П-276/2023

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 выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в ГБПОУ «ТК им. Н.Д. Кузнецова»

1. Общие положения

1.1. Положение об организации деятельности (процесса) по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в ГБПОУ «ТК им. Н.Д. Кузнецова» (далее – Положение) определяет классификацию уязвимостей информационных систем, методику оценки уровня критичности уязвимостей программных, программно-аппаратных средств.

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 ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - образовательная организация) 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. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

1.5. 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

2. Классификация уязвимостей информационных систем

2.1. Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

2.2. В основе классификации уязвимостей информационных систем используются следующие классификационные признаки:

- область происхождения уязвимости;
- типы недостатков информационных систем;
- место возникновения (проявления) уязвимости информационных систем.

2.3. В качестве уязвимых компонентов информационных систем рассматриваются общесистемное (общее), прикладное, специальное программное обеспечение, технические средства, сетевое (коммуникационное, телекоммуникационное) оборудование, средства защиты информации.

2.4. Помимо классификационных признаков уязвимостей информационных систем используются поисковые признаки (основные и дополнительные). Поисковые признаки предназначены для организации расширенного поиска в базах данных уязвимостей.

2.5. К основным поисковым признакам уязвимостей информационных систем относятся следующие:

- наименование операционной системы и тип аппаратной платформы;
- наименование программного обеспечения и его версия;
- степень опасности уязвимости.

2.6. К дополнительным поисковым признакам уязвимостей информационных систем относятся следующие:

- язык программирования;
- служба (порт), которая(ый) используется для функционирования программного обеспечения.

2.7. Уязвимости информационных систем по области происхождения подразделяются на следующие классы:

- уязвимости кода;
- уязвимости конфигурации;
- уязвимости архитектуры;
- организационные уязвимости;
- многофакторные уязвимости

2.8. Уязвимости информационных систем по типам недостатков информационных систем подразделяются на следующие:

- недостатки, связанные с неправильной настройкой параметров программного обеспечения;
- недостатки, связанные с неполнотой проверки вводимых (входных) данных;
- недостатки, связанные с возможностью прослеживания пути доступа к каталогам;
- недостатки, связанные с возможностью перехода по ссылкам;
- недостатки, связанные с возможностью внедрения команд операционной системы;
- недостатки, связанные с межсайтовым скриптингом (выполнением сценариев);
- недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки;
- недостатки, связанные с внедрением произвольного кода;
- недостатки, связанные с переполнением буфера памяти;
- недостатки, связанные с неконтролируемой форматной строкой;
- недостатки, связанные с вычислениями;
- недостатки, приводящие к утечке/раскрытию информации ограниченного доступа;
- недостатки, связанные с управлением полномочиями (учетными данными);
- недостатки, связанные с управлением разрешениями, привилегиями и доступом;
- недостатки, связанные с аутентификацией;

- недостатки, связанные с криптографическими преобразованиями (недостатки шифрования);
- недостатки, связанные с подменой межсайтовых запросов;
- недостатки, приводящие к «состоянию гонки»;
- недостатки, связанные с управлением ресурсами;
- иные типы недостатков.

2.9. Уязвимости информационных систем по месту возникновения (проявления) подразделяются на следующие:

- уязвимости в общесистемном (общем) программном обеспечении;
- уязвимости в прикладном программном обеспечении;
- уязвимости в специальном программном обеспечении;
- уязвимости в технических средствах;
- уязвимости в портативных технических средствах;
- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании;
- уязвимости в средствах защиты информации.

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

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

3.2. 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.

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

3.4. Оценка уровня критичности уязвимостей программных, программно-аппаратных средств применительно к конкретной 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 (v).

3.5. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе v осуществляется по следующей формуле:

$$V = I_{CVSS} \times I_{exp},$$

где I_{cvss} - показатель, характеризующий уровень опасности уязвимости;

I_{inft} - показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы.

3.6. Показатель I_{cvss} определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1.

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

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

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

Показатель I_{cvss} может быть рассчитан с использованием калькулятора, содержащегося в Банке данных угроз безопасности информации ФСТЭК России в разделе «Уязвимости».

В калькуляторе необходимо определить (уточнить) базовые, временные и контекстные метрики применительно к конкретной системе и сети (рисунки 1, 2, 3 Методики).

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

3.7. Показатель I_{inft} определяется по следующей формуле:

$I_{inft} = k*K + l*L + p*P$, где

K - показатель, характеризующий тип компонента информационной системы, подверженного уязвимости;

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

P - показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы;

k, l, p - весовые коэффициенты показателей.

Расчет весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на информационную систему, проводится в соответствии с таблицей 1 Методики.

3.8. По результатам расчета уровень критичности уязвимости применительно к конкретной информационной системе принимает значения, указанные в таблице:

п/п	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
	$7,0 \le V \le 10,0$	Критичный
	$4,5 \le V < 7,0$	Высокий
	$1,5 \le V < 4,5$	Средний

	V < 1,5	Низкий

4. Принятие мер защиты информации, направленных на устранение уязвимостей

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

4.2. В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен критический уровень, рекомендуется принять меры по их устранению в течение часов (до 24 часов).

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен высокий уровень критичности, рекомендуется принять меры по их устранению в течение дней (до 7 дней).

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен средний уровень критичности, рекомендуется принять меры по их устранению в течение недель (до 4 недель).

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен низкий уровень критичности, рекомендуется принять меры по их устранению в течение месяца (до 4 месяцев).

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

4.4. В случае если уязвимости содержатся в зарубежных программных, программно-аппаратных средствах или программном обеспечении с открытым исходным кодом, решение об установке обновления такого программного обеспечения, программно-аппаратного средства принимается оператором информационной системы с учетом результатов тестирования этого обновления, проведенного в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28.10.2022, и оценки ущерба от нарушения функционирования информационной системы по результатам установки обновления.

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

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

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

- изменение конфигурации уязвимых компонентов информационной системы, в том числе в части предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;
- ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей (например, отключение уязвимых служб и сетевых протоколов);
- резервирование компонентов информационной системы, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;
- использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление в информационной системе признаков эксплуатации уязвимостей;
- мониторинг информационной безопасности и выявление событий безопасности информации в информационной системе, связанных с возможностью эксплуатации уязвимостей.

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

O=ГБПОУ «ТК им. Н.Д. Кузнецова», CN=Сакеев А.Н., E=poo_tkk_su@samara.edu.ru
009939dcd2bdaa96fe
2023.06.08 10:35:22+04'00'