УДК 004.738.1:004.056.5 **doi: 10.32620/reks.2018.3.08**

А. Г. ТЕЦКИЙ

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

ПРИМЕНЕНИЕ ДЕРЕВЬЕВ АТАК ДЛЯ ОЦЕНИВАНИЯ ВЕРОЯТНОСТИ УСПЕШНОЙ АТАКИ WEB-ПРИЛОЖЕНИЯ

Развитие технологий приводит к расширению спектра оказываемых услуг в сети Интернет, активно развивается онлайн-бизнес. Как правило, при создании нового Web-ресурса для бизнеса основной акцент ставится на необходимости выделиться среди сайтов конкурентов. Зачастую владельцы Web-ресурсов узнают о возможных последствиях киберинцидента только после того, когда на их ресурс была совершена атака. В данной статье рассмотрены частые причины атак Web-приложений, созданных с помощью систем управления контентом. Системы управления контентом позволяют создавать сайты без непосредственного написания кода. Основными источниками информации о частых проблемах безопасности Web-ресурсов являются документы организаций OWASP, SANS, Positive Technologies. В связи с высокой активностью злоумышленников необходимо создание методов оценивания безопасности Web-приложения и методов противодействия атакам. В работе обусловлена необходимость оценивания вероятности успешной атаки Web-приложения. На практике невозможно определить все возможные сценарии атак, поскольку каждое Web-приложение обладает собственной функциональностью. Исследованы частые сценарии атак, на основании которых построено дерево. Использован метод оценивания вероятностей базовых событий с помощью экспертных оценок, базирующихся на результатах предварительного проведения комплекса мероприятий по выявлению проблем безопасности. Разработанный метод оценивания безопасности позволяет учитывать не только возможные уязвимости в исходном коде, но и возможные нарушения политики безопасности. Предлагаемый метод может применяться субъектами предпринимательской деятельности, работающими в сфере информационной безопасности, при выборе мер защиты для конкретного Web-приложения. Дальнейшим направлением исследований является создание метода выбора контрмер на основе описанного метода. Метод выбора должен наглядно демонстрировать влияние каждой контрмеры на вероятность успешной атаки.

Ключевые слова: *дерево атак, Web-приложение, система управления контентом, несанкционированный доступ, кибербезопасность.*

Введение

Востребованность современными организациями в представлении информации с целью увеличения объема продаж или предоставления услуг подразумевает под собой создание информационных ресурсов в сети Интернет. Часто для создания сайтов используются системы управления контентом [1].

Система управления контентом – это программное обеспечение, которое позволяет редактировать Web-страницы и создавать сайты на их основе. Примерами таких систем являются Wordpress, Joomla и другие. Подобные системы нашли применение и в образовании, например, MOODLE – система управления образовательным контентом. Такие системы получили широкую известность из-за простоты использования, количество инсталляций может измеряться миллионами экземпляров. Особенностью таких систем является модульная архитектура, благодаря этому возможно управлять функциональностью сайта, устанавливая нужные модули. Критическая уязвимость в модуле может ставить под угрозу все сайты, использующие данный модуль, поэтому злоумышленники могут взломать многие из этих сайтов по одинаковому сценарию [2]. Среди особенностей использования систем управления контентом в аспекте информационной безопасности следует выделить следующие:

– высокая распространенность и большое сообщество пользователей, которое может обнаружить уязвимости раньше злоумышленников и передать информацию разработчикам системы для выпуска патча;

– не все администраторы сайтов устанавливают обновления;

– любой разработчик может создать свой модуль и сделать его доступным для инсталляции всему сообществу. При этом неизвестно, какие уязвимости этот модуль может содержать;

–использование систем управления контентом в электронном бизнесе также привлекает злоумышленников. Взломав Интернет-магазин, злоумышленник получает доступ к информации, которую он может продать конкурирующему интернет-магазину. Взломав онлайн-обменник электронных денег, злоумышленник может получить доступ к счетам различных платежных систем и перевести деньги на произвольные счета.

Таким образом, системы управления контентом предоставляют широкое поле для деятельности в области информационной безопасности [3]. Владельцам сайтов, которые задумываются о безопасности, хочется знать, насколько легко их сайт может быть взломан. Поэтому актуальной является задача оценивания вероятности успешной атаки Web-приложения. Например, в работе [4] был приведен пример дерева атак для получения доступа к электронной почте жертвы, что является одним из сценариев взлома Web-приложения. Использование дерева позволяет определить вероятность возникновения основного события. В работе [5] был продемонстрирован метод оценивания безопасности ad hoc сети для автомобилей с помощью деревьев атак. В работе [6] рассматривались проблемы безопасности, характерные для Web-приложений, возможные причины атак и их последствия. Поскольку информация предоставлялась в текстовом виде, а не в графическом, то наглядность такой информации была ниже. Предлагаемый подход заключается в применении известного метода анализа к реальным сценариям атак Web-приложений.

Понимание сценариев атак позволяет применять необходимые методы защиты Web-приложения. Результаты аудита дают представление о том, насколько администратор заботится о безопасности своего аккаунта. Анализ исходного кода, в отличие от тестирования на проникновение методом черного ящика, позволять обнаружить на порядок больше возможных уязвимостей. На практике далеко не всегда есть возможность проанализировать код всего проекта из-за большого количества строк кода, поэтому в таких случаях целесообразно выбирать наиболее значимые компоненты для анализа, такие как классы для работы с базой данный, классы регистрации и авторизации пользователей и т.п. Исходя из вышесказанного, возникает задача определения вероятности успешной атаки P на основе исследования возможных сценариев атак, результатов аудита и анализа исходного кода.

Целью работы является исследование сценариев атак на Web-приложение и создание метода определения вероятности успешной атаки.

1. Построение дерева атак

Для исследования сценариев атак Web-приложений предлагается использовать анализ деревьев атак. Метод анализа деревьев (отказов, атак) применяется в таких сферах как авиация, атомная промышленность, военная отрасль и т.д. В области информационных технологий деревья атак могут применяться для наглядного представления возможных путей атак на различные компоненты компьютерной системы.

Частые сценарии атак визуализированы в виде дерева, показанного на рисунке 1. Построенное дерево не учитывает возможность использования двухфакторной аутентификации для доступа к панели управления. Также допускается, что отсутствует защита от перебора логинов и паролей.

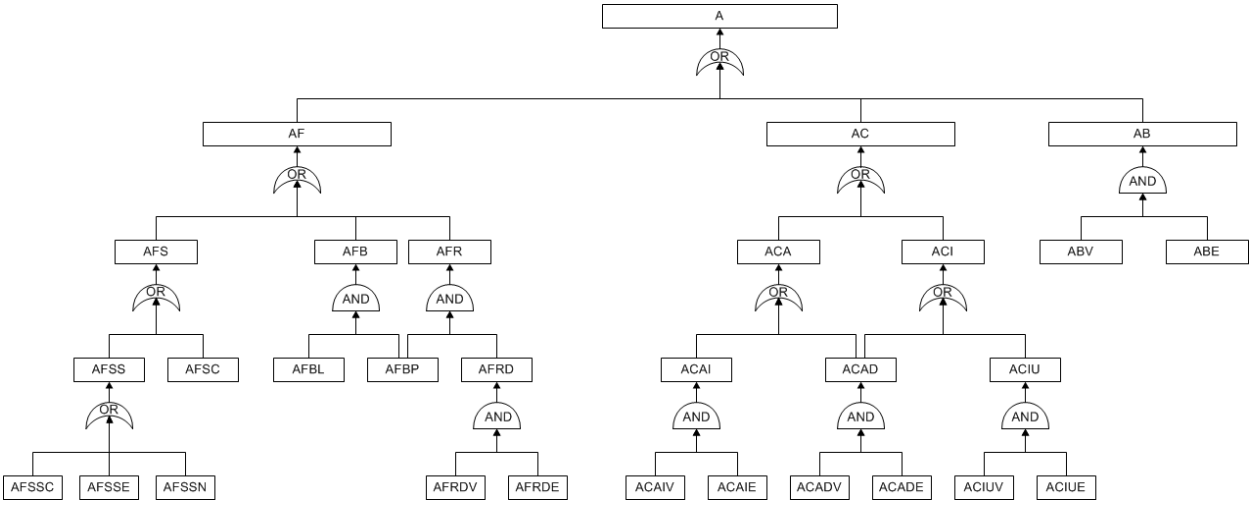

Рис. 1. Дерево атак

При построении дерева необходимо определить основное событие и исследовать возможные сценарии атак.

Названия событий, показанных на рисунке 1, и соответствующие аббревиатуры показаны в таблице 1.

Таблица 1

Названия событий

Сокращение	Полное название события
A	Получить доступ к функциям панели управления
AF	Узнать логин и пароль текущего администратора
AC	Создать новую учетную запись администратора
AB	Обойти авторизацию
AFS	Украсть логин и пароль
AFB	Узнать логин и пароль методом перебора
AFR	Подобрать пароль с помощью известного хэша
ACA	Добавить новую учетную запись с привилегиями непосредственно в базу данных
ACI	Увеличить стандартные пользовательские привилегии
ABV	Найдены уязвимости для обхода авторизации
ABE	Эксплуатируются уязвимости для обхода авторизации
AFSS	Учетные данные украдены из хранилища
AFSC	Учетные данные украдены во время передачи по незашифрованному каналу
AFBL	У злоумышленника есть словарь, который включает искомый логин
AFBP	У злоумышленника есть словарь, который включает искомый пароль
AFRD	Получить имя пользователя и пароль из базы данных
ACAI	Использование соответствующих уязвимостей (например, SQL-инъекция при вставке)
ACAD	Известны учетные данные для подключения к базе данных
ACIU	Использование соответствующих уязвимостей (например, SQL-инъекция при обновлении)
AFSSC	Учетные данные украдены с ПК
AFSSE	Учетные данные украдены из электронной почты или любого облачного хранилища
AFSSN	Учетные данные украдены из нецифрового хранилища
AFRDV	Обнаружены соответствующие уязвимости, позволяющие получить имя пользователя и пароль из базы данных
AFRDE	Эксплуатация уязвимостей, позволяющих получить имя пользователя и пароль из базы данных
ACAIV	Обнаружены соответствующие уязвимости (например, SQL-инъекция при вставке)
ACAIE	Эксплуатация уязвимостей (например, SQL-инъекция при вставке)
ACADV	Обнаружены соответствующие уязвимости для подключения к базе данных
ACADE	Эксплуатация уязвимостей для подключения к базе данных
ACIUV	Обнаружены соответствующие уязвимости (например, SQL-инъекция при обновлении)
ACIUE	Эксплуатация уязвимостей (например, SQL-инъекция при обновлении)

Основное событие – успешная атака Web-приложения. Под успешной атакой подразумевается получение несанкционированного доступа к функциям, доступным только администратору из панели управления. Варианты атак разбиты по группам и представлены ниже:

– атаки с похищением пароля администратора (AF);

– атаки с созданием нового администратора (AC);

– атаки на уязвимости в системе управления контентом (AB).

Использование элементов AND/OR является достаточным, поскольку при исследовании сценариев атак не возникало необходимости использовать другие элементы, например, XOR.

Следующим этапом является определение вероятностей базовых событий (листьев дерева). Для этого предлагается использование экспертных оценок по пятибалльной шкале. Вероятность базового события определяется по формуле

$$P = w_1 u(S) + w_2 u(C) + w_3 u(L), \quad (1)$$

где w_1, w_2, w_3 – весовые коэффициенты ($\sum_{i=1}^{3} w_i = 1$),

S – сложность атаки (1 – атаку легко реализовать, 5 – атака сложна в реализации),

C – стоимость атаки (1 – атака низкой стоимости, 5 – атака высокой стоимости),

L – сложность обнаружения атаки (1 – атаку сложно обнаружить, 5 – атаку легко обнаружить),

$u(x)$ – функция преобразования.

Функция преобразования определена следующим образом:

$$u(x) = \frac{c}{x}, \quad (2)$$

где c – коэффициент преобразования.

Коэффициент преобразования вычисляется экспериментальным путем. Значение, используемое в данной работе, вычислялось из допущения, что при минимальных оценках всех базовых событий (худший случай) вероятность основного события должна попадать под определение высокой вероятности успешной атаки. Функции принадлежности для элементов терм-множества T = {"низкий", "средний", "высокий"} были приведены в работе [7]. В данной работе используются значения $c = 0{,}3$; $w_1 = w_2 = w_3 = 1/3$.

2. Расчет вероятности основного события

Для расчетов вероятности событий, объединенных элементами AND/OR, используются формулы теории вероятности для совместных событий.

При проведении расчетов использовался табличный процессор MS Excel, в котором была определена пользовательская функция расчета вероятности основного события.

В таблице 2 показан пример оценок для базовых событий. Для каждого события или групп событий созданы рекомендации по назначению оценок. Оценки определяются после проведения комплекса мероприятий, который включает в себя следующее:

−Web-аудит, который позволяет проверить, внедрены ли политики безопасности, придерживается ли администратор сайта положений политики безопасности;

−тестирование на проникновение, которое позволяет выявить проблемы безопасности в архитектуре Web-приложения, конфигурации сервера или в исходном коде приложения. Проведение анализа исходного кода является не обязательным мероприятием, поскольку этот процесс может требовать значительных временных и финансовых затрат.

Таблица 2

Значения оценок базовых событий

Имя события	Сложность атаки	Стоимость атаки	Сложность обнаружения
ABV	4	2	4
ABE	4	3	3
AFSC	4	2	1
AFBL	4	3	1
AFBP	5	3	1
AFSSC	5	5	1
AFSSE	5	5	1
AFSSN	5	5	1
AFRDV	4	2	4
AFRDE	4	3	3
ACAIV	4	2	4
ACAIE	4	3	3
ACADV	4	2	4
ACADE	4	3	3
ACIUV	4	2	4
ACIUE	4	3	3

В соответствии с оценками, приведенными в таблице 2, и формулами (1), (2) был проведён расчёт вероятности успешной атаки, получено значение $P = 0{,}5117$. Возможно, такое значение покажется слишком высоким. Статистика, приведенная компанией Positive Technologies, говорит о том, что 94% исследованных сайтов имеют критические уязвимости [8]. Стоит заметить, что исследовались системы управления контентом, которые являются нетиповыми, то есть содержали большое количество уникального кода. У типовых систем этот показатель должен быть меньше по причине наличия мирового сообщества, которое постоянно занимается улучшением разработок и исправлением проблем безопасности. Такому высокому значению не стоит удивляться ввиду нескольких причин. Основная из них это то, что проблеме безопасности не уделяется должное внимание.

Описанный метод позволяет оценить, насколько легко может быть получен несанкционированный доступ к функциям администратора определенного Web-приложения. Комплекс мероприятий, направленных на анализ исходного кода и соблюдение политик безопасности, позволяет определить вероятности базовых событий построенного дерева.

Отличием от существующих методов оценки безопасности Web-приложения, примеры которых приведены в [9-10], является следующее:

−привязка к реальным сценариям атак. Это дает максимальную приближенность к действиям злоумышленника при атаке Web-приложения;

−использование результатов аудита. Это позволяет рассматривать сценарии атак, которые не связаны с уязвимостями целевой системы;

−отсутствие привязанности к обнаруженным уязвимостям. При оценке вероятности успешной атаки не учитываются известные уязвимости (из таких баз, как NVD [11]), но эксперты могут принимать во внимание количество и критичность уязвимостей при оценке вероятностей базовых событий.

Недостатком описанного подхода являются затраты на проведение аудита и анализ исходного кода.

Заключение

Цель проводимых исследований, заключающаяся в исследовании сценариев атак на Web-приложение и определении вероятности успешной атаки, была достигнута с помощью построения и анализа дерева атак. Исследования проводились из допущения, что невозможно предугадать все сценарии атак, которые могут быть использованы злоумышленниками, поэтому в дереве могли быть собраны только наиболее частые сценарии атак [12].

Предлагаемый метод может применяться при выборе мер защиты для конкретного Web-приложения.

Направление дальнейших исследований заключаются в исследовании способов уменьшения вероятности успешной атаки (использование различных мер защиты) и создании метода выбора контрмер.

Литература

1. Influence of web content management systems in web content accessibility [Text] / J. M. López, A. Pascual, L. Masip, T. Granollers, X. Cardet // IFIP Conference on Human-Computer Interaction. – Springer, Berlin, Heidelberg, 2011. – P. 548-551.

2. Slider Revolution Plugin Critical Vulnerability Being Exploited [Electronic resource] – Access mode: https://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html. – 7.09.2018.

3. Rehman, H. Security of Web Application: State of the Art [Text] / H. Rehman, M. Nazir, K. Mustafa // Information, Communication and Computing Technology. ICICCT 2017. Communications in Computer and Information Science. – Springer, Singapore, 2017. – Vol. 750. – P. 168-180.

4. Nagaraju, V. A survey of fault and attack tree modeling and analysis for cyber risk management [Text] / V. Nagaraju, L. Fiondella, T. Wandji // Technologies for Homeland Security (HST), 2017 IEEE International Symposium. – IEEE, 2017. – P. 1-6.

5. Du, S. Security assessment via attack tree model [Text] / S. Du, H. Zhu // Security Assessment in Vehicular Networks. – Springer, New York, 2013. – P. 9-16.

6. Lepofsky, R. The manager's guide to web application security: a concise guide to the weaker side of the web [Text] / R. Lepofsky. – Apress, 2014. – 232 p.

7. Tetskyi, A. Analysis of the Possibilities of Unauthorized Access in Content Management Systems Using Attack Trees [Text] / A. Tetskyi, V. Kharchenko, D. Uzun // Proc. PhD Symposium at ICTERI 2018, Kyiv, Ukraine, May 14-17, 2018. – CEUR-WS, 2018. – Vol. 2122. – P. 16-25.

8. Автоматизированный анализ кода: статистика уязвимостей веб-приложений за 2017 год [Электронный ресурс] / Positive Technologies. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-AI-Statistics-rus.pdf. – 7.09.2018.

9. Yu, X. A Web Security Testing Method Based on Web Application Structure [Text] / X. Yu, G. Jiang // Cloud Computing and Security. Lecture Notes in Computer Science. – Springer, Cham, 2015. – Vol. 9483. – P. 244-258.

10. Zech, P. Knowledge-based security testing of web applications by logic programming [Text] / P. Zech, M. Felderer, R. Breu // International Journal on Software Tools for Technology Transfer. – Springer, Berlin, Heidelberg, 2017. – P. 1-26.

11. National Vulnerability Database [Electronic resource] – Access mode: https://nvd.nist.gov/. – 7.09.2018.

12. Most Common Attacks Affecting Today's Websites [Electronic resource] – Access mode: https://blog.sucuri.net/2014/11/most-common-attacks-affecting-todays-websites.html. – 7.09.2018.

References

1. López, J. M., Pascual, A., Masip, L., Granollers, T., Cardet, X. Influence of web content management systems in web content accessibility. *IFIP Conference on Human-Computer Interaction*, Springer, Berlin, Heidelberg, 2011, pp. 548-551.

2. *Slider Revolution Plugin Critical Vulnerability Being Exploited*. Available at: https://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html (accessed 7.09.2018).

3. Rehman, H., Nazir, M., Mustafa, K. Security of Web Application: State of the Art. *Information, Communication and Computing Technology. ICICCT 2017. Communications in Computer and Information Science*, Springer, Singapore, 2017, vol. 750, pp. 168-180.

4. Nagaraju, V., Fiondella, L., Wandji, T. A survey of fault and attack tree modeling and analysis for cyber risk management. *Technologies for Homeland Security (HST), 2017 IEEE International Symposium*, 2017, pp. 1-6.

5. Du, S., Zhu, H. Security assessment via attack tree model. *Security Assessment in Vehicular Networks*, Springer, New York, 2013, pp. 9-16.

6. Lepofsky, R. *The manager's guide to web application security: a concise guide to the weaker side of the web*. Apress, 2014. 232 p.

7. Tetskyi, A., Kharchenko, V., Uzun, D. Analysis of the Possibilities of Unauthorized Access in Content Management Systems Using Attack Trees. *Proc. PhD Symposium at ICTERI 2018*, Kyiv, Ukraine, May 14-17, 2018, CEUR-WS, vol. 2122, pp. 16-25.

8*Avtomatizirovannyi analiz koda: statistika uyazvimostei veb-prilozhenii za 2017 god* [Automated code analysis: Web application vulnerability statistics for 2017]. *Positive Technologies*. Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-AI-Statistics-rus.pdf (accessed 7.09.2018).

9. Yu, X., Jiang, G. A Web Security Testing Method Based on Web Application Structure. *Cloud Computing and Security. Lecture Notes in Computer Science*, Springer, Cham, 2015, vol. 9483, pp. 244-258.

10. Zech, P., Felderer, M., Breu, R. Knowledge-based security testing of web applications by logic programming. *International Journal on Software Tools for Technology Transfer*, Springer, Berlin, Heidelberg, 2017, pp. 1-26.

11. *National Vulnerability Database*. Available at: https://nvd.nist.gov/ (accessed 7.09.2018).

12. *Most Common Attacks Affecting Today's Websites*. Available at: https://blog.sucuri.net/2014/11/most-common-attacks-affecting-todays-websites.html (accessed 7.09.2018).

Поступила в редакцию 7.09.2018, рассмотрена на редколлегии 12.09.2018

ЗАСТОСУВАННЯ ДЕРЕВ АТАК ДЛЯ ОЦІНЮВАННЯ ІМОВІРНОСТІ УСПІШНОЇ АТАКИ WEB-ДОДАТКА

А. Г. Тецький

Розвиток технологій призводить до розширення спектра послуг, що надаються в мережі Інтернет, активно розвивається онлайн-бізнес. Як правило, при створенні нового Web-ресурсу для бізнесу основний акцент ставиться на необхідності виділитися серед сайтів конкурентів. Часто власники Web-ресурсів дізнаються про можливі наслідки кіберінцидента тільки після того, коли на їхній ресурс була здійснена атака. У даній статті розглянуті часті причини атак Web-додатків, створених за допомогою систем управління контентом. Системи управління контентом дозволяють створювати сайти без безпосереднього написання коду. Основними джерелами інформації про часті проблеми безпеки Web-ресурсів є документи організацій OWASP, SANS, Positive Technologies. У зв'язку з високою активністю зловмисників необхідне створення методів оцінювання безпеки Web-додатків і методів протидії атакам. В роботі обумовлена необхідність оцінювання ймовірності успішної атаки Web-додатка. На практиці неможливо визначити всі можливі сценарії атак, оскільки кожний Web-додаток володіє власною функціональністю. Досліджено часті сценарії атак, на підставі яких побудовано дерево. Використаний метод оцінювання ймовірностей базових подій за допомогою експертних оцінок, що базуються на результатах попереднього проведення комплексу заходів з виявлення проблем безпеки. Розроблений метод оцінювання безпеки дозволяє враховувати не тільки можливі уразливості в сирцевому коді, але і можливі порушення політики безпеки. Пропонований метод може застосовуватися суб'єктами підприємницької діяльності, які працюють в сфері інформаційної безпеки, при виборі заходів захисту для конкретного Web-додатка. Подальшим напрямком досліджень є створення методу вибору контрзаходів на основі описаного методу. Метод повинен наочно демонструвати вплив кожного контрзаходу на ймовірність успішної атаки.

Ключові слова: дерево атак, Web-додаток, система управління контентом, несанкціонований доступ, кібербезпека.

APPLYING OF ATTACK TREES FOR ESTIMATION THE PROBABILITY OF A SUCCESSFUL ATTACK OF THE WEB-APPLICATION

A. G. Tetskyi

The development of technologies leads to the expansion of the range of services provided on the Internet, the online business is actively developing. As a rule, when creating a new Web resource for business, the main emphasis is on the need to stand out among the sites of competitors. Often, the owners of Web resources understood the possible consequences of cyber-incident only after when their resource was attacked. This paper discusses the frequent causes of attacks of Web-applications created with the content management systems. A content management system allows to create sites without directly writing code. The main sources of information about frequent security problems of Web-resources are documents of organizations OWASP, SANS, Positive Technologies. Due to the high activity of intruders, it is necessary to create methods for assessing the security of the Web-application and methods for countering attacks. In the paper, the need to assess the probability of a successful attack of Web-applications is conditioned. In practice, it is impossible to determine all possible attack scenarios, because each Web-application has its own functionality. The frequent attack scenarios on which the tree was built are investigated. The method of estimating the probabilities of basic events using expert assessments based on the results of the preliminary implementation of a set of measures to identify the security problems is used. The developed method of assessing security allows to consider not only possible vulnerabilities in the source code, but also possible security policy violations. The proposed method can be applied by business entities working in the field of information security, when choosing security measures for a particular Web-application. A further direction of research is the development of a method for choosing countermeasures based on the described method. The method should demonstrate the effect of each countermeasure on the probability of a successful attack.

Keywords: attack tree, Web-application, content management system, unauthorized access, cybersecurity.

Тецкий Артём Григорьевич – ассистент кафедры компьютерных систем, сетей и кибербезопасности Национального аэрокосмического университета им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: a.tetskiy@csn.khai.edu.

Tetskyi Artem Grygorovych – Assistant Lecturer of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkov Aviation Institute", Kharkov, Ukraine, e-mail: a.tetskiy@csn.khai.edu.