуществляет руководитель и специалисты подразделения ИБ, при отсутствии подразделения ИБ осуществляет штатный специалист по ИБ органа (организации);

2) выявление и анализ уязвимостей – осуществляет подразделение ИБ или штатный специалист по ИБ органа (организации);

3) устранение уязвимостей – осуществляет подразделение ИБ либо штатный специалист по ИБ органа (организации) и подразделение, ответственное за внедрение информационных технологий в органе (организации) (далее – подразделение ИТ), при отсутствии подразделения ИТ осуществляет штатный специалист, ответственный за внедрение информационных технологий в органе (организации) (далее – штатный специалист по ИТ органа (организации).

Роли исполнителей процесса управления уязвимостями могут распределяться и (или) совмещаться в зависимости от укомплектованности органа (организации) специалистами в области защиты информации и информационных технологий.

1.8. Процесс управления уязвимостями включает следующие этапы:

1) мониторинг уязвимостей и оценка их применимости;

2) оценка уязвимостей;

3) определение методов и приоритетов устранения уязвимостей;

4) устранение уязвимостей;

5) контроль устранения уязвимостей.

1.9. Участники процесса несут персональную ответственность за несоблюдение или ненадлежащее соблюдение положений настоящего Регламента.

2. Мониторинг уязвимостей и оценка их применимости

2.1. Этап мониторинга уязвимостей и оценки их применимости состоит из следующих последовательно выполняемых операций:

1) анализ информации об уязвимости (1);

2) оценка применимости уязвимости (2);

3) принятие решений на получение дополнительной информации (3);

4) постановка задачи на сканирование объектов ИС (4);

5) сканирование объектов ИС (5);

6) оценка защищенности (6).

2.2. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 1, 2, 4–6 пункта 2.1 настоящего Регламента, является руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации).

2.3. Лицом, ответственным за выполнение операции, предусмотренной подпунктом 3 пункта 2.1 настоящего Регламента, является специалист подразделения ИБ либо штатный специалист по ИБ органа (организации).

2.4. Целью этапа мониторинга уязвимостей и оценки их применимости является выявление уязвимостей на основании данных, полученных из различных источников.

2.5. Детальное описание операций этапа мониторинга уязвимостей и оценки их применимости, включающее наименование, описание, исполнителей, продолжительность операций, входные и выходные данные, представлено в таблице № 1 Перечня операций управления уязвимостями в органах (организациях), являющегося приложением к настоящему Регламенту (далее – Перечень операций).

3. Оценка уязвимостей

3.1. Этап оценки уязвимостей состоит из следующих последовательно выполняемых операций:

1) получение информации об объектах ИС, подверженных уязвимости (7);

2) определение уровня опасности уязвимости (8);

3) определение влияния уязвимости на ИС (9);

4) расчет критичности уязвимости (10).

3.2. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 1–3 пункта 3.1 настоящего Регламента, является специалист подразделения ИБ либо штатный специалист по ИБ органа (организации).

3.3. Лицом, ответственным за выполнение операции, предусмотренной подпунктом 4 пункта 3.1 настоящего Регламента, является руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации).

3.4. Целью этапа оценки уязвимостей является определение уровня критичности уязвимости применительно к ИС органа (организации).

3.5. Детальное описание операций этапа оценки уязвимостей, включающее наименование, описание, исполнителей, продолжительность операций, входные и выходные данные, представлено в таблице № 2 Перечня операций.

3.6. Определение уровня опасности уязвимости и определение влияния уязвимости на ИС выполняется в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной Федеральной службой по техническому и экспортному контролю 28.10.2022.

4. Определение методов и приоритетов устранения уязвимостей

4.1. Этап определения методов и приоритетов устранения уязвимостей состоит из следующих операций:

1) определение приоритетности устранения уязвимостей (11);

2) определение методов устранения уязвимостей (12);

3) принятие решения о срочной установке обновлений (13);

4) создание заявки на срочную установку обновления (14);

5) принятие решения о срочной реализации компенсирующих мер защиты информации (15);

6) создание заявки на установку обновления (16);

7) создание заявки на реализацию компенсирующих мер защиты информации (17).

4.2. Операции этапа определения методов и приоритетов устранения уязвимостей выполняются последовательно по одной из следующих схем:

11 – 12 – 13 – 14 → 18;

11 – 12 – 15 – 17 → 25;

11 – 12 – 16 → 23;

11 – 12 – 17 → 25.

4.3. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 1–5 пункта 4.1 настоящего Регламента, является руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации).

4.4. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 6, 7 пункта 4.1 настоящего Регламента, является специалист подразделения ИБ либо штатный специалист по ИБ органа (организации).

4.5. Целью этапа определения методов и приоритетов устранения уязвимостей является определение приоритетности устранения уязвимости и определение метода устранения уязвимости применительно к ИС органа (организации).

4.6. Сроки установки обновлений, указанных в подпунктах 3, 4 пункта 4.1 настоящего Регламента, формы и способы передачи заявок, указанных в подпунктах 4, 6, 7 пункта 4.1 настоящего Регламента, согласовываются между подразделением ИБ либо штатным специалистом по ИБ органа (организации) и подразделением ИТ либо штатным специалистом по ИТ органа (организации) в порядке, утверждаемом руководителем органа (организации).

4.7. Детальное описание операций этапа определения методов и приоритетов устранения уязвимостей, включающее наименование, описание, исполнителей, продолжительность операций, входные и выходные данные, представлено в таблице № 3 Перечня операций.

5. Устранение уязвимостей

5.1. Этап устранения уязвимостей состоит из следующих операций:

1) согласование установки обновления с руководителем подразделения ИТ либо штатным специалистом по ИТ органа (организации) (18);

2) тестирование обновления (19);

3) установка обновления в тестовом сегменте (20);

4) принятие решения об установке обновления (21);

5) установка обновления (22);

6) формирование плана установки обновлений (23);

7) разработка и реализация компенсирующих мер защиты информации (24);

8) определение мер защиты информации и ответственных за их реализацию (25);

9) согласование привлечения работников (26);

10) реализация организационных мер защиты информации (27);

11) настройка средств защиты информации (28);

12) организация анализа событий безопасности (29);

13) внесение изменений в систему управления информационной инфраструктурой (30).

5.2. Операции выполняются последовательно по одной из следующих схем:

→ 18 – 19 – 20 (успех) – 21 – 22 (успех) → 31;

→ 18 – 19 – 20 (успех) – 21 – 22 (неудача) → 24;

→ 18 – 19 – 20 (неудача) → 24;

→ 23 – 19 – 20 (успех) – 21 – 22 (успех) → 31;

→ 23 – 19 – 20 (успех) – 21 – 22 (неудача) → 24;

→ 23 – 19 – 20 (неудача) → 24;

→ 24 – 25 – 26 – 27 ˅ 28 ˅ 29 ˅ 30 → 31.

5.3. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 1, 7–12 пункта 5.1 настоящего Регламента, является руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации).

5.4. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 2–6, 13 пункта 5.1 настоящего Регламента, является руководитель подразделения ИТ либо штатный специалист по ИТ органа (организации).

5.5. Целью этапа устранения уязвимостей является принятие мер, направленных на устранение или исключение возможности использования (эксплуатации) уязвимостей.

5.6. Детальное описание операций этапа устранения уязвимостей, включающее наименование, описание, исполнителей, продолжительность операций, входные и выходные данные, представлено в таблице № 4 Перечня операций.

5.7. Тестирование обновления выполняется в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной Федеральной службой по техническому и экспортному контролю 28.10.2022, по решению руководителя органа (организации) в случае отсутствия соответствующих результатов тестирования в банке данных угроз безопасности информации ФСТЭК России, размещенном в информационно-телекоммуникационной сети Интернет по адресу: bdu.fstec.ru (далее – БДУ).

6. Контроль устранения уязвимостей

6.1. Этап контроля устранения уязвимостей состоит из следующих операций:

1) принятие решения о способе контроля (31);

2) проверка объектов ИС на наличие уязвимостей (32);

3) оценка защищенности (33);

4) выявление отклонений и неисполнений (34);

5) разработка предложений по улучшению процесса управления уязвимостями (35);

6) определение причин отклонений и (или) неисполнений (36);

7) корректировка механизмов мониторинга (37);

8) добавление источника сведений об уязвимостях (38);

9) корректировка механизмов оценки уязвимостей (39);

10) повторная оценка уязвимости (40);

11) согласование сроков устранения уязвимости (41);

12) создание заявки на срочную реализацию компенсирующих мер защиты информации (42).

6.2. Операции выполняются последовательно по одной из следующих схем:

→ 31 – 32 ˅ 33 – 34 (при наличии отклонения) – 35 – 36 – 37 ˅ 38 → 18;

→ 31 – 32 ˅ 33 – 34 (при наличии отклонения) – 35 – 36 – 39 → 12;

→ 31 – 32 ˅ 33 – 34 (при наличии отклонения) – 35 – 36 – 40 → 7;

→ 31 – 32 ˅ 33 – 34 (при наличии отклонения) – 35 – 36 – 41 → уязвимость устранена;

→ 31 – 32 ˅ 33 – 34 (при наличии отклонения) – 35 – 36 – 42 → 24;

→ 31 – 32 ˅ 33 – 34 (при отсутствии отклонения) – уязвимость устранена.

6.3. Лицом, ответственным за выполнение операций, предусмотренных подпунктами 1–9, 11, 12 пункта 6.1 настоящего Регламента, является руководитель подразделения ИБ, либо штатный специалист по ИБ органа (организации), либо подразделение, имеющее задачи по защите информации, либо работники других подразделений, имеющие обязанности по защите информации.

6.4. Лицом, ответственным за выполнение операции, предусмотренной подпунктом 10 пункта 6.1 настоящего Регламента, является специалист подразделения ИБ, либо штатный специалист по ИБ органа (организации), либо подразделение, имеющее задачи по защите информации, либо работники других подразделений, имеющие обязанности по защите информации.

6.5. Целью этапа контроля устранения уязвимостей является принятие решений по улучшению процесса управления уязвимостями по результатам сбора, обработки данных о процессе и доведения их до руководства органа (организации).

6.6. Детальное описание операций этапа контроля устранения уязвимостей, включающее наименование, описание, исполнителей, продолжительность операций, входные и выходные данные, представлено в таблице № 5 Перечня операций.

6.7. В случае выявления в ходе операции, предусмотренной подпунктом 3 пункта 6.1 настоящего Регламента, неизвестных ранее уязвимостей сведения о них необходимо направить в БДУ в соответствии с Регламентом включения информации об уязвимостях программного обеспечения и

программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России, утвержденным Федеральной службой по техническому и экспортному контролю 26.06.2018.

Приложение
к Регламенту выявления, анализа и устранения уязвимостей в информационных системах, эксплуатируемых в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях

Перечень
операций управления уязвимостями в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных образований Амурской области и в подведомственных им учреждениях

Таблица № 1 – операции этапа мониторинга уязвимостей и оценки их применимости

№ п/п	Наименование операции	Описание операции	Исполнитель операции	Продолжительность операции	Входные данные	Выходные данные
1	2	3	4	5	6	7
1.	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам (далее – ИС), эксплуатируемым в органах исполнительной власти Амурской области, органах местного самоуправления муниципальных	Специалисты подразделения, осуществляющего функции по защите информации в органе (организации) (далее – подразделение ИБ) либо штатный специалист	Не более 2 рабочих дней. Для уязвимостей критического уровня – не более 1 часа. Для уязвимостей высокого уровня – не более 6 часов	Сведения, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, размещенном в информационно-телекоммуникационной сети Интернет по адресу: bdu.fstec.ru (далее – БДУ), а также	Перечень (список) потенциальных уязвимостей

1	2	3	4	5	6	7
		образований Амурской области и подведомственных им учреждениях (далее – органы (организации). Агрегирование и корреляция собираемых данных об уязвимостях	по информационной безопасности (далее – ИБ) органа (организации)		иные источники, содержащие сведения об известных уязвимостях. Официальные ресурсы разработчиков программного обеспечения, программно-аппаратных средств и исследователей в области ИБ	
2.	Оценка применимости уязвимости	На основе информации об объектах ИС и их состоянии определяется применимость уязвимости к ИС с целью определения уязвимостей, не требующих дальнейшей обработки (нерелевантных уязвимостей). Оценка применимости уязвимостей производится: 1) на основе анализа данных о системе управления информационной инфраструктурой (далее – ИТ-инфраструктура), полученных из баз данных управления конфигурациями в рамках процесса «Управление конфигурацией»; 2) на основе анализа данных о возможных объектах воздействия, полученных в результате моделирования угроз в рамках	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 2 рабочих дней. Для уязвимостей критического уровня – не более 1 часа. Для уязвимостей высокого уровня – не более 6 часов	Информация об объектах ИС и их состоянии. Данные, полученные в результате моделирования угроз. Данные, полученные в результате оценки защищенности	Перечень (список) релевантных уязвимостей

1	2	3	4	5	6	7
		процесса «Оценка угроз»; по результатам оценки защищенности, предусмотренной пунктом 6 настоящего Перечня				
3.	Принятие решений на получение дополнительной информации	Запрос дополнительной информации об уязвимости (сканирование объектов ИС, оценка защищенности), если имеющихся данных недостаточно для принятия решений по управлению уязвимостями	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 2 часов. Для уязвимостей критического уровня – не более получаса. Для уязвимостей высокого уровня – не более 2 часов	Перечень (список) релевантных уязвимостей	Решение о получении дополнительной информации
4.	Постановка задачи на сканирование объектов ИС	Запрос на внеплановое сканирование объектов ИС в случае недостаточности либо неактуальности имеющихся данных, а также в случае получения информации об уязвимости после последнего сканирования	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа с момента принятия решения о сканировании объектов ИС. Для уязвимостей критического уровня и высокого уровня – незамедлительно	Решение о получении дополнительной информации	Решение о сканировании объектов ИС
5.	Сканирование объектов ИС	Поиск уязвимостей и недостатков с помощью автоматизированных систем анализа защищенности. Выбор объектов ИС и времени сканирования, уведомление заинтересованных подразделений (например, ситуационного центра, подразделения, ответственного за внедрение информационных	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 рабочего дня. Для уязвимостей критического уровня – не более 4 часов. Для уязвимостей высокого уровня – не более	Решение о сканировании объектов ИС	Отчет с результатами сканирования

1	2	3	4	5	6	7
		технологий в органе (организации) (далее – подразделение ИТ) о проведении сканирования и дальнейшее сканирование выбранных объектов ИС на наличие уязвимости		1 рабочего дня. Продолжительность может быть увеличена в зависимости от объема сканируемых объектов ИС и их технических возможностей		
6.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к ИС. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в ИС органа (организации) с использованием моделирования эксплуатации уязвимости или 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)	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 рабочего дня. Для уязвимостей критического уровня – не более 1 часа. Для уязвимостей высокого уровня – не более 6 часов. Продолжительность может быть увеличена в зависимости от объема оцениваемых объектов ИС	Решение о получении дополнительной информации	Отчет с результатами исследования

Таблица № 2 – операции этапа оценки уязвимостей

1	2	3	4	5	6	7
7.	Получение информации об объектах ИС, подверженных уязвимости	Получение выборки объектов ИС, подверженных уязвимости	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 4 часов. Для уязвимостей критического уровня – не более 1 часа. Для уязвимостей высокого уровня – не более 6 часов	Перечень (список) релевантных уязвимостей	Перечень объектов ИС, для которых уязвимость релевантна
8.	Определение уровня опасности уязвимости	Расчет базовой, контекстной и временной метрик по методике CVSS с использованием калькулятора CVSS V3 или V3.1, размещенного в БДУ	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа. Уровень критичности уязвимости определяется подсчетом суммарного количества баллов в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной Федеральной службой по техническому и экспортному контролю 28.10.2022	Основные характеристики уязвимости	Показатель опасности уязвимости (I_{cvss})

1	2	3	4	5	6	7
9.	Определение влияния уязвимости на ИС	Определение влияния уязвимого компонента на защищенность ИС выполняется с использованием результатов процесса «Оценка угроз» (в части сведений о недопустимых негативных последствиях и возможных объектах воздействий), при этом могут быть использованы данные об ИТ-инфраструктуре, полученные из баз данных управления конфигурациями (отдельные результаты из процесса «Управление конфигурацией»)	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа	Сведения об объектах воздействия, сведения об объектах инфраструктуры (тип, количество, влияние на защищенность)	Показатель влияния уязвимости (I_{infr})
10.	Расчет критичности уязвимости	Получение значений уровней критичности обнаруженных уязвимостей	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа	Показатель опасности уязвимости (I_{cvss}), показатель влияния уязвимости (I_{infr})	Сведения об уязвимостях, подлежащих устранению, и уровнях их критичности

Таблица № 3 – операции этапа определения методов и приоритетов устранения уязвимостей

1	2	3	4	5	6	7
11.	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа	Сведения об уязвимостях, подлежащих устранению, и уровнях их критичности	Приоритет устранения уязвимости
12.	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа	Приоритет устранения уязвимости	Методика устранения уязвимости
13.	Принятие решения о срочной установке обновлений	При обнаружении уязвимости критического уровня может быть принято решение о срочной установке обновления программного обеспечения объектов ИС, подверженных уязвимости	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа	Приоритет устранения уязвимости	Решение о срочной установке обновления
14.	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование руководителю подразделения ИТ либо при отсутствии подразделения ИТ штатному специалисту, ответственному за внедрение информационных технологий в органе (организации) (далее – штатный специалист по ИТ органа (организации)	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации)	Незамедлительно после принятия решения	Решение о срочной установке обновления	Заявка на срочную установку обновления

1	2	3	4	5	6	7
15.	Принятие решения о срочной реализации компенсирующих мер защиты информации	При обнаружении уязвимости критического уровня может быть принято решение о срочной реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Не более 1 часа	Приоритет устранения уязвимости	Методика устранения уязвимости (применение компенсирующих мер)
16.	Создание заявки на установку обновления	Заявка создается в случае, если определено, что установка обновления для устранения данной уязвимости не запланирована	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации)	Незамедлительно после определения методики	Методика устранения уязвимости (установка обновления)	Заявка на установку обновления
17.	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	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	Незамедлительно после определения методики	Методика устранения уязвимости (применение компенсирующих мер)	Заявка на реализацию компенсирующих мер

Таблица № 4 – операции этапа устранения уязвимостей

1	2	3	4	5	6	7
Установка обновлений						
18.	Согласование установки обновления с руководителем подразделения ИТ либо штатным специалистом по ИТ органа (организации)	Срочная установка обновлений программного обеспечения предварительно согласовывается с руководителем подразделения ИТ либо штатным специалистом по ИТ органа (организации)	Руководитель подразделения ИБ либо штатный специалист по ИБ. При участии руководителя подразделения ИТ либо штатного специалиста по ИТ органа (организации)	Не более 1 часа	Заявка на срочную установку обновления	Решение о срочной установке обновлений
19.	Тестирование обновления	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации	Специалисты подразделения ИТ либо штатный специалист по ИТ органа (организации)	Не более 2 часов. Для уязвимостей критического уровня – не более получаса	План установки обновлений. Решение о срочной установке обновлений	Решение о необходимости тестирования
20.	Установка обновления в тестовом сегменте ИС	Установка обновлений на выбранном тестовом сегменте ИС в целях определения влияния их установки на ее функционирование	Специалисты подразделения ИТ либо штатный специалист по ИТ органа (организации)	Не более 2 часов Для уязвимостей критического уровня – не более получаса	Решение о необходимости тестирования. Отсутствие результатов тестирований в БДУ	Информация о корректности и допустимости обновления
21.	Принятие решения об	В случае, если негативного влияния от установки	Руководитель подразделения ИТ	Не более 1 часа. Для уязвимостей	Информация о корректности и	Решение об установке

1	2	3	4	5	6	7
	установке обновления	обновления на выбранном тестовом сегменте ИС не выявлено, принимается решение о его распространении в ИС. В случае обнаружения негативного влияния от установки обновления на выбранном тестовом сегменте ИС дальнейшее распространение обновления не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации	либо штатный специалист по ИТ органа (организации)	критического уровня – не более получаса	допустимости обновления (положительно)	обновления
22.	Установка обновления	Распространение обновления на объекты ИС	Специалисты подразделения ИТ либо штатный специалист по ИТ органа (организации)	С момента выявления: до 24 рабочих часов для уязвимостей критического уровня; до 7 рабочих дней для высокого уровня уязвимостей; до 4 недель для среднего уровня уязвимостей; до 4 месяцев для низкого уровня уязвимостей	Решение об установке обновления	Результаты установки обновлений
23.	Формирование плана установки обновлений	Уязвимости, для устранения которых не была определена необходимость срочной	Руководитель подразделения ИТ либо штатный	В течение 24 часов с момента поступления заявки	Заявка на установку обновления	План установки обновлений

1	2	3	4	5	6	7
		установки обновлений, устраняются в ходе плановой установки обновлений. Формирование плана обновлений осуществляется с учетом заявок на установку обновлений	специалист по ИТ органа (организации)	на установку обновления		
24.	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	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации). При участии специалистов подразделения ИТ либо штатного специалиста по ИТ органа (организации)	С момента выявления: до 24 часов для уязвимостей критического уровня; до 7 рабочих дней для высокого уровня уязвимостей; до 4 недель для среднего уровня уязвимостей; до 4 месяцев для низкого уровня уязвимостей	Заявка на реализацию компенсирующих мер. Информация о корректности и допустимости обновления (отрицательно). Результаты установки обновлений (неудача)	Результаты применения мер
2. Разработка и реализация компенсирующих мер						
25.	Определение мер защиты	Определение компенсирующих мер защиты информации,	Специалисты подразделения ИБ	До 1 рабочего дня. Для уязвимостей	Заявка на реализацию компенсирующих мер.	Перечень мер и ответственных

1	2	3	4	5	6	7
	информации и ответственных за их реализацию	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	либо штатный специалист по ИБ органа (организации)	критического уровня – не более 1 часа	Информация о корректности и допустимости обновления (отрицательно) Результаты установки обновлений (неудача)	лиц
26.	Согласование привлечения работников	В случае необходимости привлечения работников других подразделений для реализации компенсирующих мер защиты информации руководитель подразделения ИБ согласует их привлечение с руководителями соответствующих подразделений	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации). При участии руководителя подразделения ИТ либо штатного специалиста по ИТ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – не более получаса	Перечень ответственных лиц (в случае привлечения сотрудников других подразделений)	Перечень ответственных лиц (согласованный)
27.	Реализация организацион-ных мер защиты информации	Реализация организационных мер защиты информации предусматривает: 1) ограничение использования ИТ-инфраструктуры; 2) организацию режима охраны (в частности, ограничение доступа к техническим	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации). При участии руководителя	С момента выявления: до 24 часов для уязвимостей критического уровня; до 7 рабочих дней для высокого уровня	Перечень мер и ответственных лиц	Результаты применения мер

1	2	3	4	5	6	7
		средствам); 3) информирование и обучение персонала органа (организации)	подразделения ИТ либо штатного специалиста по ИТ органа (организации)	уязвимостей; до 4 недель для среднего уровня уязвимостей; до 4 месяцев для низкого уровня уязвимостей		
28.	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	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации). При участии специалистов подразделения ИТ либо штатного специалиста по ИТ органа (организации)	С момента выявления: до 24 часов для уязвимостей критического уровня; до 7 рабочих дней для высокого уровня уязвимостей; до 4 недель для среднего уровня уязвимостей; до 4 месяцев для низкого уровня уязвимостей	Перечень мер и ответственных лиц	Результаты применения мер
29.	Организация анализа событий безопасности	Организация постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления и блокирования попыток эксплуатации уязвимости	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	С момента выявления: до 24 часов для уязвимостей критического уровня; до 7 рабочих дней для высокого уровня уязвимостей; до 4 недель для	Перечень мер и ответственных лиц	Результаты применения мер

1	2	3	4	5	6	7
				среднего уровня уязвимостей; до 4 месяцев для низкого уровня уязвимостей		
30.	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)	Специалисты подразделения ИТ либо штатный специалист по ИТ органа (организации)	С момента выявления: до 24 часов для уязвимостей критического уровня; до 7 рабочих дней для высокого уровня уязвимостей; до 4 недель для среднего уровня уязвимостей; до 4 месяцев для низкого уровня уязвимостей	Перечень мер и ответственных лиц	Результаты применения мер

Таблица № 5 – операции этапа устранения уязвимостей

1	2	3	4	5	6	7
Контроль установки уязвимости						
31.	Принятие решения о способе контроля	Определение способа контроля устранения уязвимости: проверка объектов ИС на наличие уязвимости (сканирование средствами анализа защищенности) либо оценка защищенности	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 1 часа	Результаты применения мер	Решение о способе контроля
32.	Проверка объектов ИС на наличие уязвимостей	Выбор объектов ИС и времени сканирования, уведомление заинтересованных подразделений (например, ситуационного центра, подразделения ИТ) о проведении сканирования и дальнейшее сканирование выбранных объектов ИС на наличие уязвимости	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 4 часов	Решение о способе контроля. Задача на сканирование	Отчет с результатами исследования
33.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к ИС. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в ИС органа (организации) с использованием моделирования эксплуатации уязвимостей или средства эксплуатации уязвимости, в том числе в ходе тестирования на проникновение (тестирования	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 4 часов	Решение о способе контроля. Заявка на исследование	Отчет с результатами исследования

1	2	3	4	5	6	7
		системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к ИС в обход ее системы защиты информации)				
34.	Выявление отклонений и неисполнений	Анализ результатов контроля устранения уязвимостей (определение корректности устранения уязвимостей и соблюдения сроков)	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 1 часа	Отчет с результатами исследования	Сведения об отклонениях, неисполнении
35.	Разработка предложений по улучшению процесса управления уязвимостями	Определение причин отклонений и неисполнений, разработка на их основе решений по улучшению процесса управления уязвимостями	Руководитель подразделения ИБ, специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 4 часов	Сведения об отклонениях, неисполнении	Решение по улучшению процесса управления уязвимостями
2. Разработка предложений по улучшению						
36.	Определение причин отклонений и (или) неисполнений	Определение причин отклонений и неисполнений операций процесса управления уязвимостями. Возможными причинами являются: 1) пропуск уязвимости в ходе мониторинга; 2) ошибки оценки уязвимостей; нарушения сроков устранения уязвимостей; 3) недостаточность принятых компенсирующих мер.	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 1 часа	Сведения об отклонениях, неисполнении	Возможные результаты: 1) отсутствие сведений об уязвимости в ходе мониторинга; 2) ошибки оценки уязвимостей; 3) нарушения сроков устранения

1	2	3	4	5	6	7
		Причины отклонений и неисполнений операций процесса управления уязвимостями могут быть дополнены по результатам анализа процесса управления уязвимостями в органе (организации)				уязвимостей; 4) невозможность установки обновления; 5) недостаточность принятых мер
37.	Корректировка механизмов мониторинга	Внесение изменений в конфигурацию и алгоритмы средств сбора и обработки данных об уязвимостях	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего часа. Для уязвимостей критического уровня и высокого уровуровня уязвимостей – незамедлительно	Отсутствие сведений об уязвимости в ходе мониторинга	Заявка на срочную установку обновлений
38.	Добавление источника сведений об уязвимостях	Поиск и организация мониторинга новых источников сведений об уязвимостях	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего часа. Для уязвимостей критического уровня и высокого уровня уязвимостей – незамедлительно	Отсутствие сведений об уязвимости в ходе мониторинга	Заявка на срочную установку обновлений
39.	Корректировка механизмов оценки уязвимостей	Внесение изменений в процедуру оценки уязвимостей	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня – до получаса. Для высокого уровня уязвимостей – до 1 часа	Ошибки оценки уязвимостей	Методика устранения уязвимости (скорректированная) – в этап определения методов и приоритетов устранения уязвимостей
40.	Повторная оценка уязвимости	Повторное определение уровня критичности уязвимости применительно к ИС органа	Специалисты подразделения ИБ либо штатный	До 1 рабочего дня. Для уязвимостей критического	Ошибки оценки уязвимостей	Переоценка критичности уязвимости – в

1	2	3	4	5	6	7
		(организации). Переход к этапу оценки уязвимостей с дальнейшим выполнением последующих этапов процесса управления уязвимостями	специалист по ИБ органа (организации)	уровня – до получаса. Для высокого уровня уязвимостей – до 1 часа		этап оценки уязвимостей
41.	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, определенными на этапе устранения уязвимостей	Руководитель подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего дня. Для уязвимостей критического уровня и высокого уровня уязвимостей – незамедлительно	Нарушения сроков устранения уязвимостей	Новый срок установки обновлений – в этап контроля устранения уязвимостей
42.	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	Специалисты подразделения ИБ либо штатный специалист по ИБ органа (организации)	До 1 рабочего часа. Для уязвимостей критического уровня и высокого уровня уязвимостей – незамедлительно	Невозможность установки обновления. Недостаточность принятых мер	Заявка на срочную реализацию компенсирующих мер защиты информации – в этап устранения уязвимостей