ДЕПАРТАМЕНТ ЦИФРОВОГО РАЗВИТИЯ ВОЛОГОДСКОЙ ОБЛАСТИ

ПРИКАЗ

«3» ноября 2023 г. г. Вологда № 92-О

Об утверждении Регламента по тестированию обновлений безопасности программных, программно-аппаратных средств

В целях исполнения требований по обеспечению безопасности информации при её обработке в информационных системах Вологодской области, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»

ПРИКАЗЫВАЮ:

1. Утвердить Регламент по тестированию обновлений безопасности программных, программно-аппаратных средств.
2. Бюджетному учреждению в сфере информационных технологий Вологодской области «Центр информационных технологий» (Н.А.Пучков), бюджетному учреждению Вологодской области «Электронный регион» (Ж.В. Пшеннова), бюджетному учреждению Вологодской области «Медицинские цифровые технологии» (А.В.Стригин) обеспечить исполнение Регламента по тестированию обновлений безопасности программных, программно-аппаратных средств.
3. Настоящий приказ вступает в силу со дня его подписания.

И.о. начальника Департамента Д.В. Плакунов

УТВЕРЖДЕН
приказом Департамента цифрового развития области
от «03» ноября 2023 г. № 92-О

РЕГЛАМЕНТ
по тестированию обновлений безопасности программных, программно-аппаратных средств

1. Общие положения

1.1. Настоящий регламент разработан в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 г.

1.2. 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 информационных системах, информационно-телекоммуникационных сетях, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры органов исполнительной государственной власти и государственных учреждений Вологодской области, в случае передачи обеспечивающих функций в сфере информационных технологий подведомственному учреждению Департамента цифрового развития Вологодской области в соответствии с постановлением Губернатора области.

1.3. Настоящий Регламент подлежит применению при принятии мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, 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. Решение об одобрении установки протестированных обновлений безопасности принимается Администратором безопасности с учетом результатов тестирования.

2. Основные понятия, сокращения

2.1. 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.

Информационная система (далее - ИС) - информационные системы, государственные информационные системы, информационные системы персональных данных, информационно-телекоммуникационные сети, в том числе функционирующие на базе информационно-телекоммуникационной инфраструктуры центров обработки данных.

Администратор безопасности – ответственный за организационно-технические и программно-аппаратные средства защиты информации, должностное лицо (или структурное подразделение) БУ ВО «ЦИТ», осуществляющее контроль выполнения требований нормативно-правовых актов в области информационной безопасности, общее руководство и контроль за обеспечением информационной безопасности в пределах компетенции БУ ВО «ЦИТ».

Администратор информационной системы (Администратор ИС) – структурное подразделение, ответственное лицо бюджетного учреждения в сфере информационных технологий Вологодской области «Центр информационных технологий» (далее - БУ ВО «ЦИТ»), бюджетного учреждения Вологодской области «Электронный регион» (далее - БУ ВО «Электронный регион»), бюджетного учреждения Вологодской области «Медицинские цифровые технологии» (далее - БУ ВО «Медицинские цифровые технологии»), обеспечивающее функционирование баз данных и прикладного программного обеспечения ИС.

Администратор серверной, в том числе виртуальной инфраструктуры (Администратор инфраструктуры) – должностное лицо (или структурное подразделение) БУ ВО «ЦИТ», обеспечивающее функционирование серверной (в том числе виртуальной) инфраструктуры.

Уязвимость - свойство (недостаток, слабость, программного (программно-технического) средства или информационной системы в целом, обусловливающее возможность реализации угроз безопасности информации.

Программное обеспечение (ПО) – совокупность программ, приложений, драйверов и операционных систем, предназначенных для обеспечения функциональности, управления и обслуживания сервера или автоматизированного рабочего места.

Недекларированные возможности – возможности в системном и прикладном программном обеспечении, используемом в информационной системе, функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

3.1. Тестирование обновлений безопасности проводится с целью своевременного выявления в них потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-

аппаратных средств, в том числе недекларированных возможностей.

3.2. Тестированию подлежат обновления безопасности, направленные на устранение уязвимостей, уровень критичности которых определен в соответствии с Методикой оценки уровня критичности уязвимостей программных и программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. и Регламентом по выявлению, анализу и устранению уязвимостей, утвержденным приказом Департамента цифрового развития области №81-0 от 19 сентября 2023 г.

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

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

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

в) 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);

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

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

е) отключение средств защиты информации и функций безопасности информации.

3.4. Тестирование обновлений безопасности организуется (проводится) Администратором безопасности.

3.5. Тестирование обновлений безопасности включает:

а) подготовку к проведению тестирования обновлений безопасности;

б) проведение тестирования обновлений безопасности;

в) оформление результатов тестирования обновлений безопасности.

3.6. Подготовка к проведению тестирования обновлений безопасности предусматривает получение обновления безопасности и подготовку среды тестирования.

Способы получения обновлений безопасности определяются Администратором безопасности, исходя из его возможностей, и не рассматриваются в данном Регламенте.

Тестирование обновлений безопасности проводится в следующих средах:

а) исследовательском стенде, специально созданном для тестирования

обновлений безопасности или иных целей;

б) тестовой зоне информационной системы («песочнице»);

в) информационной системе, функционирующей в штатном режиме.

Выбор среды тестирования обновлений безопасности осуществляется Администратором безопасности, исходя из их технических возможностей и угроз нарушения функционирования информационных систем и по согласованию с Администратором ИС и Администратором инфраструктуры, предоставляющими вычислительные ресурсы среды тестирования.

3.7. При проведении тестирования обновлений безопасности в соответствии с настоящим Регламентом должны применяться при наличии 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.

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

4.1. Общие требования к проведению тестирования

4.1.1. В ходе проведения тестирования обновлений безопасности Администратор безопасности выполняет следующие тесты:

а) сверка идентичности обновлений безопасности (Тест001);

б) проверка подлинности обновлений безопасности (Тест002);

в) антивирусный контроль обновлений безопасности (Тест003);

г) поиск опасных конструкций в обновлениях безопасности (Тест004);

д) мониторинг активности обновлений безопасности (Тест005) (осуществляется только на тестовом стенде);

е) ручной анализ обновлений безопасности (Тест006).

4.1.2. Приведенные в пункте 4.1.1. настоящего Регламента тесты выполняются по решению Администратора безопасности, исходя из возможности получения обновлений безопасности разными способами и (или) из разных источников в распакованном (расшифрованном) виде, возможности Администратора безопасности по распаковке (расшифрованию) обновлений безопасности, а также наличия инструментальных средств анализа (контроля) и иных технических возможностей. По результатам тестирования Администратор безопасности описывает результаты каждого проведенного теста.

4.1.3. В случае выявления Администратором безопасности признаков недекларированных возможностей в ходе прохождения теста, они должны быть проанализированы путем ручного анализа обновлений безопасности.

4.1.4. Администратор безопасности делает вывод о возможности установки обновления безопасности на основании результатов проведенных тестов и с учетом раздела 6 настоящего регламента.

4.2. Тест001. Сверка идентичности обновлений безопасности

4.2.1. Сверка идентичности обновлений безопасности проводится в случае возможности получения обновлений безопасности разными способами и (или) из различных источников.

4.2.2. Сверка идентичности обновлений безопасности предусматривает:

1) получение обновления безопасности разными способами и (или) получение обновлений безопасности из различных источников (например, с IP-адресов, расположенных на территории Российской Федерации, а также за ее пределами);

2) расчет контрольных сумм обновлений безопасности, полученных разными способами и (или) из различных источников;

3) сравнение обновлений безопасности, полученных разными способами и (или) из разных источников, путем сравнения их контрольных сумм.

4.2.3. По результатам выполнения теста должен быть сделан вывод об идентичности обновлений безопасности, полученных разными способами и (или) из разных источников. В случае схождения контрольных сумм обновлений тест считается успешно пройденным.

4.2.4. В случае выявления несоответствий в контрольных суммах обновлений безопасности, указанные обновления безопасности должны быть проанализированы путем ручного анализа обновлений безопасности.

4.3. Тест002. Проверка подлинности обновлений безопасности

4.3.1. Проверка подлинности обновлений безопасности проводится в случае наличия у Администратора безопасности 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.

4.3.2. Проверка подлинности обновлений предусматривает:

1) распаковку (расшифрование) файла(ов) обновления безопасности;

2) 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.

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

4.3.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены нарушения подлинности или подлинность которых невозможно проверить, должны быть проверены путем ручного анализа обновления безопасности.

4.4. Тест003. Антивирусный контроль обновлений безопасности

4.4.1. Антивирусный контроль обновлений безопасности заключается в

выявлении вредоносных компьютерных программ (вирусов) в исследуемом обновлении безопасности с использованием средств антивирусной защиты. Для проведения анализа необходимо использовать не менее двух средств антивирусной защиты разных разработчиков.

4.4.2. Антивирусный контроль обновлений безопасности предусматривает:

1) проверку обновлений безопасности средствами антивирусной защиты до их установки;

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

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

4.4.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены признаки вредоносной активности, должны быть проанализированы путем ручного анализа обновлений безопасности.

4.5. Тест004. Поиск опасных конструкций в обновлениях безопасности

4.5.1. Поиск опасных конструкций в обновлениях безопасности проводится в случае наличия у Администратора безопасности возможности получить файл(ы) обновления в распакованном (расшифрованном) виде до или после установки обновления в среде функционирования.

4.5.2. Поиск опасных конструкций в обновлениях безопасности предусматривает:

а) поиск опасных конструкций в обновлениях безопасности с применением индикаторов компрометации, YARA-правил и других способов;

б) контекстный поиск политических баннеров, лозунгов и другой противоправной информации в обновлениях безопасности.

4.5.3. Тест считается успешно пройденным в случае, если опасные конструкции не выявлены.

4.5.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены опасные конструкции, должны быть проанализированы путем ручного анализа обновлений безопасности.

4.5.5. При проведении ручного анализа Администратором безопасности должно быть исследовано назначение выявленных опасных конструкций, подтверждена или опровергнута их опасность.

4.6. Тест005. Мониторинг активности обновлений безопасности

4.6.1. Мониторинг активности обновлений безопасности заключается в получении и анализе сведений о поведении обновляемого программного, программно-аппаратного средства в результате его взаимодействия со средой функционирования или другими программами, а также анализе сведений о взаимодействии компонентов обновленного программного, программно-аппаратного средства.

4.6.2. Мониторинг активности обновлений безопасности проводится при

наличии возможности установки необходимых инструментов в среде тестирования обновляемого программного, программно-аппаратного средства.

4.6.3. Мониторинг активности обновлений безопасности предусматривает необходимость проведения:

а) анализа результатов выполнения системных вызовов обновленного программного обеспечения;

б) анализа получаемых и отправляемых обновленным программным, программно-аппаратным средством сетевых пакетов;

в) анализа состава файловой системы до и после установки обновления программного, программно-аппаратного средства;

г) сигнатурного поиска известных уязвимостей.

4.6.4. Тест считается успешно пройденным, если в ходе мониторинга активности обновлений безопасности не выявлено признаков недекларированных возможностей.

4.6.5. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены признаки недекларированных возможностей, должны быть проанализированы путем ручного анализа обновлений безопасности.

4.7. Тест006. Ручной анализ обновлений безопасности

4.7.1. Ручной анализ обновлений безопасности проводится в случае, если по результатам выполнения тестов:

а) выявлены различия в обновлениях безопасности, полученных разными способами и (или) из разных источников;

б) неуспешно пройден тест подлинности файла(ов) обновления безопасности;

в) выявлены признаки вредоносной активности в файлах обновления безопасности в результате антивирусного контроля или мониторинга активности обновления безопасности;

г) обнаружены опасные конструкции.

4.7.2. Ручной анализ обновлений безопасности проводится в отношении компонентов обновлений безопасности, в которых по результатам прохождения перечисленных выше тестов выявлены указанные в пункте 4.7.1 настоящего Регламента условия.

В случае если ручной анализ провести невозможно, Администратором безопасности делается вывод о наличии в обновлении безопасности признаков недекларированных возможностей.

4.7.3. Ручной анализ обновления безопасности предусматривает:

а) анализ логики работы (в том числе дизассемблирование или декомпиляция бинарного кода при наличии соответствующих возможностей);

б) исследование компонентов обновления безопасности с помощью отладчиков и трассировщиков;

в) проверки наличия в обновлении безопасности ключевой информации (паролей, секретных ключей и другой чувствительной информации);

г) статического и динамического анализа (при наличии исходных кодов обновлений безопасности).

4.7.4. По результатам прохождения теста Администратором безопасности делается вывод о подтверждении наличия или отсутствия выявленных ранее признаков недекларированных возможностей в компоненте(ах) обновляемого программного, программно-аппаратного средства.

4.7.5. В случае если по результатам ручного 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 Регламентом по выявлению, анализу и устранению уязвимостей, утвержденным приказом Департамента цифрового развития области №81-0 от 19 сентября 2023 г.

5. Оформление результатов тестирования

5.1. Результаты анализа обновлений безопасности оформляются Администратором безопасности 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 4 настоящего Регламента.

5.2. Отчет анализа обновления безопасности включает следующие сведения:

а) наименование обновления безопасности;

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

в) сведения об уязвимостях, на устранение которых направлено обновление безопасности;

г) наименование проведенных тестов;

д) результаты анализа (успешно/не успешно);

е) описание результатов анализа, включая средства проведения анализа, среду тестирования, выявленные признаки недекларированных возможностей, описание проведенных тестов.

5.3. Для тестов, по результатам которых выявлены признаки недекларированных возможностей, в отчет тестирования обновлений безопасности должна быть включена вся техническая информация, необходимая для пояснения выполненных в ходе исследования операций и результатов, полученных в ходе исследований (в том числе, при наличии, все отчеты инструментальных средств анализа и контроля).

В отношении выявленных признаков недекларированных возможностей Администратором безопасности определяются ограничения и условия, при которых установка обновления безопасности возможна. Указанные сведения включаются в отчет анализа обновлений безопасности.

6. Правила принятия решения об установке обновлений безопасности

При принятии решения о результатах тестирования обновлений

безопасности программных, программно-аппаратных средств Администратором безопасности обеспечивается следующий порядок определения возможности установки обновлений программных, программно-аппаратных средств.

6.1. Вывод о возможности установки обновлений безопасности.

6.1.1. В отношении проприетарных программных, программно-аппаратных средств и свободно распространяемого программного обеспечения вывод о возможности установки обновления безопасности формируется на основе выполнения следующих тестов:

- сверка идентичности обновлений безопасности и (или) проверка подлинности обновлений безопасности;
- антивирусный контроль обновлений безопасности и (или) поиск опасных конструкций безопасности;
- мониторинг активности обновлений безопасности.

6.1.2. В отношении обновлений безопасности программного обеспечения с открытым кодом вывод о возможности установки обновления безопасности формируется на основе выполнения следующих тестов:

- проверка подлинности обновлений безопасности;
- антивирусный контроль обновлений безопасности;
- мониторинг активности обновлений безопасности;
- ручной анализ обновлений безопасности.

6.2. Оценка результатов выполненных тестов.

6.2.1. Если по результатам выполнения тестов результаты реализации всех тестов являются положительными, обновление безопасности является безопасным и его установка возможна.

6.2.2. Если по результатам выполнения тестов результаты реализации одного или более тестов являются потенциально опасными и ни один из тестов не являются опасными, обновление безопасности может быть установлено при определенных ограничениях. Ограничения определяются Администратором безопасности по результатам тестирования и могут быть скорректированы для информационной системы с учетом особенностей ее архитектуры и функционирования.

6.2.3. Если по результатам выполнения тестов результаты реализации одного или более тестов являются опасными, обновление безопасности устанавливать не рекомендуется.