Научная статья
УДК 004.65.056.5
https://doi.org/10.35266/1999-7604-2025-2-9

CC BY 4.0

Анализ существующих источников знаний в виде баз данных уязвимостей автоматизированных систем

Владимир Олегович Шабля, Сергей Александрович Коноваленко, Никита Андреевич Галямин✉, Егор Олегович Орлов
Краснодарское высшее военное училище, Краснодар, Россия

Аннотация. В статье представлен анализ существующих источников знаний в виде баз данных уязвимостей автоматизированных систем как отечественного, так и иностранного производства. Рассмотрены различные базы данных уязвимостей, такие как Федеральная служба по техническому и экспортному контролю России, CVE, NVD, VulDB, JVN и CNNVD, и произведено сравнение по ключевым параметрам. Также в статье представлен анализ машинных переводчиков текста, таких как Yandex Translate, Google Translate, SDL Trados Studio, OmegaT, DeepL Translate, ABBYY Lingvo, для выбора решения, способного осуществлять точный перевод информации об уязвимостях из баз данных уязвимостей специализированных средств иностранного производства с учетом терминологического аппарата области знаний «информационная безопасность». Представлено программное решение создания объединенной базы данных уязвимостей и актуализации информации в ней путем консолидации информации об уязвимостях автоматизированных систем из существующих баз данных уязвимостей для дальнейшей обработки содержащихся в ней данных.

Ключевые слова: база данных уязвимостей, информационная безопасность, автоматизированная система

Для цитирования: Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О. Анализ существующих источников знаний в виде баз данных уязвимостей автоматизированных систем // Вестник кибернетики. 2025. Т. 24, № 2. С. 74–82. https://doi.org/10.35266/1999-7604-2025-2-9.

Original article

Analysis of existing knowledge sources in form of vulnerability databases for automated systems

Vladimir O. Shablya, Sergey A. Konovalenko, Nikita A. Galyamin✉, Egor O. Orlov
Krasnodar Higher Military School, Krasnodar, Russia

Abstract. The article presents an analysis of existing knowledge sources in the form of vulnerability databases for automated systems of both Russian and foreign production. Various vulnerability databases, such as the FSTEC of Russia, CVE, NVD, VulDB, JVN and CNNVD, are reviewed and compared by key parameters. The article also presents an analysis of machine text translators such as Yandex Translate, Google Translate, SDL Trados Studio, OmegaT, DeepL Translate, ABBYY Lingvo to select a solution capable of accurate translation of vulnerability information from vulnerability databases of specialized foreign-made tools, taking into account the terminology of the field of knowledge “information security”. We present a method for creating and updating a single vulnerability database by consolidating information security vulnerability information from existing databases for further data processing.

Keywords: vulnerability database, information security, automated system

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

***For citation*:** Shablya V. O., Konovalenko S. A., Galyamin N. A., Orlov E. O. Analysis of existing knowledge sources in form of vulnerability databases for automated systems. *Proceedings in Cybernetics*. 2025;24(2):74–82. https://doi.org/10.35266/1999-7604-2025-2-9.

ВВЕДЕНИЕ

Несмотря на совершенствование различных аспектов в области информационной безопасности, с течением времени уровень и количество компьютерных атак и угроз на автоматизированные системы остается на достаточно высоком уровне. Стоит отметить, что на сегодняшний день существует огромное количество подходов к противодействию вышеобозначенным негативным факторам. Согласно «ГОСТ Р ИСО/МЭК 15408-1–2012» безопасность связана с защитой активов, которые, в свою очередь, представляют ценность для их владельцев [1]. Среда, в которой размещаются эти активы, называется средой функционирования, под которой будем понимать автоматизированные системы. В данной статье будем придерживаться этой точки зрения.

МАТЕРИАЛЫ И МЕТОДЫ

Объектом анализа являются источники знаний в виде баз данных уязвимостей автоматизированных систем. Под уязвимостью стоит понимать недостаток, изъян или слабость в архитектуре, реализации или эксплуатационных процедурах автоматизированных систем, который при определенных условиях может быть использован нарушителями информационной безопасности для осуществления негативного воздействия на конфиденциальность, целостность и (или) доступность информации [2]. В статье отражены результаты анализа следующих классов уязвимостей: многофакторных уязвимостей, уязвимостей кода, а также уязвимостей архитектуры автоматизированных систем. Базы данных уязвимостей представляют собой открытые реестры информации об уязвимостях в программном обеспечении и аппаратных платформах автоматизированных систем. Анализ проводится путем сравнения баз данных уязвимостей автоматизированных систем между собой по различным характеристикам. Для этого был произведен сбор данных из выбранных баз данных уязвимостей автоматизированных систем, осуществлена классификация собранных данных по характеристикам, выполнен сравнительный анализ баз данных уязвимостей автоматизированных систем по выделенным характеристикам и дана оценка преимуществ и недостатков каждой базы данных уязвимостей автоматизированных систем. Выбранный метод анализа позволил комплексно оценить различные базы данных уязвимостей автоматизированных систем с учетом их структуры и предоставляемой информации.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

В настоящее время выделяют несколько взаимосвязанных источников знаний о состоянии процесса функционирования автоматизированных систем, которые, в свою очередь, характеризуются конфигурационными параметрами автоматизированных систем, представляющими собой настройки программного обеспечения, входящего в состав автоматизированной системы. Контроль вышеуказанных параметров (например, измерение или обработка) может быть осуществлен посредством специализированных программных или программно-аппаратных средств как в автоматизированном режиме, так и под управлением человека [3]. Функция контроля состояния процесса функционирования автоматизированных систем позволяет оценивать процесс функционирования автоматизированных систем, а также производить эффективный анализ защищенности вышеуказанных систем. Графически представим связь между существующими источниками знаний о состоянии процесса функционирования автоматизированных систем, а также выделим источники знаний в виде баз данных уязвимостей автоматизированных систем на рис. 1.

Стоит отметить, что наиболее эффективным подходом к анализу данных, связанных с уязвимостями автоматизированных систем,

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

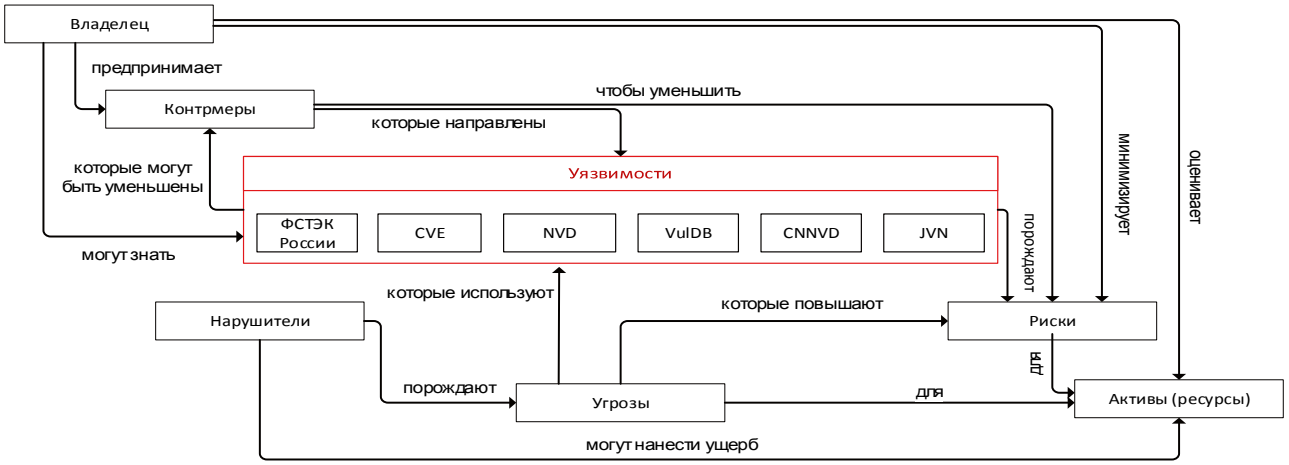

Рис. 1. Связь между существующими источниками знаний о состоянии процесса функционирования автоматизированных систем

Примечание: составлено авторами.

с точки зрения полноты информации будем считать использование не только базы данных уязвимостей ФСТЭК России, а также базы данных уязвимостей иностранного производства [4–9]. С этой целью проведем анализ отечественной и иностранных баз данных уязвимостей автоматизированных систем, результат которых сведем в табл. 1.

Выделим особенности различных баз данных уязвимостей автоматизированных систем, приведенных в табл. 1, и сведем их в табл. 2.

Таблица 1

Результаты анализа существующих баз данных уязвимостей автоматизированных систем отечественного и иностранного производства

Характеристики	**Наименование баз данных уязвимостей автоматизированных систем**					
	ФСТЭК России	**CVE**	**NVD**	**VulDB**	**JVN**	**CNNVD**
Количество уязвимостей автоматизированных систем на 03.11.2024	62345	240830	253570	282391	292004	266098
Способ распространения (бесплатно/платно)	+	+	+	+/-	+	+
Гибкость поиска уязвимостей автоматизированных систем	+	-	-	+	+	+/-
Возможность импорта данных об уязвимостях автоматизированных систем	+	+	+	+/-	-	+
Перечень программного обеспечения (аппаратных платформ), для которого существует уязвимость автоматизированных систем	+	-	+	+	+	-
Тип программного обеспечения, в котором обнаружена уязвимость автоматизированных систем	+	-	-	+	-	+
Статус уязвимости автоматизированных систем	+	-	+	+	-	-
Сведения о финансовых рисках эксплуатации уязвимости автоматизированных систем	-	-	-	+	-	-

Примечание: «+» – характеристика присутствует, «-» – характеристика отсутствует, «+/-» – характеристика присутствует не в полном объеме. Составлено авторами.

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

Таблица 2

Особенности различных существующих баз данных уязвимостей автоматизированных систем отечественного и иностранного производства

Наименование базы данных уязвимостей автоматизированных систем	Особенности базы данных уязвимостей автоматизированных систем
ФСТЭК России	Информация доступна на русском языке, присутствует возможность импорта базы данных уязвимостей автоматизированных систем в формате XLSX и XML
CVE	Все широко известные базы данных уязвимостей присваивают уязвимостям автоматизированных систем идентификаторы из базы данных уязвимостей CVE
NVD	Присутствует возможность импорта базы данных уязвимостей автоматизированных систем с помощью API, используя запрос методом GET по HTTP-протоколу
VulDB	Наличие платной подписки, открывающая возможности неограниченного просмотра и поиска уязвимостей автоматизированных систем, неограниченный доступ к API и многое другое
JVN	Имеет уникальные идентификаторы уязвимостей информационной безопасности JVNVU и JVNTA
CNNVD	Информация доступна на китайском языке, присутствует возможность импорта информации в формате XML при условии авторизации на web-сайте

Примечание: составлено авторами.

Проанализировав табл. 1, можно прийти к выводу, что использование только отечественной базы данных уязвимостей является недостаточным решением для получения полной информации о состоянии процесса функционирования автоматизированных систем, т. к. база данных уязвимостей ФСТЭК России содержит намного меньше записей об уязвимостях, чем базы данных иностранного производства, и не содержит определенные записи (рис. 2), которые имеются в иностранных базах данных уязвимостях (рис. 3), также информация об уязвимостях в базе данных уязвимостей ФСТЭК России может быть неполной (рис. 4) относительно информации, представленной в базах данных уязвимостей иностранного производства (рис. 5).

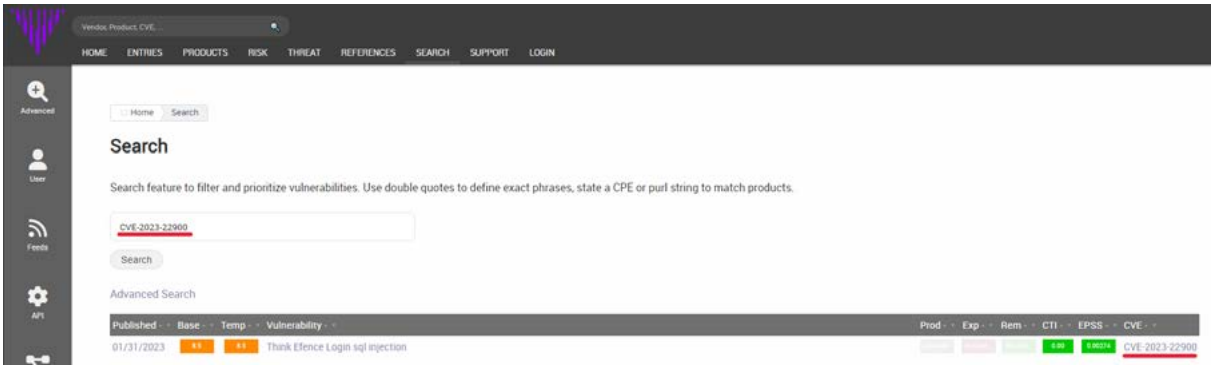

Рис. 2. Ответ на поисковый запрос «CVE-2023-22900» в базе данных уязвимостей автоматизированных систем VulDB
Примечание: составлено авторами.

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

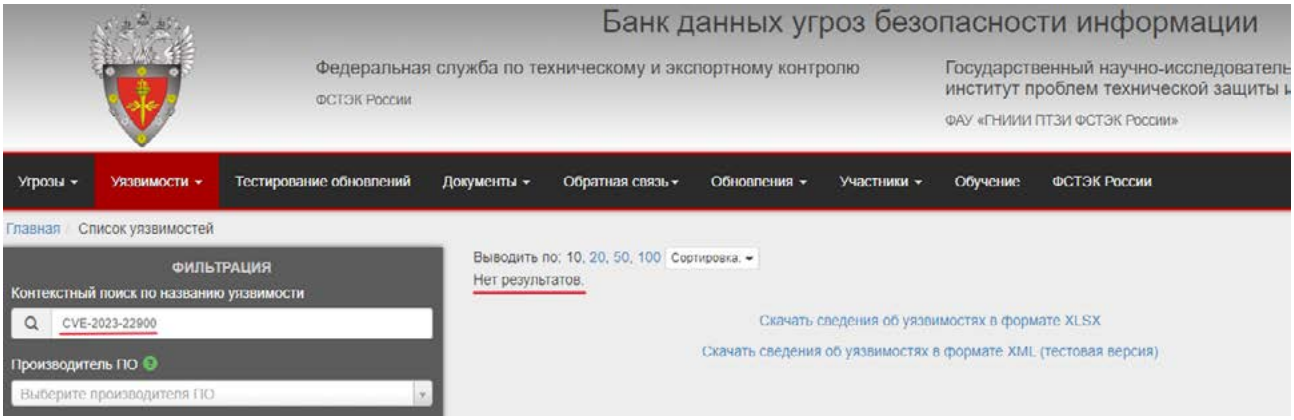

Рис. 3. Ответ на поисковый запрос «CVE-2023-22900» в базе данных уязвимостей автоматизированных систем ФСТЭК России

Примечание: составлено авторами.

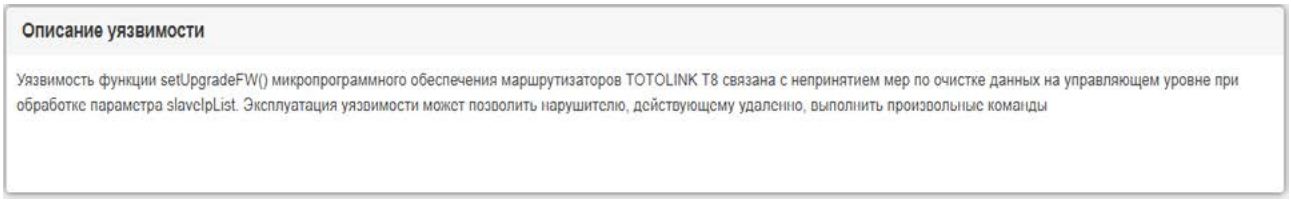

Рис. 4. Описание уязвимости «CVE-2023-24154» в базе данных уязвимостей автоматизированных систем ФСТЭК России

Примечание: составлено авторами.

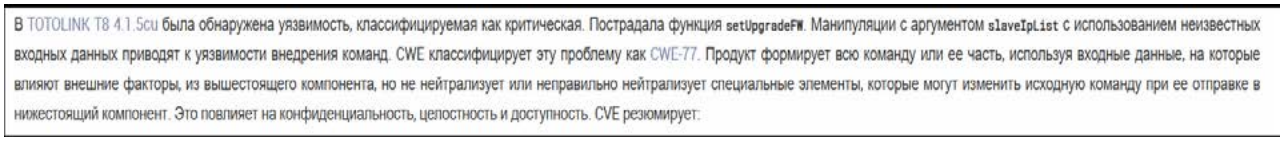

Рис. 5. Описание уязвимости «CVE-2023-24154» в базе данных уязвимостей автоматизированных систем VulDB

Примечание: составлено авторами.

Также в процессе сбора и агрегации записей из вышеуказанных баз данных уязвимостей была выявлена проблема, связанная со сложностью повышения оперативности процесса извлечения данных из различных баз данных уязвимостей путем использования HTTP API и парсинга веб-сайтов для извлечения данных. Вышеуказанные проблемы можно решить, используя разработанные «Модуль формирования базы данных уязвимостей специализированных средств», а также «Модуль парсинга баз данных уязвимостей специализированных средств» [10, 11].

Проблема повышения оперативности процесса извлечения записей из различных баз данных уязвимостей решается при применении модуля парсинга баз данных уязвимостей за счет автоматического извлечения по запросу данных об уязвимостях автоматизированных систем из различных баз данных уязвимостей (рис. 6). Проблему полноты информации при ее анализе решает модуль объединения баз данных уязвимостей за счет консолидации записей из различных баз данных уязвимостей, что, в свою очередь, позволяет обогатить информацию об уязвимостях за счет взаимного дополнения и повышает полноту обрабатываемых данных о состоянии процесса функционирования автоматизированных систем (рис. 7).

При анализе баз данных уязвимостей автоматизированных систем иностранного производства у специалиста по информационной безопасности, не обладающего должным уровнем знаний иностранного языка, на котором учтена информация в базах данных уязвимостей автоматизированных систем, возникает необходимость в использовании машинного переводчика текста.

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

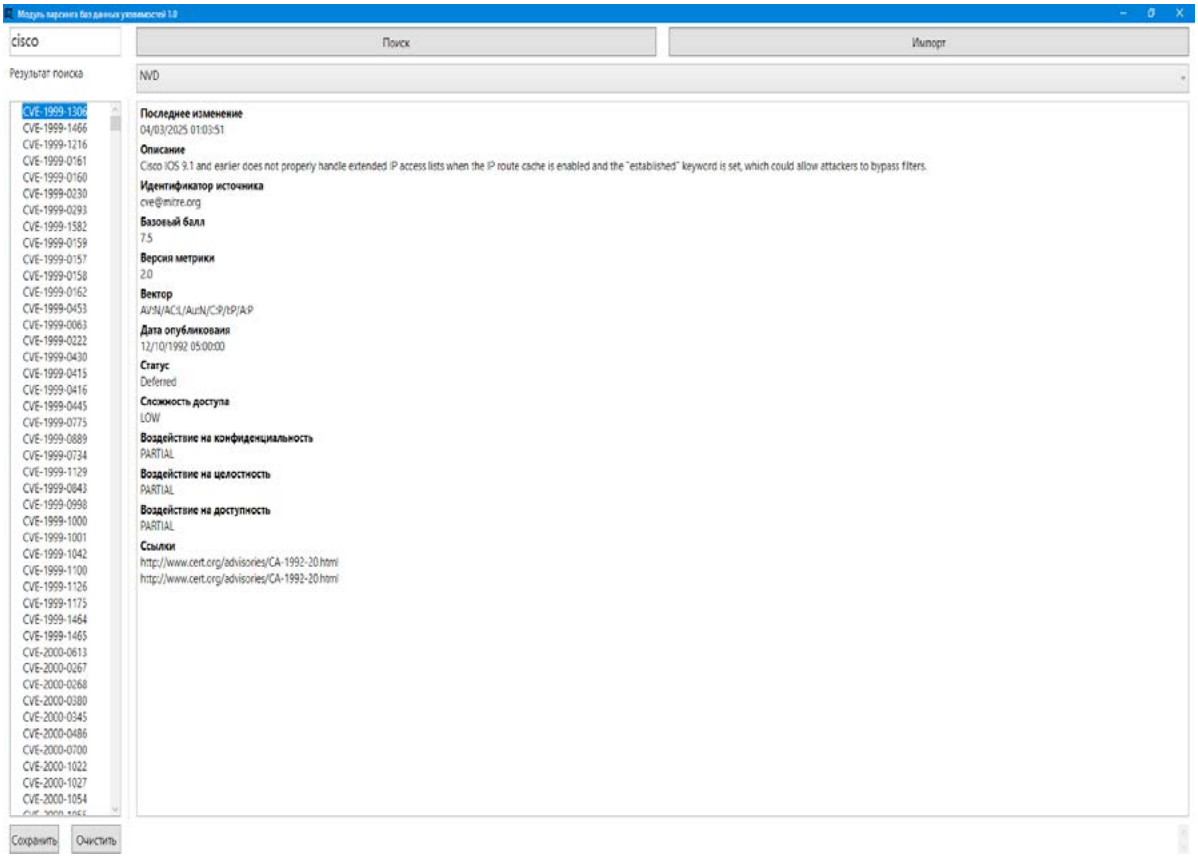

Рис. 6. Пример поиска информации в модуле парсинга баз данных уязвимостей специализированных средств

Примечание: составлено авторами.

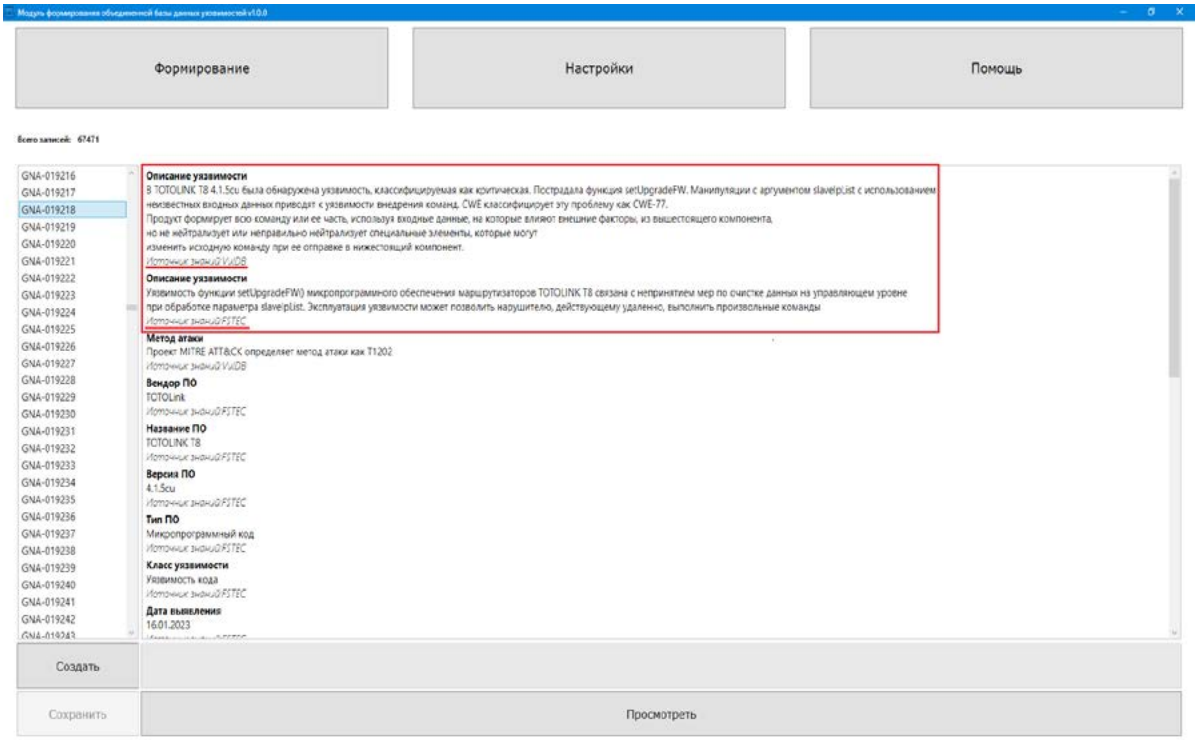

Рис. 7. Информация об уязвимости «CVE-2023-24154», представленная в модуле формирования базы данных уязвимостей специализированных средств

Примечание: составлено авторами.

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

В связи с этим рассмотрим ряд машинных переводчиков текста, способных обеспечить перевод информации с иностранного языка об уязвимостях информационной безопасности, на язык, которым владеет специалист по информационной безопасности (табл. 3) [12–16].

Таблица 3

Анализ существующих машинных переводчиков текста, способных выполнить перевод уязвимостей автоматизированных систем с иностранного языка на русский

Характеристики	Машинный переводчик текста					
	SDL Trados Studio	**OmegaT**	**ABBYY Lingvo**	**DeepL Translate**	**Google Translate**	**Yandex Translate**
Способ распространения (бесплатно/платно)	+/-	+	+/-	+/-	+/-	+
Использование искусственного интеллекта для перевода текста	+	-	-	+	+	+
Гибкость настройки перевода	+	+	+/-	+/-	+/-	+/-
Поддержка экспорта различных форматов файла для перевода	+	+/-	-	+	+	+
Возможность офлайн-доступа	+	+	+	-	+	+/-

Примечание: «+» – характеристика присутствует, «-» – характеристика отсутствует, «+/-» – характеристика присутствует не в полном объеме. Составлено авторами.

Приведем пример перевода описания уязвимости автоматизированных систем существующими машинными переводчиками текста. Для этого возьмем описание уязвимости автоматизированных систем с идентификатором «CVE-2023-22900» из базы данных уязвимостей автоматизированных систем CNNVD, исходный текст которого: «存在SQL注入漏洞┌漏洞源于在登┌功能┌用┌┌入的┌┌不足攻┌者利用┌漏洞可以注入任意SQL命令以┌┌修改或┌除┌据┌».

Пример перевода описания уязвимости автоматизированных систем при использовании машинного переводчика текста Yandex Translate: «Существует уязвимость SQL-инъекции, которая связана с недостаточной проверкой пользовательского ввода в функции входа в систему. Злоумышленник может использовать эту уязвимость для ввода любой SQL-команды для доступа, изменения или удаления базы данных».

Пример перевода описания уязвимости автоматизированных систем при использовании машинного переводчика текста Google Translate: «Существует уязвимость SQL-инъекции, возникающая из-за недостаточной проверки вводимых пользователем данных в функции входа в систему. Злоумышленник может воспользоваться этой уязвимостью для внедрения произвольных команд SQL для доступа, изменения или удаления базы данных».

Пример перевода описания уязвимости автоматизированных систем при использовании машинного переводчика текста DeepL Translator: «Уязвимость SQL-инъекции существует из-за недостаточной проверки пользовательского ввода в функции входа в систему. Злоумышленник может использовать эту уязвимость для внедрения произвольных SQL-команд для доступа, изменения или удаления базы данных».

Проанализировав перевод текста различными машинными переводчиками текста, придем к выводу, что результат работы у всех машинных переводчиков текста различен и специалисту по информационной безопасности рекомендуется выбирать наиболее подходящий результат, корректировать его с учетом особенностей предметной области (в данной статье это информационная безопасность) и различий между отечественными и иностранными терминологическими база-

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

ми нормативно-правовых актов в области информационной безопасности.

ЗАКЛЮЧЕНИЕ

Таким образом, проведенный анализ существующих баз данных уязвимостей автоматизированных систем свидетельствует о том, что использование в качестве источника знаний о состоянии процесса функционирования автоматизированных систем только отечественной базы данных уязвимостей не в полной мере обеспечивает требуемый уровень полноты знаний и оперативности процесса извлечения записей из баз данных уязвимостей, что обуславливает необходимость использования нескольких баз данных уязвимостей (отечественного и иностранного производства) автоматизированных систем. Немаловажным фактором является также проблема, связанная с необходимостью обработки большого объема данных (знаний) из различных баз данных уязвимостей автоматизированных систем. В статье были представлены разработанные программные решения данных проблем в виде модуля, объединяющего данные (знания) из различных баз данных уязвимостей в одну базу данных уязвимостей, в которой будет скоррелирована и сохранена наиболее полная информация об интересующих специалиста по информационной безопасности уязвимостях автоматизированных систем и модуля парсинга баз данных уязвимостей для повышения оперативности процесса извлечения записей из баз данных уязвимостей отечественного и иностранного производства.

Список источников

1. ГОСТ Р ИСО/МЭК 15408-1–2012. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. М. : Стандартинформ, 2014. 50 с.
2. ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. М. : Стандартинформ, 2018. 7 с.
3. Коноваленко С. А., Шабля В. О., Титов Г. О. Анализ методов контроля состояния процесса функционирования сложных технических систем // Наукосфера. 2021. № 2. С. 224–230.
4. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю России (ФСТЭК России). URL: https://bdu.fstec.ru/vul (дата обращения: 03.11.2024).
5. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org (дата обращения: 03.11.2024).
6. National Vulnerability Database. URL: https://nvd.nist.gov/search (дата обращения: 03.11.2024).
7. Vulnerability Database. URL: https://vuldb.com (дата обращения: 03.11.2024).
8. Japan Vulnerability Notes. URL: http://jvn.jp/en (дата обращения: 03.11.2024).
9. National Information Security Vulnerability Database. URL: https://www.cnnvd.org.cn/home/childHome (дата обращения: 03.11.2024).
10. Шабля В. О., Коноваленко С. А., Орлов Е. О. и др. Модуль формирования базы данных уязвимостей специализированных средств : патент № 2025612554 Рос. Федерация № 2025610374 заявл. 10.01.2025 ; опубл. 31.01.2025. URL: https://www.elibrary.ru/download/elibrary_80410736_65539681.PDF (дата обращения: 12.04.2025).

References

1. GOST (State Standard) R ISO/IEC 15408-1–2012. Security methods and tools. Information technology security assessment criteria. Part 1. Introduction and general model. Moscow: Standartinform; 2014. 50 p. (In Russ.).
2. GOST (State Standard) R 56545–2015. Information protection. Information system vulnerabilities. Vulnerability description rules. Moscow: Standartinform; 2018. 7 p. (In Russ.).
3. Konovalenko S. A., Shablya V. O., Titov G. O. Analysis of methods for control of the condition of the functioning process of complex technical systems. *Naukosfera*. 2021;(2):224–230. (In Russ.).
4. Bank dannykh ugroz bezopasnosti informatsii. Federalnaya sluzhba po tekhnicheskomu i eksportnomu kontrolyu Rossii (FSTEK Rossii). URL: https://bdu.fstec.ru/vul (accessed: 03.11.2024). (In Russ.).
5. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org (accessed: 03.11.2024).
6. National Vulnerability Database. URL: https://nvd.nist.gov/search (accessed: 03.11.2024).
7. Vulnerability Database. URL: https://vuldb.com (accessed: 03.11.2024).
8. Japan Vulnerability Notes. URL: http://jvn.jp/en (accessed: 03.11.2024).
9. National Information Security Vulnerability Database. URL: https://www.cnnvd.org.cn/home/childHome (accessed: 03.11.2024).
10. Shablya V. O., Konovalenko S. A., Orlov E. O. et al. Module for forming a database of vulnerabilities of specialized tools. RU Patent No. 2025612554 No. 2025610374, filed January 10, 2025, issued January 31, 2025. URL: https://www.elibrary.ru/download/elibrary_80410736_65539681.PDF (accessed: 12.04.2025). (In Russ.).

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025

11. Шабля В. О., Коноваленко С. А., Орлов Е. О. и др. Модуль парсинга баз данных уязвимостей специализированных средств : патент 2025612938 Рос. Федерация № 2025610328 заявл. 10.01.2025 ; опубл. 05.02.2025. URL: https://www.elibrary.ru/download/elibrary_80411121_75697915.PDF (дата обращения: 12.04.2025).
12. Trados Studio. URL: https://www.trados.com/product/studio (дата обращения: 03.11.2024).
13. OmegaT. URL: https://omegat.org/ (дата обращения: 03.11.2024).
14. DeepL Translate. URL: https://www.deepl.com/translator (дата обращения: 03.11.2024).
15. Google Translate. URL: https://translate.google.ru (дата обращения: 03.11.2024).
16. Yandex Translate. URL: https://translate.yandex.ru (дата обращения: 03.11.2024).
17. ABBYY Lingvo. URL: https://lingvo.ru (дата обращения: 03.11.2024).

11. Shablya V. O., Konovalenko S. A., Orlov E. O. et al. Module for parsing databases of vulnerabilities of specialized tools. RU Patent 2025612938 No. 2025610328, filed January 10, 2025, issued February 5, 2025. URL: https://www.elibrary.ru/download/elibrary_80411121_75697915.PDF (accessed: 12.04.2025). (In Russ.).
12. Trados Studio. URL: https://www.trados.com/product/studio (accessed: 03.11.2024).
13. OmegaT. URL: https://omegat.org/ (accessed: 03.11.2024).
14. DeepL Translate. URL: https://www.deepl.com/translator (accessed: 03.11.2024).
15. Google Translate. URL: https://translate.google.ru (accessed: 03.11.2024). (In Russ.).
16. Yandex Translate. URL: https://translate.yandex.ru (accessed: 03.11.2024). (In Russ.).
17. ABBYY Lingvo. URL: https://lingvo.ru (accessed: 03.11.2024). (In Russ.).

Информация об авторах

В. О. Шабля – преподаватель;
ne.404@mail.ru
С. А. Коноваленко – кандидат технических наук;
konovalenko_rcf@mail.ru
Н. А. Галямин – студент;
galyamin03@mail.ru✉
Е. О. Орлов – студент;
egor535553@mail.ru

About the authors

V. O. Shablya – Lecturer;
ne.404@mail.ru
S. A. Konovalenko – Candidate of Sciences (Engineering);
konovalenko_rcf@mail.ru
N. A. Galyamin – Student;
galyamin03@mail.ru✉
E. O. Orlov – Student;
egor535553@mail.ru

© Шабля В. О., Коноваленко С. А., Галямин Н. А., Орлов Е. О., 2025