РАЗРАБОТКА ТИПОВОЙ МЕТОДИКИ АНАЛИЗА УЯЗВИМОСТЕЙ В ВЕБ-ПРИЛОЖЕНИЯХ ПРИ ПРОВЕДЕНИИ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Барабанов А.В.[1], Федичев А.В.[2]

Статья посвящена вопросам оценки соответствия защищенных веб–приложений требованиям по безопасности информации. Представлено исследование существующих подходов к приведению анализа уязвимостей веб–приложений при проведении сертификационных испытаний по требованиям безопасности информации. На основе международного стандарта ISO/IEC TR 20004 с учетом особенностей отечественной системы сертификации средств защиты информации разработана методика анализа уязвимостей веб–приложения на основе применения сценариев типовых атак на веб–приложения с учетом сформированного в работе перечня потенциальных уязвимостей веб–приложений. Выполнены экспериментальные исследования предлагаемой методики и показано сокращение времени анализа уязвимостей по сравнению с известными способами в среднем на 4%. Сделан вывод о необходимости использования предложенной методики в рамках системы производства веб–приложений.

***Ключевые слова**: сертификация программного обеспечения, защита информации, анализ уязвимостей, веб–приложение.*

Введение

В последнее время веб-технологии стали активно использоваться для выполнения задач, критичных с точки зрения обеспечения защиты информации (например, выполнение банковских операций, получение различных государственных услуг) [1-3]. Для информационных систем, реализующих веб-технологии, все более актуальными становится угрозы безопасности информации, связанные с использованием для выполнения компьютерных атак уязвимостей веб-приложений [4]. Для эффективного построения системы защиты информации подобных информационных систем, наряду с защитой от несанкционированного доступа к информации, необходима реализация защиты на уровне используемого программного обеспечения – информационные системы должны быть защищены от угроз, связанных с наличием уязвимостей в программном обеспечении информационных систем, в том числе веб-приложениях. Контроль защищенности веб-приложений, как правило, выполняется в рамках сертификации по требованиям безопасности информации, которая предусматривает тестирование на проникновение. Следует отметить, что в настоящее время еще не разработано типовой методики проведения тестирования на проникновения веб-приложений, выполняемого в ходе проведения сертификационных испытаний, которая позволила бы обеспечить повторяемость и воспроизводимость результатов испытания и учесть особенности отечественной системы сертификации [5]. При проведении анализа уязвимостей в рамках сертификационных испытаний экспертами испытательных лабораторий в настоящее время активно используются методические рекомендаций приведенные в ГОСТ Р ИСО/МЭК 18045 – документа, содержащего общую методологию оценки, используемую при проведении сертификационных испытаний по линии «Общих критериев» [6-10]. Предлагаемая данным документом методика предполагает выполнение идентификации множества потенциальных уязвимостей объекта сертификации и проведение тестирования на проникновение с целью проверки выдвинутых гипотез относительно наличия потенциальных уязвимостей. Разработанный международный стандарт ISO/IEC TR 20004 уточняет и детализирует действия эксперта испытательной лаборатории, выполняемые при анализе уязвимостей, описанные в документе ГОСТ Р ИСО/МЭК 18045-2013. В частности, этот документ направлен на детализацию и пояснение действий оценщика «Идентификация потенциальной уязвимости в общедоступных источниках» и

1 Барабанов Александр Владимирович, кандидат технических наук, директор департамента ЗАО «НПО «Эшелон», Москва, ab@cnpo.ru

2 Федичев Андрей Валерьевич, кандидат технических наук, доцент, директор НЦПИ Минюста России, Москва, andrey.fedichev@scli.ru

«Тестирование проникновения», изложение которых не обладают необходимой полнотой в части поиска, идентификации и тестирования потенциальных уязвимостей. В то же время указанные документы не содержат детальных рекомендаций и указаний по проведению анализа уязвимостей в отношении программного обеспечения, реализующего веб-технологии. Таким образом, задача разработки и совершенствования методического обеспечения анализа уязвимостей веб-приложений при проведении сертификационных испытаний по требованиям безопасности информации в настоящее время является актуальной.

Цель проведенного исследования состояла в сокращении времени анализа уязвимостей при проведении сертификационных испытаний веб-приложений по требованиям безопасности информации за счет использования типовой методики анализа уязвимостей в веб-приложениях.

Результаты разработки типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний

Типовая методика анализа уязвимостей представляет собой набор сценариев типовых атак на веб-приложения, которые должны быть выполнены экспертом испытательной лаборатории при проведении сертификационных испытаний. Для формирования множества типовых сценариев атак на веб-приложения была использована методика, предлагаемая стандартом ISO/IEC TR 20004, модифицированная с учетом особенностей отечественной системы сертификации средств защиты информации.

На первом этапе был сформулирован перечень потенциальных уязвимостей веб-приложений. При выполнении идентификации потенциальных уязвимостей веб-приложений было выполнено исследование следующих источников информации:

- документация на различные веб-приложения, представленная для проведения сертификационных испытаний в испытательную лабораторию [11];
- модель веб-приложения, построенная с использованием диаграммы информационных потоков [11, 12];
- банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) [13];
- база данных уязвимостей программного обеспечения «Common Vulnerabilities and Exposures (CVE)» (mitre.org) [14];
- база данных недостатков (слабостей) программного обеспечения «Common Weakness Enumeration» (cwe.mitre.org);
- база данных шаблонов компьютерных атак «Common Attack Pattern Enumeration and Classification» (capec.mitre.org);
- исследовательские статьи, в которых сообщается об уязвимостях в веб-технологиях и атаках на эти технологии (owasp.org).

В результате идентификации потенциальных уязвимостей веб-приложений был сформирован перечень, представленный в таблице 1.

На втором этапе в рамках исследования для каждой потенциальной уязвимости были разработаны следующие типовые сценарии атаки: AS-1 «Межсайтовое выполнение скриптов, AS-2 «Внедрение SQL-кода», AS-3 «Межсайтовая подделка запросов», AS-4 «Обход средств контроля доступа», AS-5 «Обход средств аутентификации (использование данных учетных записей, созданных по умолчанию)». Каждый сценарий атаки включает в себя порядок выполнения теста и ожидаемые результаты. Далее в качестве иллюстрации приведен типовой сценарий атаки AS-1 «Межсайтовое выполнение скриптов».

Порядок выполнения теста

1. Авторизация на автоматизированном рабочем месте с использованием данных учетной записи администратора операционной системы.
2. Запуск браузера, выполнение доступа к веб-приложению путем ввода в адресной строке браузера соответствующего адреса.
3. Авторизация в веб-приложении с использованием данных учетной записи администратора веб-приложения.
4. Поиск и идентификация частей веб-приложения (веб-страниц), которые обеспечивают получение, обработку и последующее использование данных, полученных от пользователя (администратора) веб-приложения, для генерации веб-страниц (эти части веб-приложения могут быть использованы для проведения атаки типа «Межсайтовое выполнение скриптов»).
5. Для каждой идентифицированной части веб-приложения (веб-страницы), которая потенциально может использоваться для проведения атаки типа «Межсайтовое выполнение скриптов», осуществление атак типа «Межсайтовое выполнение скриптов» путем отправки запросов веб-приложению, содержащих наборы данных (например, «<SCRIPT>alert(‹XSS›);</SCRIPT>» или «‹›;!--»<XSS>=&{()}»), реализующих попытки выполнения сценариев в браузере (данное действие выполняется с использованием специализированных инструментальных средств, например, средства анализа защищенности «Сканер-ВС»).

Таблица 1

Результаты формирования перечня потенциальных уязвимостей веб-приложений

Идентификатор потенциальной уязвимости	Краткое описание	Ссылка на международные базы данных
VUL_P1	Потенциальная уязвимость связана с отсутствием корректной обработки программным кодом веб-приложения данных, используемых для генерации веб-страниц, возвращаемых пользователю. Для генерации страниц могут использоваться данные, полученные из недоверенного источника (от нарушителя). Возможным последствием от использования уязвимости нарушителем является выполнение произвольного кода на компьютере (веб-браузере) пользователя («межсайтовое выполнение скриптов»). Уязвимость может быть использована нарушителем с компетенциями в области разработки веб-приложений. Для использования уязвимости специального оборудования не требуется.	CWE-79 OWASP A3 CAPEC-8
VUL_P2	Потенциальная уязвимость связана с отсутствием корректной обработки программным кодом веб-приложения данных, поступающих из недоверенных источников (от нарушителя) и используемых для генерации запросов, написанных на языке SQL, к базам данных. Возможным последствием от использования уязвимости нарушителем является выполнение произвольного запроса к базе данных (внедрение SQL-кода). Уязвимость может быть использована нарушителем с компетенциями в области разработки веб-приложений. Для использования уязвимости специального оборудования не требуется.	CWE-89 OWASP A1 CAPEC-6
VUL_P3	Потенциальная уязвимость связана с отсутствием корректного подтверждения того, что HTTP-запрос, полученный от аутентифицированного пользователя, действительно был сформирован и отправлен этим пользователем. Нарушитель имеет возможность заставить веб-браузер, используемый аутентифицированным пользователем, отправить (незаметно для пользователя) запрос веб-приложению. Запрос будет обработан веб-приложением как легальный запрос, полученный от аутентифицированного пользователя. Возможным последствием от использования уязвимости нарушителем является выполнение произвольного кода на стороне веб-приложения от имени аутентифицирвоанного пользователя. Уязвимость может быть использована нарушителем с компетенциями в области разработки веб-приложений. Для использования уязвимости специального оборудования не требуется.	CWE-352 OWASP A8 CAPEC-62
VUL_P4	Потенциальная уязвимость связана с недостатком в реализации механизма контроля доступа к ресурсам, защищаемым веб-приложением. Нарушитель имеет возможность сгенерировать специальный HTTP-запрос для получения несанкционированного доступа к защищаемым ресурсам в обход средств разграничения доступом, реализованных в веб-приложении. Возможным последствием от использования уязвимости нарушителем является несанкционированный доступ к защищаемым ресурсам веб-приложения. Уязвимость может быть использована нарушителем с компетенциями в области разработки веб-приложений. Для использования уязвимости специального оборудования не требуется.	CWE-285 OWASP A7 CAPEC-1
VUL_P5	Потенциальная уязвимость связана с возможностью использования данных учетных записей (идентификаторы учётных записей, пароли), созданных по умолчанию. Поскольку данные учетных записей, создаваемых по умолчанию, как правило, известны (документация разработчика, публикации в общедоступных источниках информации), то нарушитель может использовать эту информацию для получения несанкционированного доступа к ресурсам, защищаемым веб-приложением. Возможным последствием от использования уязвимости нарушителем является несанкционированный доступ к защищаемым ресурсам веб-приложения. Уязвимость может быть использована нарушителем с компетенциями в области разработки веб-приложений. Для использования уязвимости специального оборудования не требуется.	CWE-798 OWASP A5 CAPEC-70

6. Выполнение перехвата данных, которые высылает веб-приложение в ответ на сформированные запросы.

7. Анализ сформированных запросов, посылаемых веб-приложению, и ответов веб-приложения, полученных на данные запросы, а также данных отображаемых браузером с целью выявления ошибок, связанных с отсутствием обработки данных, получаемых от пользователя, или недостаточной обработки таких данных, которые могут быть использованы для выполнения сценариев браузером. Идентификация веб-страниц, содержащих указанные ошибки, переход к данным страницам и выполнение попытки запуска сценариев (например, <SCRIPT>alert(‹XSS›);</SCRIPT>).

Ожидаемые результаты

Если потенциальная уязвимость VUL_P1 актуальна для веб-приложения, то в ходе проведения теста AS-1 будут идентифицированы ошибки, связанные с обработкой веб-приложением данных от пользователя, и идентифицированные ошибки позволят выполнить запуск сценария в браузере. Если потенциальная уязвимость VUL_P1 не является актуальной для веб-приложения, то в ходе проведения теста AS-1 ошибки, связанные с обработкой веб-приложением данных от пользователя, обнаружены не будут (попытки запуска сценариев завершаться неуспешно).

В ходе выполнения исследования была выполнена оценка следующих характеристик разработанных типовых сценариев атак (таблица 2): время, затрачиваемое на идентификацию уязвимости и её использование (время), требуемая техническая компетентность специалиста (компетентность), знание проекта веб-приложения и особенностей его функционирования (знание), возможность доступа к веб-приложению, инструментальные средства, требуемое для эксплуатации уязвимости (оборудование), оценка потенциала нападения, требуемого для выполнения сценария атаки. Оценка потенциала нападения выполнена с учетом методических рекомендаций, представленных в приложении В ГОСТ Р ИСО/МЭК 18045.

Результаты анализа уязвимостей, проведенного с использованием разработанной типовой методики, должны подтверждать стойкость веб-приложения к действиям нарушителя с потенциалом нападения «Базовый». Если результаты показывают, что веб-приложение, находящиеся в заданных средах функционирования, имеет уязвимости, пригодные для использования нарушителем с потенциалом меньшим или равным заданному потенциалу, делается отрицательное заключение по результатам анализа уязвимостей. В случае обнаружения пригодных для использования уязвимостей сертификационные испытания могут быть продолжены только после устранения их разработчиком веб-приложения.

Результаты экспериментальных исследований

В ходе проведения исследования была проведена оценка эффективности разработанной методики анализа уязвимостей. Для оценки эффективности были выполнены экспериментальные исследования веб-приложений, испытываемых в аккредитованной испытательной лаборатории НПО «Эшелон», с использованием следующих методик:

- методика №1 – методика анализа уязвимостей на основе Общей методологии оценки и стандарта ISO/IEC TR 20004 [11];

Таблица 2

Оценка характеристик разработанных типовых сценариев атак

Идентификатор сценария/типовой уязвимости	Краткое описание сценария атаки					Оценка потенциала нападения
	время	компетентность	знание	возможность доступа	оборудование	
AS-1/VUL_P1	<1 дня (0)	профессионал (3)	общедоступная информация (0)	простой доступ (1)	стандартное (0)	Базовый (4)
AS-2/VUL_P2	<1 дня (0)	профессионал (3)	общедоступная информация (0)	простой доступ (1)	стандартное (0)	Базовый (4)
AS-3/VUL_P3	<1 дня (0)	профессионал (3)	общедоступная информация (0)	простой доступ (1)	стандартное (0)	Базовый (4)
AS-4/VUL_P4	<1 дня (0)	профессионал (3)	общедоступная информация (0)	простой доступ (1)	стандартное (0)	Базовый (4)
AS-5/VUL_P5	<1 дня (0)	профессионал (3)	общедоступная информация (0)	простой доступ (1)	стандартное (0)	Базовый (4)

Таблица 3

Результаты оценки эффективности

	ПО №1		ПО №2		ПО №3	
	T, ч	E, %	T, ч	E, %	T, ч	E, %
Методика №1	10,6	2/4=50%	9,1	0/4=0	16,2	0/2=0
Методика №2	13,1	1/5=20%	12,9	1/4=25%	20,7	0/2=0
Методика №3	12,4	2/5=40%	8,7	3/5=60%	14,2	1/5=20%

- методика №2 – методика анализа уязвимостей, основанная на применении статистического анализа исходных текстов ПО [15, 16];

- методика №3 – разработанная методика анализа уязвимостей.

В ходе проведения исследования для каждой методики оценивались следующие показатели эффективности: *T* - время выполнения анализа уязвимостей, *E* - отношение числа подтвержденных уязвимостей веб-приложения к числу потенциальных уязвимостей веб-приложения. Результаты оценки эффективности представлены в таблице 3.

Выводы и рекомендации

Разработана методика анализа уязвимостей веб-приложений, которая может использоваться при проведении сертификационных испытаний по требованиям безопасности информации. При разработке методики на основе формирования перечня потенциальных уязвимостей веб-приложений выполнен синтез перечня сценариев типовых атак на веб-приложения с учетом особенностей отечественной системы сертификации средств защиты информации. Оценка эффективности разработанной методики, проведенная в ходе настоящего исследования, показала сокращение времени анализа уязвимостей по сравнению с известными способами в среднем на 4% [11]. Применение комбинированной методики позволило выявить 7 реальных уязвимостей веб-приложений, испытываемых в аккредитованной испытательной лаборатории НПО «Эшелон» [4].

Разработанная методика внедрена и успешно используется в работе аккредитованной испытательной лаборатории НПО «Эшелон» и может быть рекомендована к внедрению в работу испытательных лабораторий различных систем сертификации средств защиты информации при проведении испытаний веб-приложений для подтверждения стойкости веб-приложения к действиям нарушителя с потенциалом нападения «Базовый».

Кроме того, методические решения могут быть полезны в рамках построения системы производства безопасного программного обеспечения [18,19].

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э. Баумана, Москва, v.tsirlov@bmstu.ru*

Литература:

1. Баранов А.П. Актуальные проблемы в сфере обеспечения информационной безопасности программного обеспечения // Вопросы кибербезопасности. 2015. № 1 (9). С. 2-5.
2. Калашников А.О., Ермилов Е.В., Чопоров О.Н., Разинкин К.А., Баранников Н.И. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков. Под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга». 2013. – 160 с.
3. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1 (46). С. 27-34.
4. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.
5. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации // Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.
6. Barabanov A., Markov A. Modern Trends in The Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI: 10.1145/2799979.2799980.
7. Higaki W.H. Successful Common Criteria Evaluations: A Practical Guide for Vendors. CreateSpace Independent Publishing Platform. 2010. 282 p.
8. Merkow M.S., Breithaupt J. Computer Security Assurance Using the Common Criteria. Thomson Delmar Learning, 2005. 278 p.
9. Prieto-Diaz R. The Common Criteria Evaluation Process. Technical Report CISC-TR-2002-003, CISC, 2002, 56 p.

10. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264-270.
11. Барабанов А.В., Евсеев А.Н. Вопросы повышения эффективности анализа уязвимостей при проведении сертификационных испытаний программного обеспечения по требованиям безопасности информации // Труды международного симпозиума Надежность и качество. 2015. Т. 1. С. 330-333.
12. Gary McGraw. 2015. Software security and the building security in maturity model (BSIMM). J. Comput. Sci. Coll. 30, 3 (January 2015), pp.7-8.
13. Гончаров И.В., Гончаров Н.И., Кирсанов Ю.Г., Паринов П.А., Райков О.В. Порядок проведения анализа состояния информационной системы персональных данных различного применения в рамках выполнения требований по защите информации // ИТ-Стандарт. 2015. Т. 1. № 4-1 (5). С. 37-41.
14. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3 (51). С. 56-61.
15. Зубарев И.В., Жидков И.В., Кадушкин И.В. Применение системной инженерии к формированию нормативно-методической базы испытаний программных средств по требованиям безопасности информации. В сборнике: Информационные и математические технологии в науке и управлении Ответственный редактор Л.В. Массель. 2015. С. 181-186.
16. Марков А.С., Матвеев В.А., Фадин А.А., Цирлов В.Л. Эвристический анализ безопасности программного кода // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2016. № 1 (106). С. 98-111. DOI: 10.18698/0236-3933-2016-1-98-111.
17. Kara M. Review on Common Criteria as a Secure Software Development Model. IJCSIT, 2012, V. 4, No 2 (Apr. 2012), pp. 83-94. DOI: 10.5121/ijcsit.2012.4207.
18. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1 (1). С. 37-41.
19. Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 93-97. DOI: 10.1145/2799979.2799998.

ON DEVELOPMENT OF WEB APPLICATION VULNERABILITY ANALYSIS TECHNIQUE DURING SOFTWARE SECURITY EVALUATION

Barabanov A.V.[3], Fedichev A.V. [4]

A research of the existing approaches to the vulnerability analysis during web application security evaluation was conducted. The new vulnerability analysis technique based on ISO / IEC TR 20004 and features or Russian IT security certification scheme was developed. The new vulnerability analysis technique is based on proposed web applications attack patterns and a set of potential web application vulnerabilities. Example of using new developed vulnerability analysis technique during vulnerability assessment of web applications was shown. Experimental studies of the proposed vulnerability analysis technique shown that vulnerability analysis time was reduced compared to known techniques by an average of 4%.

Keywords*: security software evaluation, vulnerability analysis, web application.*

References:

1. Baranov A.P. Aktual›nye problemy v sfere obespecheniya informatsionnoy bezopasnosti programmnogo obespecheniya, Voprosy kiberbezopasnosti [Cybersecurity issues], 2015, No 1 (9), pp.2-5.
2. Kalashnikov A.O., Ermilov E.V., Choporov O.N., Razinkin K.A., Barannikov N.I. Ataki na informatsionno-tekhnologicheskuyu infrastrukturu kriticheski vazhnykh ob'ektov: otsenka i regulirovanie riskov. Pod red. chl.-korr. RAN D.A. Novikova. – Voronezh: Izdatel'stvo «Nauchnaya kniga», 2013. – 160 s.
3. Sheremet I.A. Ugrozy tekhnosfere Rossii i protivodeystvie im v sovremennykh usloviyakh, Vestnik akademii voennykh nauk, 2014, No 1 (46), pp.27-34.
4. Markov A.S., Tsirlov V.L. Opyt vyyavleniya uyazvimostey v zarubezhnykh programmnykh produktakh, Voprosy kiberbezopasnosti [Cybersecurity issues], 2013, No 1 (1), pp.42-48.
5. Markov A.S., Sheremet I.A. Teoreticheskie aspekty sertifikatsii sredstv zashchity informatsii [Theoretical Aspects of Information Security Certification], Oboronnyy kompleks - nauchno-tekhnicheskomu progressu Rossii [Defense Industry Achievements - Russian Scientific and Technical Progress], 2015, No 4 (128), pp.7-15.

3 Alexander Barabanov, Ph.D, CIO for NPO Echelon, Moscow, ab@cnpo.ru
4 Andrei Fedichev, Ph.D., director at SCLI Russian Ministry of Justice, Moscow, andrey.fedichev@scli.ru

6. Barabanov A., Markov A. Modern Trends in The Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI: 10.1145/2799979.2799980.
7. Higaki W.H. Successful Common Criteria Evaluations: A Practical Guide for Vendors. CreateSpace Independent Publishing Platform, 2010. 282 p.
8. Merkow M.S., Breithaupt J. Computer Security Assurance Using the Common Criteria. Thomson Delmar Learning, 2005. 278 p.
9. Prieto-Diaz R. The Common Criteria Evaluation Process. Technical Report CISC-TR-2002-003, CISC, 2002, 56 p.
10. Barabanov A.V., Markov A.S., Tsirlov V.L. Otsenka sootvetstviya sredstv zashchity informatsii «Obshchim kriteriyam» [The Conformity Assessment of Information Security Solutions According to the Common Criteria], Informatsionnye tekhnologii [Information Technologies], 2015. V. 21, No 4, pp.264-270.
11. Barabanov A.V., Evseev A.N. Voprosy povysheniya effektivnosti analiza uyazvimostey pri provedenii sertifikatsionnykh ispytaniy programmnogo obespecheniya po trebovaniyam bezopasnosti informatsii, Trudy mezhdunarodnogo simpoziuma Nadezhnost' i kachestvo, 2015. T. 1, pp.330-333.
12. Gary McGraw, 2015. Software security and the building security in maturity model (BSIMM). J. Comput. Sci. Coll. 30, 3 (January 2015), pp.7-8.
13. Goncharov I.V., Goncharov N.I., Kirsanov Yu.G., Parinov P.A., Raykov O.V. Poryadok provedeniya analiza sostoyaniya informatsionnoy sistemy personal'nykh dannykh razlichnogo primeneniya v ramkakh vypolneniya trebovaniy po zashchite informatsii, IT-Standart, 2015. T. 1, No 4-1 (5), pp.37-41.
14. Markov A.S., Fadin A.A. Sistematika uyazvimostey i defektov bezopasnosti programmnykh resursov, Zashchita informatsii. Insayd, 2013, No 3 (51), pp.56-61.
15. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Primenenie sistemnoy inzhenerii k formirovaniyu normativno-metodicheskoy bazy ispytaniy programmnykh sredstv po trebovaniyam bezopasnosti informatsii. V sbornike: Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii Otvetstvennyy redaktor L.V. Massel', 2015, pp.181-186.
16. Markov A.S., Matveev V.A., Fadin A.A., Tsirlov V.L. Evristicheskiy analiz bezopasnosti programmnogo koda, Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya: Priborostroenie, 2016, No 1 (106), pp. 98-111. DOI: 10.18698/0236-3933-2016-1-98-111.
17. Kara M. Review on Common Criteria as a Secure Software Development Model. IJCSIT, 2012, V. 4, No 2 (Apr, 2012), pp. 83-94. DOI: 10.5121/ijcsit.2012.4207.
18. Barabanov A.V. Standartizatsiya protsessa razrabotki bezopasnykh programmnykh sredstv, Voprosy kiberbezopasnosti [Cybersecurity issues], 2013, No 1 (1), pp. 37-41.
19. Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 93-97. DOI: 10.1145/2799979.2799998.