12. *Polenov M.YU., Ivanov D.A.* Organizatsiya raspredelennoy arkhitektury obrabotki dannykh dlya geoinformatsionnykh sistem [Organization of a distributed data processing architecture for geoinformation systems], *Komp'yuternye i informatsionnye tekhnologii v nauke, inzhenerii i upravlenii «KomTekh-2020»: Mater. Vserossiyskoy nauchno-tekhnicheskoy konferentsii s mezhdunarodnym uchastiem* [Proceedings of the All-Russian scientific and technical conference with international participation on Computer and information technologies in science, engineering and management (ComTech-2020)]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2020, Vol. 1, pp. 480-484.
13. Qt 5.15. Available at: https://doc.qt.io/qt-5/index.html (accessed 27 October 2020).
14. osgEarth – Geospatial SDK for OpenSceneGraph. Available at: http://osgearth.org/ (accessed 27 October 2020).
15. OpenSceneGraph. Available at: http://www.openscenegraph.org/ (accessed 27 October 2020).
16. *Ivanov D.A.* Ispol'zovanie geoprostranstvennykh dannykh Cesium Ion v srede osgEarth [Using Cesium Ion geospatial data in the osgEarth environment], *Informatsionnye tekhnologii, sistemnyy analiz i upravlenie (ITSAU-2019): Sb. trudov XVII Vserossiyskoy nauchnoy konferentsii* [Proceedings of the XVII All-Russian scientific conference on Information technology, system analysis and management (ITSAU-2019)]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2019, Vol. 1, pp. 10-12.
17. eProsima Fast DDS Documentation. Available at: https://fast-dds.docs.eprosima.com/en/latest/ (accessed 27 October 2020).
18. Fast RTPS installation PX4 v1.9.0 Developer Guide. Available at: https://dev.px4.io/v1.9.0/en/setup/fast-rtps-installation.html (accessed 27 October 2020).
19. *Hohpe G. Woolf B.* Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Pearson Education, 2012, 106 p.
20. *Buschmann F., Meunier R., Rohnert H., Sommerlad P., Stal M.* Pattern Oriented Software Architecture. A System of Patterns. Vol. 1. John Wiley & Sons, 1996, pp. 339-343.

Статью рекомендовал к опубликованию д.т.н., профессор В.И. Божич.

Поленов Максим Юрьевич – Южный федеральный университет; e-mail: mypolenov@sfedu.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634371550; кафедра вычислительной техники; к.т.н.; доцент.

Иванов Даниил Александрович – АО «Научно-конструкторское бюро вычислительных систем»; e-mail: ivanovdaniil2009@yandex.ru; 347936, г. Таганрог, ул. 1-я Линия, 144а; тел.: 88634682560; программист.

Polenov Maxim Yuryevich – Southern Federal University; e-mail: mypolenov@sfedu.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +78634371550; the department of computer engineering; cand. of eng. sc.; associate professor.

Ivanov Daniil Alexandrovich – JSC “Scientific Design Bureau of Computing Systems”; e-mail: ivanovdaniil2009@yandex.ru; 1 Liniya street, 144-a, Taganrog, 347936, Russia; phone: +78634682560; programmer.

УДК 004.021 DOI 10.18522/2311-3103-2020-6-108-117

А.В. Анзина, А.Д. Медведева, Е.А. Емельянов

АЛГОРИТМ АВТОМАТИЧЕСКОГО ПОДБОРА МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ЗАВИСИМОСТИ ОТ РЕЗУЛЬТАТОВ ОТЧЕТА СКАНЕРА УЯЗВИМОСТИ

Эффективная защита информации в информационной системе подразумевает регулярное проведение диагностики и мониторинга сети, компьютеров и приложений на предмет обнаружения возможных проблем в системе безопасности. Для сканирования безопасности существуют сканеры уязвимостей, сертифицированные Федеральной службой

по техническому и экспортному контролю. В результате сканирования могут быть выявлены уязвимости информационной системы, устранение которых предполагает незамедлительное реагирование, так как злоумышленники могут воспользоваться уязвимостью информационной системы и совершить атаку. Однако подбор мер защиты является трудоемким процессом и требует достаточно большого количества времени, из-за чего возникает проблема автоматизации выбора мер защиты информации. Разработка алгоритма автоматического подбора мер защиты информации является одной из задач при автоматизации процесса работы специалиста по защите информации. Основные задачи при разработке алгоритма: выбор основополагающей характеристики уязвимости, генерирование оптимального списка мер защиты с учетом класса защищенности информационной системы, сопоставление мер защиты с выбранной характеристикой. После анализа информации об уязвимостях основным показателем выбран вектор уязвимости, включающий основные метрики, оценка которых позволяет сделать выбор мер защиты. Каждой метрике путем экспертной оценки сопоставлен набор мер защиты информации. При работе алгоритма сотрудник в качестве входных параметров задает вектор уязвимости и класс защищенности информационной системы и в результате получает список необходимых мер защиты. Таким образом, алгоритм автоматического подбора предполагает сопоставление метрик уязвимости с мерами защиты информации, что позволяет сотруднику оперативно подбирать меры на основе выявленных уязвимостей.

Сканер безопасности; уязвимость; вектор уязвимости; метрика; меры защиты информации; алгоритм автоматизации.

A.V. Anzina, A.D. Medvedeva, E.A. Emelyanov

ALGORITHM FOR AUTOMATIC SELECTION OF INFORMATION PROTECTION MEASURES DEPENDING ON THE RESULTS OF THE VULNERABILITY SCANNER REPORT

Effective protection of information in an information system implies regular diagnostics and monitoring of the network, computers, and applications to detect possible problems in the security system. There are vulnerability scanners certified by the Federal Service for Technical and Export Control for security scanning. As a result of scanning, vulnerabilities of the information system can be identified, the elimination of which requires an immediate response, since attackers can take advantage of the vulnerability of the information system and carry out an attack. However, the selection of protection measures is a laborious process and requires a large amount of time, then the problem of automating the selection of information protection measures arises. The development of an algorithm for the automatic selection of information security measures is the main goal in automating the work process of an information security specialist. The main tasks in the development of the algorithm: selection of the fundamental characteristics of the vulnerability, generation of a list of protection measures taking into account the security class of the information system, comparison of protection measures with the selected characteristic. After analyzing the information about vulnerabilities, the main indicator is chosen the vulnerability vector, which includes the main metrics, the assessment of which allows the choice of protection measures. A set of information protection measures was compared to each metric by means of expert assessment. During the operation of the algorithm, the employee sets the vulnerability vector and the security class of the information system as input parameters and as a result receives a list of necessary protection measures. Thus, the automatic selection algorithm assumes a comparison of vulnerability metrics with information protection measures, which will allow an employee to quickly select measures based on the identified vulnerabilities.

Security scanner; vulnerability; vulnerability vector; metric; information protection measures; automation algorithm.

Введение. Специалистам по защите информации необходимо проводить регулярное сканирование безопасности информационной системы [1]. Для этого можно использовать следующие сканеры уязвимостей, сертифицированные Федеральной службой по техническому и экспортному контролю [2]:

- программный комплекс «Средство анализа защищенности «Сканер-ВС» [3];
- программное изделие «Сетевой сканер безопасности XSpider 7.8.25» [4];
- программный комплекс сканера «SCADA-аудитор» [5];
- система анализа защищенности программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер Ревизор Сети версия 3.0) [6];
- система контроля защищенности и соответствия стандартам MaxPatrol 8 [7].

Результатом сканирования информационной системы является отчет о выявленных уязвимостях, которые требует быстрого реагирования для предотвращения возможных атак на уязвимости. Для этого необходимо проверить исключается ли выявленная уязвимость обновлением программного обеспечения (ПО) и не содержит ли уязвимостей обновленная версия ПО. Некоторые уязвимости невозможно решить при помощи обновления, поэтому для их устранения необходимо прибегнуть к дополнительным мерам защиты информации. Выбор мер защиты и их внедрение несет достаточно большое количество временных затрат и является трудоемким процессом, так как меры защиты содержатся в различных документах, например, Приказ ФСТЭК 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [8], Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [9], Методический документ меры защиты информации в государственных информационных системах [10]. Сопоставление и выявление мер защиты может затянуться на большой период времени, когда реагировать надо незамедлительно, ведь злоумышленник может воспользоваться моментом и совершить вредоносную атаку.

По данным статистики сайта tadviser.ru [11] проблема несвоевременного устранения критических уязвимостей приводит к крупным утечкам данных. Из-за несвоевременного реагирования на уязвимость RunC CVE-2019-5736, позволяющей выполнить код в системе с правами суперпользователя. Проект Docker Hub упустил в апреле 2019 года данные порядка 190 тыс. пользователей, включая токены для репозиториев GitHub и Bitbucket.

Анализ основных характеристик для разработки алгоритма. Для решения проблем несвоевременного устранения уязвимостей предлагается автоматизировать выбор мер защиты. Таким образом, целью исследования является разработка алгоритма автоматического подбора мер защиты информации в зависимости от основных характеристик уязвимости.

Главные задачи для достижения необходимого результата:

- анализ отчетов проверки описанными выше средствами сервисов и систем на предмет присутствия уязвимостей;
- анализ основных характеристик уязвимости,
- выбор основополагающей характеристики для определения мер;
- генерирование списка мер защиты с учетом класса защищенности информационной системы;
- определение базовых правил для сопоставления мер защиты с выбранной характеристикой.

В качестве аналогов автоматизации управления уязвимостями может выступать комплексное решение Security Vision Cyber Risk System (CRS). Область оценки автоматически измеряется в качественных и количественных характеристиках, обнаруженные риски подвергаются моделированию исходов, риски автоматически обрабатываются (при использовании совместно с Security Vision [IRP]). [12]. Данное программное обеспечение включает модуль управления уязвимостями, который осуществляет мониторинг ИТ-инфраструктуры, контролируя появление новых уяз-

вимостей и категорируя по степени критичности уже найденные. В отличие от CRS, новизной алгоритма автоматического подбора мер защиты информации является анализ данных после сканирования безопасности, соответствующими программными изделиями, и наличие оптимального сопоставления мер защиты уязвимостям.

В результате сканирования безопасности выдается отчет о его результатах, в котором содержится название уязвимости, меры по ее устранению, в некоторых случая меры не указываются. Алгоритм автоматического подбора мер защиты предполагает анализ результатов сканирования, основной информацией является название уязвимости и идентификатор в формате «CVE:», а также некоторые отчеты, например отчет MaxPatrol 8 включает в себя информацию о векторе уязвимости. Учитывая данную информацию, можно найти любую уязвимость в базе данных и получить другие характеристики уязвимости.

Согласно ISO/IEC 27000:2014 [13] уязвимостью называют слабость актива или управления, эксплуатация которой приведет к реализации одной или нескольких угроз.

Для сопоставления уязвимости и мер защиты необходимо оценить показатели уязвимости, которые отражают возможные проблемы в информационной системе [14]. Таким показателем является вектор уязвимости, представляющий собой текстовую строку с перечислением основным критериев, интерпретировать которые можно на основе общей системы оценки уязвимостей.

Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS) [15] представляет собой стандарт, который позволяет выявить основные характеристики уязвимости и получить числовую оценку, отражающую ее серьезность. CVSS включает в себя три группы метрик:

- Базовая группа показателей отражает характеристики уязвимости, которые постоянны во времени и не зависят от среды исполнения.
- Временная группа метрик представляет характеристики уязвимости, которые меняются со временем, но не среди пользовательских сред.
- Контекстная группа метрик описывает характеристики уязвимости, которые актуальны для конкретной пользовательской среды.

Каждая группа метрик представляет собой числовой показатель по десятибалльной шкале, на основе которого можно определить приоритет уязвимости и своевременно принять необходимые меры по устранению возможной угрозы безопасности.

Количественная оценка степени опасности уязвимости осуществляется на основе анализа базового вектора уязвимости, а временные и контекстные метрики применяются для уточнения оценки опасности уязвимости, если информации из базового вектора недостаточно.

Базовый вектор уязвимости CVSS включает в себя шесть метрик, каждые из которых могут принимать одно из трёх значений:

1. Способ получения доступа (Access Vector – AV):
   - Локальный (Local – L) – получение физического доступа к объекту.
   - Смежный (Adjacent – A) – получение доступа к объекту из локальной вычислительной сети.
   - Глобальный (Network – N) – получение доступа к объекту из любой вычислительной сети, связанной с объектом атаки.
2. Сложность получения доступа (Access Complexity – AC):
   - Высокая (High – H) – для получения доступа необходимо выполнение особых условий (повышение привилегий и др.).
   - Средняя (Mid – M) – для получения доступа необходимо выполнение специальных условий (прохождение нестандартной процедуры аутентификации и др.).
   - Низкая (Low – L) – для получения доступа не требуется выполнение специальных условий.

3. Показатель аутентификации (Authentication – Au):
- ♦ None (N) – аутентификация не требуется.
- ♦ Single (S) – требуется однократная аутентификация.
- ♦ Multiple (M) – требуется многократная аутентификация.

4. Влияние на конфиденциальность (Confidentiality Impact – C):
- ♦ None (N) – нет влияния на конфиденциальность данных.
- ♦ Partial (P) – частичное влияние на конфиденциальность данных.
- ♦ Complete (C) – полное нарушение конфиденциальности данных.

5. Влияние на целостность (Integrity Impact – I):
- ♦ None (N) – нет влияния на целостность данных.
- ♦ Partial (P) – частичное уничтожение или модифицирование данных.
- ♦ Complete (C) – полное нарушение целостности данных.

6. Влияние на доступность (Availability Impact – A):
- ♦ None (N) – нет влияния на доступность данных.
- ♦ Partial (P) – кратковременное блокирование данных.
- ♦ Complete (C) – полное нарушение доступности данных.

Разработанный алгоритм. Первые три метрики предназначены для получения информации о проблемах в информационной системе, которые могут привести к атаке. Следующие три метрики базовой группы определяют возможные последствия эксплуатации уязвимости.

На основе текстовых критериев можно определить наиболее подходящие меры защиты, которые позволяют своевременно устранить уязвимости [16]. Сопоставление метрик из базового вектора и мер защиты информации показаны в виде блок-схемы, изображенной на рис. 1.

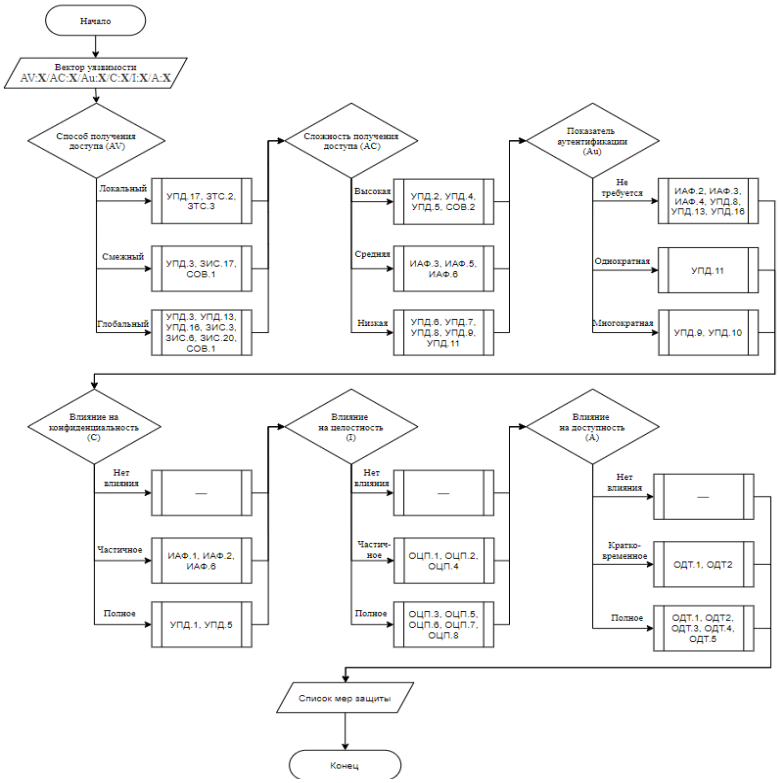

Рис. 1. Алгоритм работы модуля сопоставления мер защиты и уязвимостей

Перед началом работы алгоритма автоматического подбора мер защиты информации производится сканирование на предмет защищенности информационной системы [17], применяя сканеры уязвимостей. При выполнении алгоритма анализируется сгенерированный отчет на предмет наличия вектора уязвимости, если его нет, то по названию уязвимости и обращению к базе данных уязвимостей находится вектор. Следующим шагом происходит сопоставление метрик вектора уязвимости и мер защиты, который представлена на рис. 1. В результате работы алгоритма выводится список мер защиты информации [18–20]. Работа алгоритма представлена в виде блок-схемы на рис. 2.

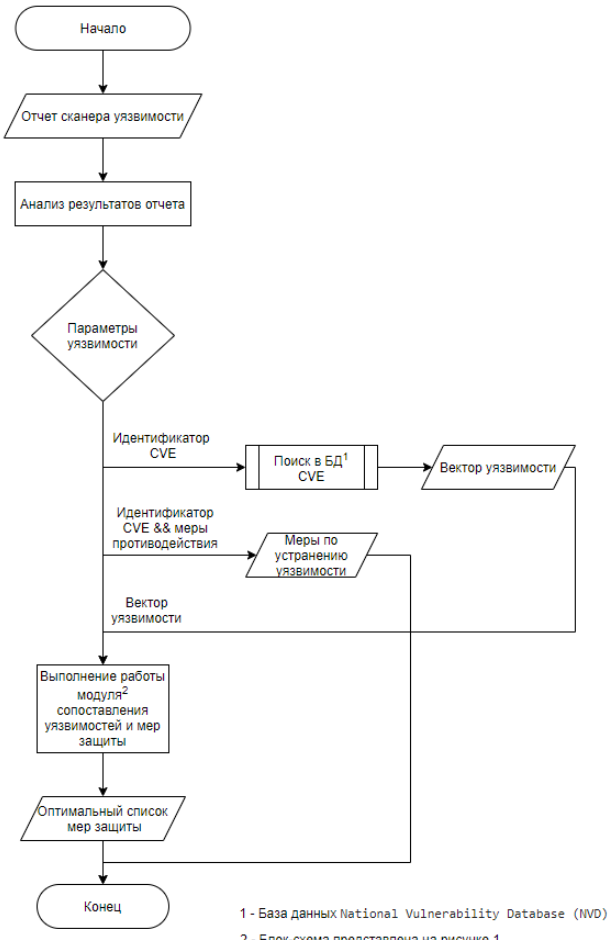

Рис. 2. Блок-схема автоматического подбора мер защиты информации в зависимости от результатов отчета сканера уязвимости

Заключение. В результате исследования разработан алгоритм автоматического подбора мер защиты, исходя из результатов отчета сканера уязвимости. Алгоритм предлагает оптимальный набор мер, которые позволяют устранить уязвимости. Выбор мер защиты происходит на основании метрик, содержащихся в векторе уязвимости. Информация о векторе содержится в отчете сканеров безопасности, либо осуществляется поиск в общедоступной базе данных уязвимостей. Таким образом, алгоритм позволяет пользователю своевременно получить оптимальный список мер и внедрить их. В дальнейшем в качестве улучшения может быть пред-

ложено рассмотрение не только вектора уязвимости, но дополнительных параметров – для повышения эффективности сопоставления мер защиты, а также сопоставление мер и средств защиты, что приведет к сокращению времени между выявлением уязвимостей и внедрением мер защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – URL: https://fstec.ru/component/attachments/download/290 (дата обращения: 01.12.2020).
2. Государственный реестр сертифицированных средств защиты информации. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения: 01.12.2020).
3. Средство анализа защищенности «Сканер-ВС». – URL: https://scaner-vs.ru/ (дата обращения: 28.11.2020).
4. Сетевой сканер безопасности XSpider 7.8.25. – URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (дата обращения: 28.11.2020).
5. Программный комплекс сканера «SCADA-аудитор». – URL: http://ntcsiz.ru/stuff/products/prez_scada_auditor.pdf (дата обращения: 28.11.2020).
6. Система анализа защищенности программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер Ревизор Сети версия 3.0). – URL: http://prp.su/files/support/rseti/rseti3.0_rukovodstvo_po_ustanovke_i_ekspluatatsii.pdf (дата обращения: 28.11.2020).
7. Система контроля защищенности и соответствия стандартам MaxPatrol. – URL: https://www.ptsecurity.com/ru-ru/products/mp8/ (дата обращения: 28.11.2020).
8. Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – URL: https://fstec.ru/component/attachments/ download/566 (дата обращения: 28.11.2020).
9. Приказ ФСТЭК РФ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – URL: https://fstec.ru/component/attachments/download/561 (дата обращения: 28.11.2020).
10. Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 г. – URL: https://fstec.ru/component/attachments/download/675 (дата обращения: 28.11.2020).
11. Анализ «громких» инцидентов в сфере информационной безопасности в 2019 году. – URL: https://www.tadviser.ru/index.php/Статья:Анализ_громких_инцидентов_в_сфере_информационной_безопасности_в_2019_году (дата обращения: 01.12.2020).
12. Security Vision Cyber Risk System (CRS). – URL: https://www.securityvision.ru/products/crs/ (дата обращения: 01.12.2020).
13. Международный стандарт ISO/IEC 27000:2014 «Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь». – URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf (дата обращения: 01.12.2020).
14. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». – URL: http://base.garant.ru/70252506/ (дата обращения 01.12.2020).
15. Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/ (дата обращения: 01.12.2020).
16. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // Российская газета. – 2014, 17 сентября. – N 6483(211).

17. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах». – URL: https://fstec.ru/component/ attachments/download/812 (дата обращения: 01.12.2020).
18. Руководящий документ от 30.03.1992 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». – URL: https://fstec.ru/component/ attachments/download/296 (дата обращения: 01.12.2020).
19. Аудит информационной безопасности. – URL: https://studref.com/431893/informatika/ audit_informatsionnoy_bezopasnosti (дата обращения: 01.12.2020).
20. Аудит сетевой и телекоммуникационной инфраструктуры. – URL: http://www.nestor.minsk.by/sr/2005/07/sr50714.html (дата обращения: 01.12.2020).

REFERENCES

1. Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh [Methodology for determining actual threats to the security of personal data during their processing in personal data information systems]. Available at: https://fstec.ru/component/attachments/download/290 (accessed 01 December 2020).
2. Gosudarstvennyy reestr sertifitsirovannykh sredstv zashchity informatsii [State register of certified information security]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (accessed 01 December 2020).
3. Sredstvo analiza zashchishchennosti «Skaner-VS» [Security analysis tool "Scanner-VS"]. Available at: URL: https://scaner-vs.ru/ (accessed 28 November 2020).
4. Setevoy skaner bezopasnosti XSpider 7.8.25 [Network security scanner XSpider 7.8.25]. Available at: URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (accessed 28 November 2020).
5. Programmnyy kompleks skanera «SCADA-auditor» [Software complex of the scanner "SCADA-auditor"]. Available at: http://ntcsiz.ru/stuff/products/prez_scada_auditor.pdf (accessed 28 November 2020).
6. Sistema analiza zashchishchennosti programmnogo i apparatnogo obespecheniya TCP/IP setey (setevoy skaner Revizor Seti versiya 3.0) [System for analyzing the security of software and hardware TCP / IP networks (network scanner Network Inspector version 3.0)]. Available at: http://prp.su/files/support/rseti/rseti3.0_rukovodstvo_po_ustanovke_i_ekspluatatsii.pdf (accessed 28 November 2020).
7. Sistema kontrolya zashchishchennosti i sootvetstviya standartam MaxPatrol [Security control system and compliance with standards MaxPatrol 8]. Available at: https://www.ptsecurity.com/ ru-ru/products/mp8/ (accessed 28 November 2020).
8. Prikaz FSTEK RF ot 11 fevralya 2013 g. № 17 «Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh» [Order of the FSTEC RF of February 11, 2013 No. 17 "On approval of requirements for the protection of information that does not constitute a state secret contained in state information systems"]. Available at: https://fstec.ru/component/attachments/download/566 (accessed 28 November 2020).
9. Prikaz FSTEK RF ot 18 fevralya 2013 g. № 21 «Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» [Order of the FSTEC RF dated February 18, 2013 No. 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems"]. Available at: https://fstec.ru/component/ attachments/download/561 (accessed 28 November 2020).
10. Metodicheskiy dokument «Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh», utverzhdennyy FSTEK Rossii 11 fevralya 2014 g. [Methodological document "Measures of information protection in state information systems", approved by the FSTEC of Russia on February 11, 2014] Available at: https://fstec.ru/component/attachments/download/675 (accessed 28 November 2020).

11. Analiz «gromkikh» intsidentov v sfere informatsionnoy bezopasnosti v 2019 godu [Analysis of "high-profile" incidents in the field of information security in 2019]. Available at: https://www.tadviser.ru/index.php/Stat'ya:Analiz_gromkikh_intsidentov_v_sfere_informatsionnoy_bezopasnosti_v_2019_godu (accessed 01 December 2020).
12. Security Vision Cyber Risk System (CRS). Available at: https://www.securityvision.ru/ products/crs/ (accessed 01 December 2020).
13. Mezhdunarodnyy standart ISO/IEC 27000:2014 «Informatsionnye tekhnologii – Metody i sredstva obespecheniya bezopasnosti – Sistemy menedzhmenta informatsionnoy bezopasnosti – Obshchie svedeniya i slovar'». [International standard ISO / IEC 27000: 2014 "Information technology - Methods and means of ensuring security – Information security management systems – General information and vocabulary"]. Available at: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf (accessed 01 December 2020).
14. Postanovlenie Pravitel'stva RF ot 01.11.2012 №1119 «Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» [Decree of the Government of the Russian Federation of 01.11.2012 No. 1119 "On approval of requirements for the protection of personal data when processing them in personal data information systems"]. Available at: http://base.garant.ru/70252506/ (accessed 01 December 2020).
15. Bank dannykh ugroz bezopasnosti informatsii [Databank of threats to information security]. Available at: https://bdu.fstec.ru/ (accessed 01 December 2020).
16. Prikaz Federal'noy sluzhby bezopasnosti Rossiyskoy Federatsii ot 10 iyulya 2014 g. N 378 g. Moskva «Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh s ispol'zovaniem sredstv kriptograficheskoy zashchity informatsii, neobkhodimykh dlya vypolneniya ustanovlennykh Pravitel'stvom Rossiyskoy Federatsii trebovaniy k zashchite personal'nykh dannykh dlya kazhdogo iz urovney zashchishchennosti» [Order of the Federal Security Service of the Russian Federation of July 10, 2014 N 378, Moscow "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems using cryptographic information protection tools required to fulfill the requirements established by the Government of the Russian Federation for the protection of personal data for each of the security levels"], *Rossiyskaya gazeta* [Rossiyskaya Gazeta], 2014, 17 sentyabrya, N 6483(211).
17. Metodicheskiy dokument FSTEK Rossii «Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh» [Methodological document of FSTEC of Russia "Methodology for determining threats to information security in information systems"]. Available at: https://fstec.ru/component/attachments/download/812 (accessed 01 December 2020).
18. Rukovodyashchiy dokument ot 30.03.1992 «Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii» [Guidance document dated 30.03.1992 “Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection”. Available at: https://fstec.ru/ component/attachments/download/296 (accessed 01 December 2020).
19. Audit informatsionnoy bezopasnosti [Audit of information security]. Available at: https://studref.com/431893/informatika/audit_informatsionnoy_bezopasnosti (accessed 01 December 2020).
20. Audit setevoy i telekommunikatsionnoy infrastruktury [Audit of the network and telecommunications infrastructure]. Available at: http://www.nestor.minsk.by/sr/2005/07/sr50714.html (accessed 01 December 2020).

Статью рекомендовал к опубликованию к.т.н., доцент Д.В. Орёл.

Анзина Антонина Викторовна – Северо-Кавказский федеральный университет; e-mail: anttoniinav@gmail.com; 355041, г. Ставрополь, ул. Кулакова, 2; студентка.

Медведева Анастасия Дмитриевна – e-mail: medvedeva.nastya26@mail.ru; студентка.

Емельянов Евгений Алексеевич – e-mail: eemelianov@ncfu.ru: тел.: +79886261908; преподаватель.

Anzina Antonina Viktorovna – North Caucasus Federal University; e-mail: anttoniinav@gmail.com; 2, Kulakova street, Stavropol, 355041, Russia; student.

Medvedeva Anastasia Dmitrievna – e-mail: medvedeva.nastya26@mail.ru; student.

Emelyanov Evgeny Alekseevich – e-mail: eemelianov@ncfu.ru; phone: +79886261908; lecturer.

УДК 004.056.5 DOI 10.18522/2311-3103-2020-6-117-128

В.А. Буковшин, П.А. Чуб, Д.А. Короченцев, Л.В. Черкесова, Н.В. Болдырихин, О.А. Сафарьян

АНАЛИЗ ЗАШИФРОВАННОГО СЕТЕВОГО ТРАФИКА НА ОСНОВЕ ВЫЧИСЛЕНИЯ ЭНТРОПИИ И ПРИМЕНЕНИЯ НЕЙРОСЕТЕВЫХ КЛАССИФИКАТОРОВ

Анализ сетевого трафика позволяет решить множество задач, таких как: определение закономерности передачи данных по сети, сбор статистики об использовании веб–приложений, мониторинг и дальнейшее исследование сетевой нагрузки, определение потенциальных вредоносных программных средств и сетевых атак и т.д. На данный момент до 40% Интернет–траффика принадлежит неизвестным приложениям. Это говорит о том, что для области анализа сетевого трафика задача классификации приложений приобрела особую важность. Совершенствование программного обеспечения в области сетевых технологий способствовало обнаружению серьёзных уязвимостей в реализации некоторых сетевых протоколов, а именно: TCP и HTTP. С помощью анализаторов сетевого трафика злоумышленник получал доступ к содержимому пакетов данных, передающихся по сети. Однако с повышением квалификации информационного сообщества в области компьютерной безопасности, а также с развитием стандартов сетевых технологий, анализ сетевого трафика заметно усложнился. Возросшее применение математических методов защиты информации, таких как симметричные и ассиметричные криптографические протоколы, привела к тому, что большинство подходов к анализу сетевого трафика потеряли значение и перестали применяться. Поэтому актуален поиск новых решений задачи классификации сетевого трафика с учетом возможности его шифрования. Статья посвящена описанию нового смешанного подхода к анализу сетевого трафика, основанного на совокупном использовании теории информации и алгоритмов машинного обучения. Также приводится сравнительный анализ предложенного метода с уже существующими подходами, основанными как на теории информации, так и на машинном обучении. Целью исследований является разработка алгоритма, основанного на интеллектуальном подходе к анализу сетевого трафика. Предлагаемый алгоритм базируется на вычислении энтропии и применении нейросетевых классификаторов. Задачи исследований включают: проведение теоретического обоснования предложенного подхода в области теории информации, а также алгоритмов машинного обучения; проведение структурного описания реализованных алгоритмов вычисления энтропии и классификации приложений, генерирующих зашифрованный траффик; сравнительный анализ предложенного алгоритма с уже существующими подходами к анализу зашифрованного сетевого трафика. Результатом исследований является новый алгоритм, позволяющий с высокой степенью достоверности классифицировать различные виды зашифрованного трафика.

Сетевой трафик; машинное обучение; персептрон; нейронная сеть; нейрон; автокодировщик; функция активации; N-усечённая энтропия; функция максимального правдоподобия.