П-277/2023

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

СОГЛАСОВАНО
Протокол заседания Совета Учреждения
от 06.06.2023г. № 24

Протокол заседания Совета обучающихся Учреждения
от 06.06.2023г. № 24

Протокол заседания Совета родителей Учреждения
от 06.06.2023г. № 24

УТВЕРЖДАЮ
И.о. директора
ГБПОУ «ТК им. Н.Д. Кузнецова»

_____Е.В. Буланкина
«06» июня 2023г.

Приказ № 372 о/д от 06.06.2023

Положение об организации деятельности (процесса) по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения в ГБПОУ «ТК им. Н.Д. Кузнецова»

1. Общие положения

1.1. Положение об организации деятельности (процесса) по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения (далее – Положение) определяет порядок организации деятельности по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - образовательная организация).

1.2. Настоящее Положение основано на следующих нормативных документах:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утв. Федеральной службой по техническому и экспортному контролю 28.10.2022) (далее – Методика);
- Устав образовательной организации и иные локальные нормативные акты.

1.3. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.4. Система защиты информации – это совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

1.5. Цель защиты информации – минимизировать (предотвратить) ущерб обладателю информации из-за возможных нарушений свойств ее безопасности.

1.6. Безопасное программное обеспечение – программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы.

2. Программные и программно-аппаратные средства защиты информации

2.1. Программные средства защиты информации – это специальные программы и программные комплексы, предназначенные для защиты информации в информационной системе.

2.2. К программным средствам защиты информации относятся:

- встроенные средства защиты информации – это средства, реализующие авторизацию и аутентификацию пользователей (вход в систему с использованием пароля), разграничение прав доступа, защиту программного обеспечения от копирования, корректность ввода данных в соответствии с заданным форматом и так далее. К данной группе средств относятся встроенные средства операционной системы по защите от влияния работы одной программы на работу другой программы при работе компьютера в мультипрограммном режиме, когда в его памяти может одновременно находиться в стадии выполнения несколько программ, попеременно получающих управление в результате возникающих прерываний;
- антивирусные программы – программы, предназначенные для обнаружения компьютерных вирусов, лечения или удаления инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.
- специализированные программные средства защиты информации от несанкционированного доступа – обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Специализированные программы предназначены для: защиты папок и файлов на компьютере; контроля за выполнением пользователями правил безопасности при работе с компьютером, выявления и пресечения попыток несанкционированного доступа к конфиденциальным данным, хранящимся на персональном компьютере; наблюдения за действиями, происходящими на контролируемом компьютере, работающем автономно или в локальной вычислительной сети;
- программные средства тестового контроля, предупреждающие и выявляющие дефекты, а также удостоверяющие надежность программ и оперативно защищающие функционирование программных средств при их проявлениях;
- межсетевые экраны (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней, что позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети.

2.3. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

2.4. Программно-аппаратные средства защиты – это способы контроля оборудования и программных средств от взлома, перехвата информации, несанкционированного подключения третьих лиц. Программно-аппаратные средства защиты в большинстве случаев охраняют информацию, доступ к которой ограничен на основании требований закона.

2.5. Обеспечение безопасности информации на программно-аппаратном уровне предохраняет сведения от несанкционированного доступа и снижает риски хищения и дальнейшего неправомерного использования полученных сведений.

2.6. Принцип работы системы: при попытке получения доступа к данным программа отправляет запрос к устройству, обеспечивающему работу ключа (токену, ридеру, электронному идентификатору, после подключения которого к компьютеру тот дает разрешение на работу), и функционирует только при его положительной реакции.

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

3.1. Управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования информационной системы осуществляются в ходе управления (администрирования) системой защиты информации информационной системы.

3.2. Тестирование программного обеспечения, в том числе с открытым исходным кодом, предназначается для устранения уязвимостей программных, программно-аппаратных средств (далее - обновления безопасности).

3.3. Общие требования к проведению тестирования.

3.3.1. В ходе проведения тестирования обновлений безопасности должны выполняться следующие тесты:

- сверка идентичности обновлений безопасности (Т001);
- проверка подлинности обновлений безопасности (Т002);
- антивирусный контроль обновлений безопасности (Т003);
- поиск опасных конструкций в обновлениях безопасности (Т004);
- мониторинг активности обновлений безопасности в среде функционирования (Т005);
- ручной анализ обновлений безопасности (Т006).

3.3.2. Приведенные в пункте 3.3.1 настоящего Положения 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.

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

3.3.4. Оператор информационной системы делает вывод о возможности установки обновления безопасности на основании результатов проведенных исследователем тестов.

3.4. Сверка идентичности обновлений безопасности (Т001)

3.4.1. Сверка идентичности обновлений безопасности (Т001) проводится в случае возможности получения обновлений безопасности разными способами и (или) из различных источников.

3.4.2. Сверка идентичности обновлений безопасности (Т001) предусматривает:

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

3.4.3. 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.

3.4.4. В случае выявления несоответствий в контрольных суммах обновлений безопасности, указанные обновления безопасности должны быть проанализированы путем ручного анализа обновлений безопасности (Т006).

3.5. Проверка подлинности обновлений безопасности (Т002)

3.5.1. Проверка подлинности обновлений безопасности (Т002) 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.

3.5.2. Проверка подлинности обновлений (T002) 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.

3.5.3. 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.

3.5.4. 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 (T006).

3.6. Антивирусный контроль обновлений безопасности (T003)

3.6.1. Антивирусный контроль обновлений безопасности (T003) 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.

3.6.2. Антивирусный контроль обновлений безопасности (T003) 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.

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

3.6.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены признаков вредоносной активности, должны быть проанализированы путем ручного анализа обновлений безопасности (T006).

3.7. Поиск опасных конструкций в обновлениях безопасности (T004)

3.7.1. Поиск опасных конструкций в обновлениях безопасности (T004) проводится в случае наличия у исследователя возможности получить файл(ы) обновления в распакованном (расшифрованном) виде до или после установки обновления в среде функционирования.

3.7.2. Поиск опасных конструкций в обновлениях безопасности (T004) предусматривает:

- поиск опасных конструкций в обновлениях безопасности с применением индикаторов компрометации, YARA-правил и других способов;
- контекстный поиск политических баннеров, лозунгов и другой противоправной информации в обновлениях безопасности.

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

3.7.4. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены опасные конструкции, должны быть проанализированы путем ручного анализа обновлений безопасности (T006).

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

3.8. Мониторинг активности обновлений безопасности в среде тестирования (T005)

3.8.1. Мониторинг активности обновлений безопасности в среде тестирования (Т005) 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.

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

3.8.3. Мониторинг активности обновлений безопасности в среде тестирования предусматривает необходимость проведения:

- анализа результатов выполнения системных вызовов обновленного программного обеспечения;
- анализа получаемых и отправляемых обновленным программным, программно-аппаратным средством сетевых пакетов;
- анализа состава файловой системы до и после установки обновления программного, программно-аппаратного средства;
- сигнатурного поиска известных уязвимостей.

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

3.8.5. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены признаки недекларированных возможностей, должны быть проанализированы путем ручного анализа обновлений безопасности (Т006).

3.9. 3.9. Ручной анализ обновлений безопасности (Т006)

3.9.1. Ручной анализ обновлений безопасности (Т006) проводится в случае, если по результатам выполнения тестов:

- выявлены различия в обновлениях безопасности, полученных разными способами и (или) из разных источников;
- неуспешно пройден тест подлинности файла(ов) обновления безопасности;
- выявлены признаки вредоносной активности в файлах обновления безопасности в результате антивирусного контроля или мониторинга активности обновления безопасности в среде функционирования;
- обнаружены опасные конструкции.

3.9.2. Ручной анализ обновлений безопасности проводится в отношении компонентов обновлений безопасности, в которых по результатам прохождения перечисленных выше тестов выявлены указанные в пункте 3.9.1 настоящего Положения условия.

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

3.9.3. Ручной анализ обновления безопасности предусматривает:

- анализ логики работы (в том числе дизассемблирование или декомпиляция бинарного кода при наличии соответствующих возможностей);
- исследование компонентов обновления безопасности с помощью отладчиков и трассировщиков;
- проверки наличия в обновлении безопасности ключевой информации (паролей, секретных ключей и другой чувствительной информации);
- статического и динамического анализа (при наличии исходных кодов обновлений безопасности).

3.9.4. 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.

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

4. Оформление результатов тестирования

4.1. Результаты тестирования 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 Положения.

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, выявленные признаки недекларированных возможностей, описание проведенных тестов.

Форма и содержание типового отчета тестирования обновления безопасности приведены в приложении № 2 Методики.

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 тестирования обновлений безопасности.

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

4.4. Отчеты тестирования обновления безопасности рекомендуется направлять на адрес электронной почты webmaster@bdu.fstec.ru с темой письма «Результаты тестирования обновлений». К результатам тестирования прилагаются контактные данные исследователя (имя, адрес электронной почты и (или) номер телефона).

Результаты тестирования могут направляться с использованием PGP-ключей, размещенных в разделе «Обратная связь» Банка данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

4.5. Оператор Банка данных угроз безопасности информации ФСТЭК России проводит верификацию результатов тестирования и размещает их в Банке данных угроз безопасности информации ФСТЭК России в течение 1 (одного) рабочего дня.

4.6. В случае если по результатам тестирования одного обновления безопасности разными исследователями получены разные результаты, размещению на сайте Банка данных угроз безопасности информации ФСТЭК России подлежат результаты тестирования, содержащие худший результат.

5. Правила принятия решения о результатах тестирования обновлений безопасности программных, программно-аппаратных средств

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

5.1.1. Вывод о возможности установки обновлений безопасности.

5.1.1.1. 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 (Т001) и (или) проверка подлинности обновлений безопасности (Т002);
- антивирусный контроль обновлений безопасности (Т003) и (или) поиск опасных конструкций безопасности (Т004);
- мониторинг активности обновлений безопасности в среде функционирования (Т005).

5.1.1.2. 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 (Т002);
- антивирусный контроль обновлений безопасности (Т003);
- мониторинг активности обновлений безопасности в среде функционирования (Т005);
- ручной анализ обновлений безопасности (Т006).

5.1.2. Оценка результатов выполненных тестов.

5.1.2.1. Если по результатам выполнения тестов результаты реализации всех тестов являются положительными (обозначены зеленым цветом), обновление безопасности является безопасным и его установка возможна.

5.1.2.2. Если по результатам выполнения тестов результаты реализации одного или более тестов являются потенциально опасными (обозначены желтым цветом) и ни один из тестов не являются опасными (не обозначен красным цветом), 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.

5.1.2.3. Если по результатам выполнения тестов результаты реализации одного или более тестов являются опасными (обозначены красным цветом), обновление безопасности устанавливать не рекомендуется.

По результатам тестирования обновлений безопасности могут быть сделаны выводы, указанные в таблице.

Сверка идентичности обновлений, полученных из разных источников (Т001)	**Проверка подлинности обновлений (Т002)**	**Антивирусный контроль обновлений (Т003)**	**Поиск опасных конструкций (Т004)**	**Мониторинг активности обновлений в среде функционирования (Т005)**	**Ручной анализ обновления (Т006)**
1	2	3	4	5	6
Обновления идентичны	Установлена подлинность обновлени	Не выявлены признаки вредоносной активности	Опасные конструкции не найдены	Не выявлено признаков недекларированных возможностей	Наличие недекларированных возможностей опровергнуто

	й				
Выявлены различия, объяснены исследователем и не вызывают опасности	Обновления не прошли проверку подлинности	Признаки вредоносной активности выявлены, сигнатура вредоносного программного обеспечения не определена	Найдены потенциально опасные конструкции, идентифицировать назначение которых не удалось	Найдены признаки недекларированных возможностей, идентифицировать назначение которых не удалось	Выявлены недекларированные возможности без деструктивного функционала
1	2	3	4	5	6
Выявлены различия, идентифицировать назначение которых не удалось		Признаки вредоносной активности выявлены, сигнатура вредоносного программного обеспечения определена	Опасные конструкции найдены	Найдены признаки недекларированных возможностей	Выявлены недекларированные возможности с неустановленным функционалом
Выявлены признаки недекларированных возможностей					Выявлены недекларированные возможности

Положение вступает в силу с момента его утверждения.

В случае необходимости в Положение могут вноситься изменения и дополнения по согласованию с Советом учреждения.

Разработчик:
заместитель директора по общим вопросам

_____/ Ю.Ю. Алексеев /

ЭП

О=ГБПОУ «ТК им. Н.Д. Кузнецова», CN=Сакеев А.Н., E=poo_tkk_su@samara.edu.ru
009939dcd2bdaa96fe
2023.06.08 10:36:11+04'00'