**А Д М И Н И С Т Р А Ц И Я**

**Я Г О Д Н И Н С К О Г О М У Н И Ц И П А Л Ь Н О Г О О К Р У Г А**

**М А Г А Д А Н С К О Й О Б Л А С Т И**

686230, поселок Ягодное, Ягоднинский район, Магаданская область, улица Спортивная, дом 6, тел. (8 41343) 2-35-29, факс (8 41343) 2-20-42, E-mail: Priemnaya\_yagodnoe@49gov.ru

**РАСПОРЯЖЕНИЕ**

от «22» января 2024 года № 11-р

|  |
| --- |
| Об утверждении Регламента оценки уровня критичности уязвимостей программных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах |

В целях повышения информационной безопасности, защиты информации, содержащейся в муниципальных информационных системах, и определения порядка оценки уровня критичности уязвимостей, выявленных в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах:

1. Утвердить прилагаемый Регламент оценки уровня критичности уязвимостей рпрограммных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах.
2. Настоящее распоряжение подлежит официальному опубликованию в газете «Северная правда» и размещению на официальном сайте администрации Ягоднинского муниципального округа Магаданской области www.yagodnoeadm.ru.
3. Контроль за исполнением настоящего распоряжения возложить на руководителя управления кадров, муниципальной службы, организационной работы и информационной безопасности администрации Ягоднинского муниципального округа Магаданской области Баль Е.А.

Глава Ягоднинского

муниципального округа

Магаданской области Н.Б. Олейник

Проект распоряжения «Об утверждении Регламента оценки уровня критичности уязвимостей программных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и ее отраслевых (функциональных) органах подгтовлен руководителем управления кадров, муниципальной службы, организационной работы и информационной безопасности администрации Ягоднинского муниципального округа Магаданской области Баль Е.А.

«22» января 2024 года

СОГЛАСОВАНО:

|  |  |  |  |
| --- | --- | --- | --- |
| Должность, место работы | Подпись | Инициалы, фамилия | Дата |
| Руководитель управления правового обеспечения и исполнения полномочий администрации Ягоднинского муниципального округа Магаданской области |  | А.П. Старков |  |

РАЗОСЛАТЬ:

|  |  |  |
| --- | --- | --- |
| Наименование комитетов (отделов, организаций, предприятий) | Количество экземпляров | Подпись  |
| управление кадров муниципальной службы, организационной работы и информационной безопасности  | 2 |  |
| Управление финансов | 1 |  |
| Управление образования | 1 |  |
| Управление ЖКХ | 1 |  |
| Отдел культуры | 1 |  |
| Отдел физической культуры, спорта и туризма | 1 |  |

|  |
| --- |
| УТВЕРЖДЕНраспоряжением администрации Ягоднинского муниципального округа Магаданской областиот «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ года № \_\_\_\_\_\_\_ |

Регламент

оценки уровня критичности уязвимости программных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах

# ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий регламент оценки уровня критичности уязвимостей программных, программно-аппаратных средств (далее – Регламент) разработан
в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Регламент определяет порядок оценки уровня критичности уязвимостей, выявленных в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центров обработки данных (далее – информационные системы).

1.3. Настоящий Регламент подлежит применению операторами информационных систем при принятии ими мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем
в соответствии с требованиями о защите информации, содержащейся
в государственных информационных системах, требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, а также иными нормативными правовыми актами
и методическими документами ФСТЭК России.

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

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

# 2. ПОРЯДОК ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2.1. Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения операторами информационных систем о необходимости устранения уязвимостей, выявленных в программных, программно-аппаратных средствах по результатам анализа уязвимостей в информационных системах.

2.2. Исходными данными для определения критичности уязвимостей являются:

а) 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;

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

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

г) результаты контроля защищенности информационных систем, проведенные оператором.

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

2.3. Оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится специалистами по защите информации (информационной безопасности).

2.4. Оценка уровня критичности уязвимостей программных, программно-аппаратных средств применительно к конкретной информационной системе 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 информационной системы);

3) расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе ($V$).

2.5. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе $V$ осуществляется по следующей формуле:

$V=I\_{cvss}×I\_{infr}$,

где $I\_{cvss}$ *–* показатель, характеризующий уровень опасности уязвимости;

$I\_{infr}$ *–* показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы.

2.6. Показатель $I\_{cvss}$ определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1. (https://www.first.org/cvss.).

Базовые метрики отражают основные характеристики уязвимостей, влияющие на доступность, целостность и конфиденциальность информации, которые не изменяются с течением времени и не зависят от среды функционирования программных, программно-аппаратных средств. Базовые метрики включают показатели, характеризующие вектор атаки, сложность атаки, уровень привилегий, взаимодействие с пользователем, влияние на конфиденциальность, целостность и доступность.

Временные метрики отражают характеристики уязвимости, которые изменяются со временем, но не зависят от среды функционирования программных, программно-аппаратных средств. Временные метрики включают показатели, характеризующие доступность средств эксплуатации, доступность средств устранения, степень доверия к информации об уязвимостях.

Контекстные метрики отражают характеристики уязвимости, зависящие от среды функционирования программных, программно-аппаратных средств.

Показатель $I\_{cvss}$ может быть рассчитан с использованием калькулятора, содержащегося в Банке данных угроз безопасности информации ФСТЭК России в разделе «Уязвимости»(https://bdu.fstec.ru/calc3, https://bdu.fstec.ru/calc31.).

В калькуляторе необходимо определить (уточнить) базовые, временные
и контекстные метрики применительно к конкретной системе и сети
(приложение № 1).

Уровень опасности уязвимости применительно к конкретной информационной системе при задании оператором различных метрик в калькуляторе рассчитывается автоматически и отображается в поле «Контекстные метрики» (приложение № 1).

Итоговый показатель $I\_{cvss}$ определяется совокупностью показателей базовых, временных и контекстных метрик применительно к конкретной информационной системе.

2.7. Показатель $I\_{infr}$ определяется по следующей формуле:

$I\_{infr}=k\*K+l\*L+p\*P$, где

$K$ *–* показатель, характеризующий тип компонента информационной системы, подверженного уязвимости;

$L$ *–* показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов);

$P$ *–* показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы;

*k, l, p* – весовые коэффициенты показателей.

Расчет весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на информационную систему, проводится в соответствии с приложением № 2.

2.8.  По результатам расчета уровень критичности уязвимости применительно к конкретной информационной системе принимает значения, указанные в приложении № 3.

#

# 3. ПРИНЯТИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ,

# НАПРАВЛЕННЫХ НА УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

3.1. В зависимости от уровня критичности уязвимостей программных, программно-аппаратных средств в конкретной информационной системе оператором принимается решение о необходимости их устранения.

3.2. В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящим Регламентом присвоен критический уровень, рекомендуется принять меры по их устранению в течение 24 часов.

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящим Регламентом присвоен высокий уровень критичности, рекомендуется принять меры по их устранению в течение 7 календарных дней.

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящим Регламентом присвоен средний уровень критичности, рекомендуется принять меры по их устранению в течение 4-х недель.

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящим Регламентом присвоен низкий уровень критичности, рекомендуется принять меры по их устранению в течение
4-х месяцев.

3.3. Уязвимости программных, программно-аппаратных средств могут быть устранены путем установки обновления программного обеспечения, программно-аппаратного средства или принятия компенсирующих организационных
и технических мер защиты информации.

3.4. В случае если уязвимости содержатся в зарубежных программных, программно-аппаратных средствах или программном обеспечении с открытым исходным кодом, решение об установке обновления такого программного обеспечения, программно-аппаратного средства принимается оператором информационной системы с учетом результатов тестирования этого обновления, проведенного в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022г., и оценки ущерба от нарушения функционирования информационной системы по результатам установки обновления.

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

3.6. Выбор компенсирующих мер по защите информации осуществляется оператором с учетом архитектуры и особенностей функционирования информационной системы, а также способов эксплуатации уязвимостей программных, программно-аппаратных средств.

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

- изменение конфигурации уязвимых компонентов информационной системы, 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 информационной системы, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

- использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление в информационной системе признаков эксплуатации уязвимостей;

- мониторинг информационной безопасности и выявление событий безопасности информации в информационной системе, связанных с возможностью эксплуатации уязвимостей.

|  |
| --- |
| Приложение № 1 к Регламенту оценки уровня критичности уязвимости программных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах |

Расчет базовых метрик уязвимости



Расчет временных метрик уязвимости



Расчет контекстных метрик уязвимости



Значение уровня опасности уязвимости применительно к конкретной системе, сети



|  |
| --- |
| Приложение № 2 к Регламенту оценки уровня критичности уязвимости программных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п | показатель | вес | значение | оценка | Итог*(k\*Ki,l\*Li,p\*Pm)* |
| 1 | Тип компонента информационной системы, подверженного уязвимости (К) | 0,4 | Уязвимости подвержены компоненты информационной системы, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий | 1 | 0,4 |
|  |  | Уязвимости подвержены серверы | 0,8 | 0,32 |
|  |  | Уязвимости подвержено телекоммуникацион-ное оборудование, система управления сетью передачи данных | 0,8 | 0,32 |
|  |  | Уязвимости подвержены автоматизированные рабочие места | 0,5 | 0,20 |
|  |  | Уязвимости подвержены другие компоненты | 0,5 | 0,20 |
| 2 | Количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникацион-ного оборудования, средств защиты информациии других компонентов) ($L$) | 00,2 | Более 70% компонентов от общего числа компонентовв информационной системе | 1 | 0,2 |
|  |  | 50-70%компонентов от общего числа компонентовв информационной системе | 0,8 | 0,16 |
|  |  | 10-50%компонентов от общего числа компонентовв информационной системе | 0,6 | 0,12 |
|  |  | Менее 10% компонентов от общего числа компонентовв информационной системе | 0,5 | 0,10 |
| 33 | Влияние на эффективность защиты периметра системы, сети (Р) | 00,4 | Уязвимое программное, программно-аппаратное средство доступно из сети «Интернет» | 1 | 0,4 |
| Уязвимое программное, программно-аппаратное средство недоступно из сети «Интернет» | 0,5 | 0,2 |

|  |
| --- |
| Приложение № 3 к Регламенту оценки уровня критичности уязвимости программных, программно-аппаратных средств в администрации Ягоднинского муниципального округа Магаданской области и её отраслевых (функциональных) органах |

|  |  |  |
| --- | --- | --- |
| № п/п | Суммарное количество баллов уязвимости | Оценка уровня критичностиуязвимости |
| 1 | 7,0 ≤ V ≤ 10,0 | Критичный |
| 2 | 4,5 ≤ V < 7,0 | Высокий |
| 3 | 1,5 ≤ V < 4,5 | Средний |
| 4 | V < 1,5 | Низкий |