КОМИТЕТ
ЦИФРОВОГО РАЗВИТИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

от 18 октября 2023 года № 15

Об утверждении регламента
осуществления анализа и установки обновлений безопасности
программных, программно-аппаратных средств, находящихся в эксплуатации
на объектах критической информационной инфраструктуры органов
исполнительной власти Ленинградской области

В соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств от 28 октября 2022 года и Методикой тестирования обновлений безопасности программных, программно-аппаратных средств от 28 октября 2022 года, утвержденными Федеральной службой по техническому и экспортному контролю

п р и к а з ы в а ю:

1. Утвердить регламент осуществления анализа и установки обновлений безопасности программных, программно-аппаратных средств, находящихся в эксплуатации на объектах критической информационной инфраструктуры органов исполнительной власти Ленинградской области, согласно приложению к настоящему приказу.

2. Контроль за исполнением настоящего приказа возложить на первого заместителя председателя Комитета цифрового развития Ленинградской области – начальника департамента информационной безопасности и инфраструктуры.

Председатель
Комитета цифрового развития
Ленинградской области А.С. Сытник

Утвержден
приказом Комитета
цифрового развития
Ленинградской области
от 18.10.2023 № 15

(Приложение)

РЕГЛАМЕНТ
осуществления анализа и установки обновлений безопасности программных, программно-аппаратных средств, находящихся в эксплуатации на объектах критической информационной инфраструктуры органов исполнительной власти Ленинградской области

1. Общие положения

1.1. Настоящий регламент по анализу и установке обновлений безопасности программных, программно-аппаратных средств, находящихся в эксплуатации на объектах критической информационной инфраструктуры органов исполнительной власти Ленинградской области (далее – Регламент, КИИ, ОИВ ЛО) разработан с учетом рекомендаций, содержащихся в Методике тестирования обновлений безопасности программных, программно-аппаратных средств утвержденной Федеральной службой по техническому и экспортному контролю (далее - 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, автоматизированных системах управления, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центров обработки данных (далее – информационные системы). Регламент может быть использован для тестирования иных обновлений программных, программно-аппаратных средств по решению оператора информационной 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 КИИ 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. Решение об установке протестированных обновлений безопасности принимается оператором информационной системы с учетом результатов тестирования и оценки рисков нарушения функционирования информационной системы от установки таких обновлений.

1.6. 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 осуществления анализа обновлений безопасности программных, программно-аппаратных средств

2.1. Анализ обновлений безопасности проводится с целью своевременного выявления в них потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе отображение на устройствах вывода информации политических

баннеров, лозунгов, призывов и иной противоправной информации (далее – недекларированные возможности).

2.2. Анализу подлежат обновления безопасности, направленные на устранение уязвимостей, уровень критичности которых определен в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств утвержденной ФСТЭК России от 28 октября 2022 г.

2.3. Для целей настоящего регламента к признакам наличия 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.

2.4. Анализ обновлений безопасности организуется (проводится) специалистами по защите информации (информационной безопасности) оператора информационной системы (далее – исследователь).

2.5. Анализ обновлений безопасности включает:

а) подготовку к проведению тестирования обновлений безопасности;

б) проведение тестирования обновлений безопасности;

в) оформление результатов тестирования обновлений безопасности.

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

Способы получения обновлений безопасности определяются исследователем, исходя из его возможностей, и не рассматриваются в данном Регламенте. Анализ 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 осуществляет исследователь, исходя из его технических возможностей и угроз нарушения функционирования информационной системы.

2.7. При проведении анализа 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 анализу обновлений безопасности программных, программно-аппаратных средств

3.1. Общие требования к проведению тестирования.

3.1.1. В ходе проведения анализа обновлений безопасности должны выполняться следующие тесты:

а) сверка идентичности обновлений безопасности;

б) проверка подлинности обновлений безопасности;

в) антивирусный контроль обновлений безопасности;

г) поиск опасных конструкций в обновлениях безопасности;

д) мониторинг активности обновлений безопасности в среде функционирования;

е) ручной анализ обновлений безопасности.

3.1.2. Приведенные в пункте 3.1.1 настоящего Регламента тесты выполняются по решению исследователя, исходя из возможности получения обновлений безопасности разными способами и (или) из разных источников в распакованном (расшифрованном) виде, возможности исследователя по распаковке (расшифрованию) обновлений безопасности, а также наличия инструментальных средств анализа (контроля) и иных технических возможностей. По результатам тестирования исследователь описывает результаты каждого проведенного теста.

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

3.2. Сверка идентичности обновлений безопасности.

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

3.2.2. 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.

3.2.3. 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.

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

3.3. Проверка подлинности обновлений безопасности.

3.3.1. Проверка подлинности обновлений безопасности проводится в случае наличия у исследователя 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.

3.3.2. 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.

3.3.3. 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.

3.3.4. 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.

3.4. Антивирусный контроль обновлений безопасности.

3.4.1. 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.

3.4.2. 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.

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

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

3.5. Поиск опасных конструкций в обновлениях безопасности.

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

3.5.2. 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.

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

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

3.5.5. При проведении ручного анализа исследователем должно быть исследовано назначение выявленных опасных конструкций, подтверждена или опровергнута их опасность.

3.6. Мониторинг активности обновлений безопасности в среде тестирования.

3.6.1. Мониторинг активности обновлений безопасности в среде тестирования 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.

3.6.2. Мониторинг активности обновлений безопасности в среде функционирования проводится при наличии возможности установки необходимых инструментов в среде тестирования обновляемого программного, программно-аппаратного средства.

3.6.3. Мониторинг активности обновлений безопасности в среде тестирования 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.

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

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

3.7. Ручной анализ обновлений безопасности.

3.7.1. 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 в среде функционирования;

г) обнаружены опасные конструкции.

3.7.2. Ручной анализ обновлений безопасности проводится в отношении компонентов обновлений безопасности, в которых по результатам прохождения перечисленных выше тестов выявлены указанные в пункте 3.7.1 настоящего Регламента условия. В случае если ручной анализ провести невозможно, исследователем делается вывод о наличии в обновлении безопасности признаков недекларированных возможностей.

3.7.3. 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).

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

3.7.5. 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 установленным регламентом.

4. Оформление результатов тестирования

4.1. Результаты анализа обновлений безопасности оформляются 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 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.

4.3. 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 все отчеты инструментальных средств анализа и контроля). В отношении выявленных признаков недекларированных возможностей исследователем определяются ограничения и условия, при которых установка обновления безопасности возможна. Указанные сведения включаются в отчет анализа обновлений безопасности.

5. Установка обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения

При принятии решения о результатах тестирования обновлений безопасности программных, программно-аппаратных средств реализуется следующий порядок определения возможности установки обновлений программных, программно-аппаратных средств.

5.1 Вывод о возможности установки обновлений безопасности.

5.1.1. 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 в среде функционирования.

5.1.2. 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 в среде функционирования;

– ручной анализ обновлений безопасности.

5.2. Оценка результатов выполненных тестов.

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

5.2.2. 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 исследователем по результатам тестирования и могут быть уточнены оператором информационной системы с учетом особенностей ее архитектуры и функционирования.