Зарегистрировано 23.06.2023
Регистрационный номер № 111/23/3-П

МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ АСТРАХАНСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

23.06.2023 № 3-П

О повышении защищенности информационных систем исполнительных органов Астраханской области

В целях минимизации угроз информационной безопасности информационных систем органов исполнительной власти Астраханской области в соответствии с рекомендациями ФСТЭК России министерство государственного управления, информационных технологий и связи Астраханской области
ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые:

– регламент тестирования и установки обновлений безопасности программных, программно-аппаратных средств;

– регламент оценки и устранения критичных уязвимостей программных, программно-аппаратных средств, используемых в информационных системах;

– форму плана реализации комплекса мер, направленных на снижение возможности по реализации информационного воздействия через уязвимые и незадействованные службы, доступные из сети Интернет.

2. Отделу информационной безопасности министерства обеспечить размещение текста настоящего постановления на официальном сайте министерства в информационно-телекоммуникационной сети «Интернет» по адресу http://mingos.astrobl.ru/.

3. Управлению связи и массовых коммуникаций министерства в трехдневный срок со дня подписания настоящего постановления обеспечить его опубликование на официальном интернет-портале правовой информации (http://pravo.gov.ru/).

4. Отделу нормативно-правового обеспечения проектов министерства:

– в семидневный срок со дня подписания настоящего постановления направить его копию в Думу Астраханской области и прокуратуру Астраханской области;

– в семидневный срок со дня официального опубликования направить его

копию в Управление Министерства юстиции Российской Федерации по Астраханской области и поставщикам справочно-правовых систем ООО «АИЦ «Консультант Плюс» и ООО «Астрахань-Гарант-Сервис».

5. Постановление вступает в силу со дня его официального опубликования.

Министр А.В. Набутовский

Приложение № 1
к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 23.06.2023 № 3-Т

Регламент тестирования и установки обновлений безопасности программных, программно-аппаратных средств

1. Общие положения

1.1. Регламент тестирования и установки обновлений безопасности программных, программно-аппаратных средств (далее – регламент) определяет порядок и содержание работ по тестированию программного обеспечения, в том числе с открытым исходным кодом, предназначенного для устранения уязвимостей программных, программно-аппаратных средств (далее – обновления безопасности), применяемых в работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС) и разработан в соответствии с законодательством Российской Федерации в области обеспечения информационной безопасности.

1.2. Для целей настоящего регламента используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.3. Настоящий регламент подлежит применению администратором ЕМТС и администраторами сегментов ЕМТС (далее – администраторы) 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. Обновление сертифицированных программных, программно-аппаратных средств защиты информации обеспечивается администраторами в приоритетном порядке в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

1.5. Решение об установке протестированных обновлений безопасности принимается администраторами с учетом результатов тестирования и оценки

рисков нарушения функционирования информационной системы от установки таких обновлений.

2. Порядок тестирования обновлений безопасности программных, программно-аппаратных средств

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

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

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

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

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

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

изменения конфигурации среды функционирования, не имеющие отношения к обновляемому прикладному программному обеспечению, программному, программно-аппаратному средству (например, появление новых автоматически загружаемых программ);

отключение средств защиты информации и функций безопасности информации.

2.3. Тестирование обновлений безопасности организуется (проводится) администраторами.

2.4. Тестирование обновлений безопасности включает:

подготовку к проведению тестирования обновлений безопасности;

проведение тестирования обновлений безопасности;

оформление результатов тестирования обновлений безопасности.

2.5. Подготовка к проведению тестирования обновлений безопасности

предусматривает получение обновления безопасности и подготовку среды тестирования.

Способы получения обновлений безопасности определяются разработчиком программного обеспечения, исходя из его возможностей, и не рассматриваются в данном регламенте.

Тестирование обновлений безопасности проводится в следующих средах:

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

тестовой зоне информационной системы («песочнице»);

информационной системе, функционирующей в штатном режиме.

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

2.6. При проведении тестирования обновлений безопасности в соответствии с настоящим регламентом должны применяться инструментальные средства анализа и контроля, функциональные возможности которых обеспечивают реализацию положений настоящего регламента, имеющие техническую поддержку и возможность адаптации (доработки) под особенности проводимых тестирований, свободно распространяемые в исходных кодах или средства тестирования собственной разработки. Рекомендуется применять инструментальные средства анализа и контроля, не имеющие каких-либо ограничений по их применению, адаптации (доработки) на территории Российской Федерации.

3. Содержание работ по тестированию обновлений безопасности программных, программно-аппаратных средств

3.1. Общие требования к проведению тестирования

3.1.1. В ходе проведения тестирования обновлений безопасности выполняются следующие тесты:

проверка подлинности обновлений безопасности;

антивирусный контроль обновлений безопасности.

3.1.2. Приведенные в пункте 3.1.1 настоящего регламента тесты выполняются администраторами. По результатам тестирования администраторы описывают результаты каждого проведенного теста.

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

3.2. Проверка подлинности обновлений безопасности

3.2.1. Проверка подлинности обновлений безопасности проводится в случае наличия у администраторов возможности получить файл(ы)

обновления безопасности в распакованном (расшифрованном) виде до его установки в среде функционирования, а также при наличии предоставляемых разработчиком обновления штатных средств проверки подлинности файла(ов) обновления безопасности.

3.2.2. Проверка подлинности обновлений предусматривает:

распаковку (расшифрование) файла(ов) обновления безопасности;

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

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

3.3. Антивирусный контроль обновлений безопасности

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

3.3.2. Антивирусный контроль обновлений безопасности предусматривает:

проверку обновлений безопасности средствами антивирусной защиты до их установки;

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

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

4. Оформление результатов тестирования обновлений безопасности программных, программно-аппаратных средств

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

4.2. Отчет тестирования обновления безопасности включает следующие сведения:

наименование обновления безопасности;

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

сведения об уязвимостях, на устранение которых направлено обновление безопасности;

наименование проведенных тестов;

результаты тестирования (успешно/не успешно);

описание результатов тестирования, включая средства проведения тестирования, среду тестирования, описание проведенных тестов.

Форма и содержание типового отчета тестирования обновления безопасности приведены в приложении к настоящему регламенту.

4.3. Для тестов, по результатам которых выявлены вредоносные компьютерные программы (вирусы), в отчет тестирования обновлений безопасности включается вся техническая информация, необходимая для пояснения выполненных в ходе исследования операций и результатов, полученных в ходе исследований (в том числе все отчеты инструментальных средств анализа и контроля).

По решению исследователя в отчет может быть включена техническая информация об иных проведенных тестах.

Приложение
к Регламенту тестирования и установки обновлений безопасности программных, программно-аппаратных средств

Форма отчета о тестировании обновления программного, программно-аппаратного средства

1. Сведения об обновлении безопасности.

1.1. Наименование обновления безопасности.

1.2. Описание обновления безопасности.

1.3. Адрес информационного ресурса, на котором размещено обновление (URL-адрес).

1.4. Контрольная сумма программного, программно-аппаратного средства, в порядке, определенном разработчиком обновляемого программного, программно-аппаратного средства и иным алгоритмам.

1.5. Дата выпуска обновления безопасности.

1.6. Разработчик обновления безопасности.

1.7. Версия программного, программно-аппаратного средства.

1.8. Идентификаторы уязвимостей, на устранение которых направлено обновление безопасности.

1.9. Дата начала и завершения тестирования обновления безопасности.

2. Результаты тестирования обновления безопасности приведены в таблице.

Таблица

Наименование теста	Результат[1]	Среда тестирования[2]	Описание результатов тестирования[3]
проверка подлинности обновлений безопасности			
антивирусный контроль обновлений безопасности			
Вердикт	Обновление программного, программно-аппаратного средства является безопасным и его установка возможна; обновление может быть установлено при определенных ограничениях[4]; обновление является небезопасным и устанавливать его не рекомендуется		

[1] В результате указывается выполнен или не выполнен тест. В случае, если выполнен, указывается успешно или не успешно он выполнен.

[2] Указывается среда тестирования обновления (исследовательский стенд, тестовая зона информационной системы («песочница»), информационная система).

[3] Описание результатов тестирования представляется в произвольной форме и должно включать описание теста, средств проведения тестирования, среды тестирования.

[4] Исследователем указываются конкретные ограничения.

Приложение № 2
к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 23.06.2023 № 3-П

Регламент оценки и устранения критичных уязвимостей программных, программно-аппаратных средств, используемых в информационных системах

1. Общие положения

1.1. Регламент оценки и устранения критичных уязвимостей программных, программно-аппаратных средств, используемых в информационных системах (далее – регламент) определяет порядок оценки уровня критичности уязвимостей, выявленных в программных, программно-аппаратных средствах информационных систем, в работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС).

1.2. Для целей настоящего регламента используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.3. Настоящий регламент подлежит применению Настоящий регламент подлежит применению администратором ЕМТС и администраторами сегментов ЕМТС (далее – администраторы) 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. Обновление с целью устранения уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации обеспечивается администраторами в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

1.5. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе осуществляется в соответствии с методическим документом «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств»,

утвержденным ФСТЭК России 28.10.2022.

2. Порядок оценки уровня критичности уязвимостей программных, программно-аппаратных средств

2.1. Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения администраторами 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:

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

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

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

результаты контроля защищенности информационных систем, проведенные оператором.

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

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

расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе.

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

администраторами принимаются решения о необходимости их устранения.

3.2. В отношении уязвимостей программных, программно-аппаратных средств, которым присвоен критический уровень, оператором информационной системы принимаются меры по их устранению в течение 24 часов.

В отношении уязвимостей программных, программно-аппаратных средств, которым присвоен высокий уровень критичности, оператором информационной системы принимаются меры по их устранению в течение 7 дней.

В отношении уязвимостей программных, программно-аппаратных средств, которым присвоен средний уровень критичности, оператором информационной системы принимаются меры по их устранению в течение 4 недель.

В отношении уязвимостей программных, программно-аппаратных средств, которым присвоен низкий уровень критичности, оператором информационной системы принимаются меры по их устранению в течение 4 месяцев.

3.3. Уязвимости программных, программно-аппаратных средств устраняются администраторами 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 с учетом результатов тестирования этого обновления, проведенного в соответствии с Регламентом тестирования и установки обновлений безопасности программных, программно-аппаратных средств, 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 администраторами 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 № 3
к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 23.06.2023 № 3-Т

План
реализации комплекса мер, направленных на снижение возможности по реализации информационного воздействия через уязвимые и незадействованные службы, доступные из сети Интернет
_____ (далее – ведомство)
(наименование исполнительного органа Астраханской области)
(Форма)

№ п/п	Наименование мероприятия	Ответственный	Срок выполнения	Примечание
1.*	2.*	3.	4.*	5.
1.	Актуализация перечня публичных (внешних) IPv4/v6-адресов, зарегистрированных за организацией в базе данных RIPE или полученных от провайдера интернет и/или провайдера облачных услуг, а также доменных имен, которые используются для обеспечения функционирования информационной инфраструктуры (информационные системы, веб-сервисы) ведомства.	ФИО, должность ответственного сотрудника за проведение мероприятий в ведомстве	Ежеквартально	
2.	Актуализация перечня сервисов (служб), функционирующих в информационной инфраструктуре ведомства, которые в перечне публичных (внешних) IP-адресов доступны из сети Интернет.	ФИО, должность ответственного сотрудника за проведение мероприятий в ведомстве	Ежеквартально	
3.	Проведение по согласованию с государственным бюджетным учреждением Астраханской области «Инфраструктурный центр электронного правительства», являющимся администратором Единой мультисервисной телекоммуникационной сети Правительства Астраханской области, сканирования на	ФИО, должность ответственного сотрудника за проведение мероприятий в ведомстве	Еженедельно	

1.*	2.*	3.	4.*	5.
	наличие уязвимостей в сервисах (службах), размещаемых на таких IP-адресах.			
3.1.	Принятие ведомством необходимых мер по устранению уязвимостей, выявленных в ходе сканирования.	ФИО, должность ответственного сотрудника за проведение мероприятий в ведомстве	В зависимости от уровня критичности уязвимостей программных, программно-аппаратных средств: - в отношении уязвимостей, которым присвоен критический уровень, принимаются меры по их устранению в течение 24 часов; - в отношении уязвимостей, которым присвоен высокий уровень критичности, принимаются меры по их устранению в течение 7 дней; - в отношении уязвимостей, которым присвоен средний уровень критичности, принимаются меры по их устранению в течение 4 недель; - в отношении уязвимостей, которым присвоен низкий уровень критичности, принимаются меры по их устранению в течение 4 месяцев.	
4.	Актуализация конфигурации средств защиты информации, используемых для защиты сервисов служб, в отношении которых выявлены уязвимости, проведение внеочередного анализа зарегистрированных событий информационной безопасности на предмет	ФИО, должность ответственного сотрудника за проведение мероприятий в ведомстве	В течении 7 дней	

1.*	2.*	3.	4.*	5.
	возможных фактов несанкционированного доступа к защищаемому сервису службе.			
5.	Организация публикации новых сервисов, сетевых служб по согласованию с лицом ответственным за обеспечение информационной безопасности в ведомстве.	ФИО, должность ответственного сотрудника за проведение мероприятий в ведомстве	Постоянно, по мере необходимости	

---

* Текст в столбце не подлежит изменению.