УДК 004.056
Doi: 10.31772/2712-8970-2022-23-4-593-601

Для цитирования: Исаев С. В., Кононов Д. Д. Исследование динамики и классификация атак на веб-сервисы корпоративной сети // Сибирский аэрокосмический журнал. 2022. Т. 23, № 4. С. 593–601. Doi: 10.31772/2712-8970-2022-23-4-593-601.

For citation: Isaev S. V., Kononov D. D. [A study of dynamics and classification of attacks on corporate network web services]. *Siberian Aerospace Journal.* 2022, Vol. 23, No. 4, P. 593–601. Doi: 10.31772/2712-8970-2022-23-4-593-601.

Исследование динамики и классификация атак на веб-сервисы корпоративной сети

С. В. Исаев, Д. Д. Кононов*

Институт вычислительного моделирования СО РАН
Российская Федерация, 660036, Красноярск, ул. Академгородок, 50/44
*E-mail: ddk@icm.krasn.ru

В статье представлено исследование динамики атак на веб-сервисы с использованием классификации киберугроз по типам на примере корпоративной сети Красноярского научного центра СО РАН. Анализ проведен на основе журналов веб-сервисов и позволяет решить актуальные задачи обеспечения комплексной безопасности веб-сервисов, в том числе выявить как существующие, так и потенциальные угрозы кибербезопасности. Проведен обзор основных подходов к обработке и анализу журналов. Авторы описывают тип и состав источников данных и приводят список используемого программного обеспечения. Особенностью исследования является длительный период наблюдения. Предложена структура системы обработки и реализован программный комплекс для анализа и классификации атак. В работе показано, что использование классифицированных выборок позволяет обнаружить периодичность и выявить тренды по отдельным видам атак. Анализ показал, что наиболее эффективным способом обнаружения повышения риска киберугроз является анализ классифицированных угроз с агрегацией до месяца. Неклассифицированные атаки имеют схожие параметры распределения по разным годам, в случае же применения классификации параметры распределения существенно меняются, что позволяет отслеживать риски в автоматизированных системах предотвращения вторжений. Была построена матрица корреляций по типам атак. Анализ показал, что большинство типов атак имеет слабую корреляцию, за исключением атак «инъекция команд», «просмотр директории», «инъекция кода Ява», которые можно агрегировать. Авторами предложен эвристический метод сравнения рисков, основанный на классификации киберугроз. Метод использует статистические параметры распределений выборок и позволяет работать с различными временными интервалами. В работе выполнена геопривязка IP-адресов, с которых проводились атаки, построены профили атак для разных стран и приведен список стран, имеющих стабильный профиль атак. В заключение указаны особенности предложенного метода и обозначены перспективы использования в других областях.

Ключевые слова: анализ, безопасность, веб, интернет, атака, корпоративная сеть.

A study of dynamics and classification of attacks on corporate network web services

S. V. Isaev, D. D. Kononov*

Institute of Computational Modelling of the SB RAS
50/44, Akademgorodok St., Krasnoyarsk, 660036, Russian Federation
*E-mail: ddk@icm.krasn.ru

The article presents a study of the dynamics of attacks on web services using the classification of cyber threats by type on the example of the corporate network of the Krasnoyarsk Scientific Center of the Siberian Branch of the Russian Academy of Sciences. The analysis was carried out on the basis of web services logs and allows solving urgent problems of ensuring the integrated security of web services, including identifying both existing and potential cybersecurity threats. A review of the main approaches to the processing and analysis of logs is provided. The authors describe the type and composition of data sources and provide a list of the software used. A feature of the study is the long observation period. The structure of the processing system is proposed and software tools for attack analysis and classification are implemented. The work shows that the use of classified samples allows detecting periodicity and reveal trends of certain types of attacks. Unclassified attacks have similar distribution parameters for different years, while in the case of classification, the distribution parameters change significantly, which makes it possible to track risks in automated intrusion prevention systems. A correlation matrix by type of attack was constructed. The analysis showed that most attack types have weak correlation, with the exception of the attacks "command injection", "directory browsing", "Java code injection", which can be aggregated. The authors proposed a heuristic method of risk comparison based on cyber threat classification. The method uses statistical parameters of sample distributions and allows working with different time intervals. The paper georeferenced the IP addresses from which the attacks were carried out, built attack profiles for different countries, and provided a list of countries with a stable attack profile. The conclusion indicates the features of the proposed method and outlines the prospects for its use in other areas.

Keywords: analysis, security, web, internet, attack, corporate network.

Введение

В настоящее время многие компании используют веб-технологии для организации корпоративных сервисов различного уровня (почта, облачные технологии, хостинг, видеоконференции). Необходимо отметить, что веб-сервисы подвержены рискам информационной безопасности, поскольку функционируют в открытой сети Интернет. Важной часть функционирования современных информационных систем является задача обеспечения информационной безопасности, которая является комплексной и включает набор мероприятий на различных уровнях, выполнение которых позволяет снизить риски киберугроз. Одним из важных компонентов по обеспечению безопасности является анализ различных журналов активности, которые генерирует система [1]. В частности, представляет интерес журналы веб-серверов nginx и apache, анализ которых позволяет выявить кибератаки, совершаемые на систему. В веб-системах объемы журналов могут иметь значительные размеры, что затрудняет их анализ в ручном режиме, в этом случае необходимо использовать автоматизированные инструменты для обработки и анализа данных [2]. Как правило, анализ данных предусматривает обработку различными программными средствами и представляет собой многоступенчатый процесс [3; 4]. Полученные при анализе данные можно использовать для моделирования системы информационной безопасности [5] либо для сопоставления поведенческих шаблонов оборудования реальным кибератакам [6].

Смежные работы

При анализе журналов используются разные подходы. Один из самых популярных методов является сигнатурный анализ. Обработчики журналов используют заранее определенные сигнатуры для идентификации вредоносных событий и их классификацию [7; 8]. При этом из элементов журнала могут извлекаться дополнительные параметры и характеристики, которые могут быть использованы для последующего анализа, например, кластеризации и обнаружения аномалий [9]. Как правило, сбои во время кибератак порождают записи журнала, которые отличаются от записей, представляющих штатное поведение системы. Поэтому целесообразно обращать внимание на отдельные записи журнала, которые не вписываются в общую картину. При кластеризации такие записи идентифицируются высокой степенью несходства со всеми существующими кластерами или не соответствуют никаким сигнатурам [10; 11]. Однако не все неблагоприятное события системы проявляются в виде отдельных аномальных записей журнала,

а, скорее, в виде динамических или последовательных аномалий. Поэтому необходимы подходы, которые позволяют группировать последовательности записей или выявлять временные закономерности и корреляции. Динамическая кластеризация позволяет идентифицировать события, имеющие несколько разнородных и разрозненных по времени записей в журнале [12; 13], что даёт возможность обнаруживать неявное нештатное поведение.

Существующие работы используют различные методы анализа журналов сервисов. Часто авторы описывают методику анализа и в качестве примера используют тестовые данные, что не позволяет оценить работоспособность подхода на реальных данных. Либо используются реальные данные с короткими временными интервалами, что затрудняет анализ динамики происходящих процессов за различные периоды.

В данной работе проводится исследование безопасности корпоративной сети Красноярского научного центра (ФИЦ КНЦ СО РАН) на основе анализа журналов веб-сервисов. Целью работы является анализ безопасности веб-сервисов в динамике за последние 2 года, классификация кибератак по видам, выявление зависимостей между различными параметрами атак. В отличие от существующих работ, анализ выполняется на длительных временных интервалах, что позволяет выявить динамику поведения веб-сервисов по часам, дням, месяцам и годам. Работа является продолжением исследования безопасности веб-сервисов корпоративной сети [14], по сравнению с предыдущей работой выполнена классификация киберугроз по типам, предложен метод оценки рисков.

Источник данных и методика обработки

Источниками данных для анализа в работе являются данные веб-сервисов за 2020–2021 гг. и неполный 2022 г. (объем 45 Гб, 176 млн элементов). Анализ выполнялся с помощью следующих программных инструментов: UNIX tools, GAccess, libmaxmind, JSON tools, Python, Microsoft Excel. На рис. 1 представлены стадии обработки данных. Первичная обработка включает агрегацию журналов со всех веб-сервисов и унификацию формата для последующей обработки. Для всех данных выполняется геопривязка источника – определение страны по IP-адресу (GeoIP). Затем выполняется обработка ошибок (как клиентских, так и серверных) с агрегацией по различным интервалам времени (год, месяц, день, час). Также выполняется обработка атак, которая включает классификацию по типам с последующей агрегацией по геоданным. Классификация атак по типам осуществляется по OWASP [15] с использованием набора правил ModSecurity Core Rule Set [16], предназначенного для идентификации киберугроз веб-приложений. Для обработки атак был разработан комплекс программ GSec на языках Go и C, осуществляющий автоматизированную классификацию атак по типам и агрегацию данных по различным временным интервалам.

Рис. 1. Стадии обработки данных

Fig. 1. Stages of data processing

Анализ данных WWW

Анализ общего числа атак за 2020–2022 гг. показывает, что в среднем их ежедневное количество меняется в небольших пределах: 3664 в 2020 г., 3481 в 2021 г. и 3698 в 2022 г. (3 % отклонения от среднего по году). Вместе с тем максимальное число атак изменяется в широких пределах от 8500 до 21000 за день, что свидетельствует об одновременном функционировании нескольких нескоординированных источников. На рис. 2 представлена общая динамика обнаруженных атак по месяцам за 2020–2022 гг. Мы фиксируем отсутствие выраженной периодичности как при ежедневном, так и при ежемесячном суммировании.

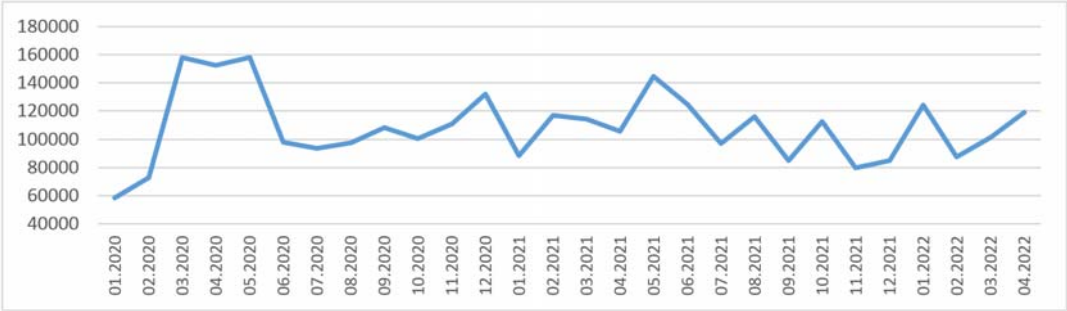


Рис. 2. Общая динамика атак по месяцам

Fig. 2. General dynamics of attacks by month

При переходе к анализу атак по видам можно выделить явные тренды на увеличение количества атак отдельных видов. На рис. 3 представлено ежемесячное количество атак типов POLICY/EXT_RESTR (запрещенное расширение) и WEB/FILE_INJ (инъекция файла), на примере которых отчетливо видно увеличение интенсивности в 2 и более раза, незаметное на рис. 2.

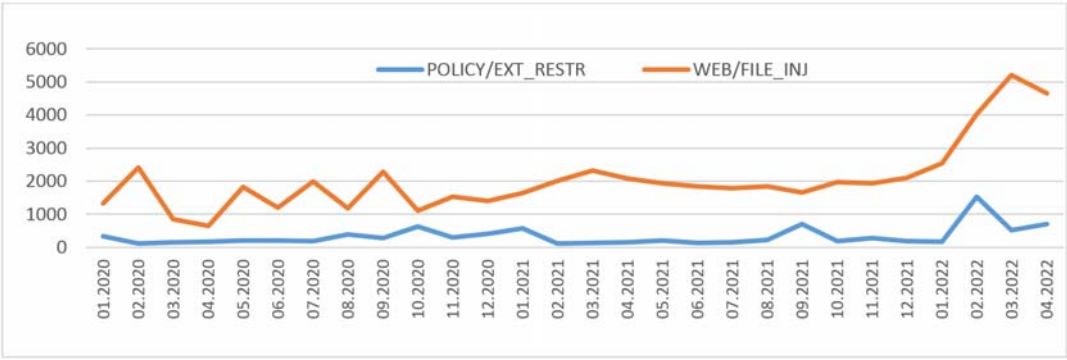


Рис. 3. Динамика классифицированных атак по месяцам

Fig. 3. Dynamics of classified attacks by month

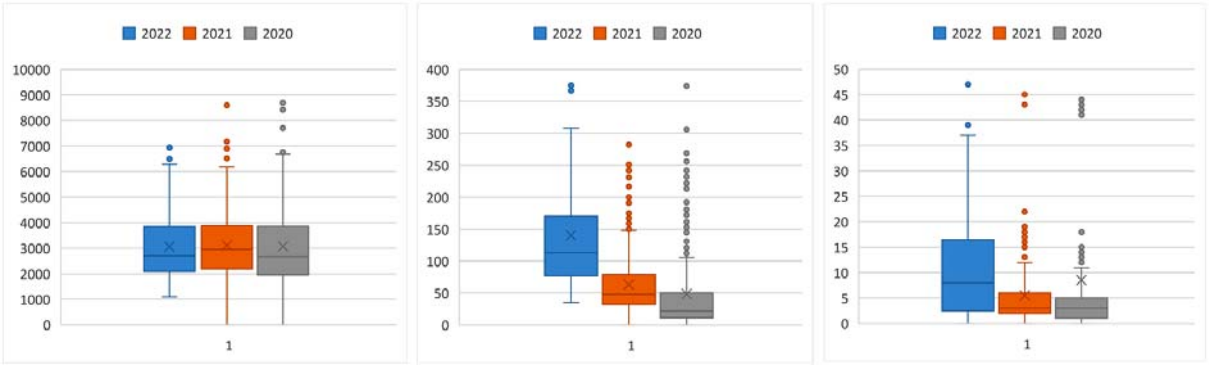
На графике агрегации по дням за 2022 г. (рис. 4) незаметен обнаруженный на рис. 3 восходящий тренд. Виден отдельный пик в районе 26 февраля 2022 г., который можно связать с массовыми кибератаками на интернет-ресурсы России. Таким образом, наиболее эффективным способом обнаружения повышения риска киберугроз является анализ классифицированных угроз с агрегацией до месяца.

На рис. 5 приведены диаграммы размаха для распределений за 2022, 2021 и 2020 гг.: неклассифицированные атаки (*а*), атаки типа WEB/CMD_INJ (инъекция команд) (*б*) и атаки типа WEB/FILE_INJ (инъекция файла) (*в*). Если неклассифицированное распределение атак имеет схожие параметры за разные годы, то в случае применения классификации параметры распределения изменяются достаточно существенно, особенно для 2022 г., который характеризуется

увеличением риска киберугроз. Для выбора набора показателей была построена матрица корреляций их распределений по дням за весь наблюдаемый период 2020–2022 гг. (рис. 6). Большинство показателей имеют слабую корреляцию, за исключением WEB/CMD_INJ (инъекция команд), WEB/DIR_TRAVERSAL (просмотр директории) и WEB/JAVA_INJ (инъекция кода Ява), которые можно агрегировать.

Рис. 4. Динамика неклассифицированных атак и атак типа «инъекция файлов»

Fig. 4. Dynamics of unclassified attacks and file injection attacks



а *б* *в*

Рис. 5. Диаграммы размаха атак по годам:
а – неклассифицированные; *б* – WEB/CMD_INJ; *в* – WEB/FILE_INJ

Fig. 5. Range diagrams of attacks by year:
a – unclassified; *b* – WEB/CMD_INJ; *c* – WEB/FILE_INJ

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. AUTO/CRAWLER		0,21	0,44	0,38	-0,34	0,10	-0,09	-0,10	-0,14	0,24	0,00	0,20	0,25	0,31	-0,20
2. AUTO/SCRIPT	0,21		0,10	-0,02	-0,06	-0,01	-0,15	-0,18	-0,34	0,13	-0,05	0,66	-0,34	0,28	-0,11
3. AUTO/SEC_SCAN	0,44	0,10		0,04	-0,24	-0,06	-0,30	-0,25	-0,29	-0,04	-0,22	0,09	0,17	0,29	-0,19
4. OTHERS	0,38	-0,02	0,04		-0,18	0,63	-0,08	-0,06	-0,09	0,23	-0,01	0,09	0,06	0,52	0,01
5. POLICY/EXT_RESTR	-0,34	-0,06	-0,24	-0,18		-0,09	0,55	0,60	0,46	0,12	0,50	-0,16	-0,09	-0,17	0,82
6. PROTOCOL	0,10	-0,01	-0,06	0,63	-0,09		0,20	0,18	0,06	0,09	0,28	0,41	-0,26	0,64	0,01
7. WEB/CMD_INJ	-0,09	-0,15	-0,30	-0,08	0,55	0,20		0,99	0,73	0,04	0,97	0,11	-0,11	-0,10	0,47
8. WEB/DIR_TRAVERSA	-0,10	-0,18	-0,25	-0,06	0,60	0,18	0,99		0,75	0,07	0,96	0,05	-0,06	-0,15	0,52
9. WEB/FILE_INJ	-0,14	-0,34	-0,29	-0,09	0,46	0,06	0,73	0,75		0,31	0,62	-0,11	0,07	-0,40	0,59
10. WEB/HEADER_INJ	0,24	0,13	-0,04	0,23	0,12	0,09	0,04	0,07	0,31		-0,01	-0,02	0,28	0,08	0,15
11. WEB/JAVA_INJ	0,00	-0,05	-0,22	-0,01	0,50	0,28	0,97	0,96	0,62	-0,01		0,22	-0,13	0,00	0,42
12. WEB/PHP_INJ	0,20	0,66	0,09	0,09	-0,16	0,41	0,11	0,05	-0,11	-0,02	0,22		-0,27	0,41	-0,13
13. WEB/RFI	0,25	-0,34	0,17	0,06	-0,09	-0,26	-0,11	-0,06	0,07	0,28	-0,13	-0,27		-0,26	-0,11
14. WEB/SQL_INJ	0,31	0,28	0,29	0,52	-0,17	0,64	-0,10	-0,15	-0,40	0,08	0,00	0,41	-0,26		-0,11
15. WEB/XSS	-0,20	-0,11	-0,19	0,01	0,82	0,01	0,47	0,52	0,59	0,15	0,42	-0,13	-0,11	-0,11	

Рис. 6. Матрица корреляций распределений классифицированных атак

Fig. 6. Distributions correlations matrix of classified attacks

Метод оценки изменения рисков киберугроз

На основе проведенного анализа видно, что отдельные классифицированные типы атак содержат больше информации по динамике рисков, чем неклассифицированные. Выбирая независимые классифицированные типы атак и вычисляя для временных выборок их статистические показатели, можно предложить следующий эвристический метод для оценки изменения рисков киберугроз, основанный на сравнении параметров распределений выборок. Для выборок V_1 и V_2, содержащих N независимых показателей, введем следующую функцию R оценки изменения рисков:

$$R(V_1,V_2)=\frac{1}{N}\cdot\sum_{i=1}^{N}K_i,$$

где $K_i=\begin{cases}1, \text{ если } \mu_i > 0{,}6745\cdot\sigma_i,\\ 0, \text{ если } -0{,}6745\cdot\sigma_i \le \mu_i \le 0{,}6745\cdot\sigma_i,\\ -1, \text{ если } \mu_i < -0{,}6745\cdot\sigma_i;\end{cases}$ μ_i – среднее значение выборки i-го признака выборки V_2; σ_i – среднеквадратическое отклонение выборки i-го признака выборки V_1.

Согласно предложенному методу, если среднее значение всех N признаков выборки V_2 больше третьего квартиля выборки V_1, то значение изменения риска равно 1, которое можно интерпретировать как существенное увеличение риска по всем показателям. Если среднее значение всех N признаков выборки V_2 меньше первого квартиля выборки V_1, то значение изменения риска равно –1 (уменьшение риска по всем показателям). Значение $R(V_1,V_2) \in [-1,1]$, что позволяет использовать этот показатель для анализа с помощью методов искусственного интеллекта, в частности, метода Шортлиффа.

Оценка профилей атак

Из журналов была извлечена информация о геопривязке IP-адресов и проведен анализ источников атак по типам. Рассчитаны корреляции выборок 2020 и 2021 гг. по типам атак для стран из топ-15 по интенсивности атак. Если допустить предположение, что соотношение показателей атак разного типа (профиль атаки) определяется набором программного обеспечения, используемого для проведения атаки, то высокую корреляцию таких выборок по одной стране в разные периоды времени можно интерпретировать как фиксированный набор используемого для атак ПО (атакуемых уязвимостей). Полученная диаграмма рис. 7 показывает, что странами с наиболее стабильной структурой атак являются Китай, Россия, Германия, Великобритания, США и Польша.

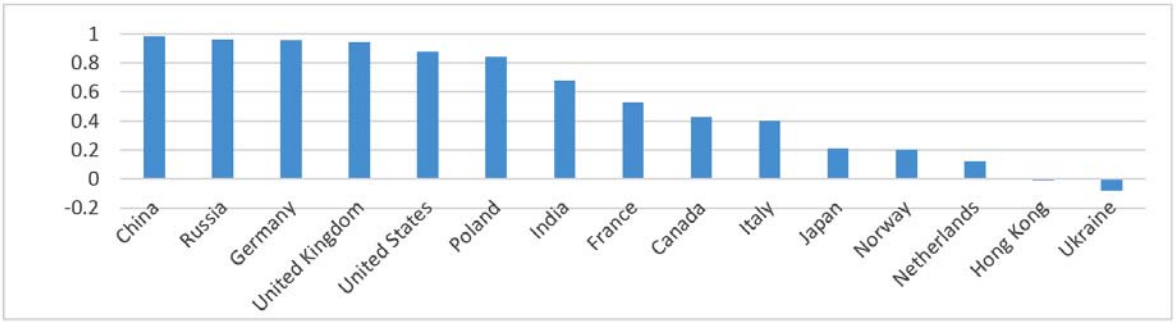


Рис. 7. Корреляция структуры атак 2020 и 2021 гг. по странам

Fig. 7. Correlation of attack patterns in 2020 and 2021 by country

Страны с низкой корреляцией (Голландия, Гонконг, Украина) не имеют постоянного набора программного обеспечения для атак и, вероятно, используются разными группами злоумышленников, контролирующих ботнет-сети.

Заключение

В работе рассмотрена динамика атак на веб-сервисы по странам, выделены основные группы стран с постоянным профилем атак и высокой их интенсивностью. Выполнено сравнение попарных корреляций различных видов атак, выявлены атаки с высокой корреляцией, которые можно агрегировать при оценке рисков. Предложен метод сравнения рисков кибербезопасности для различных периодов, использующий классификацию по видам атак. Метод не зависит от сравниваемых временных интервалов и объема выборок, так как основан на статистических показателях. Метод оценки рисков кибербезопасности может использоваться в других областях, в которых существует классификация показателей.

Библиографические ссылки

1. System log clustering approaches for cyber security applications: A survey / M. Landauer, F. Skopik, M. Wurzenberger, A. Rauber // Computers & Security. 2020. Vol. 92. P. 101739.

2. Towards Automated Log Parsing for Large-Scale Log Data Analysis / P. He, J. Zhu, S. He, J. Li et al. // IEEE Transactions on Dependable and Secure Computing. 2017. Vol. 15, No. 6. P. 931–944.

3. Detecting Web Attacks Using Multi-stage Log Analysis / M. Moh, S. Pininti, S. Doddapaneni, T. Moh // IEEE 6th International Conference on Advanced Computing (IACC). 2016. P. 733–738.

4. Tools and Benchmarks for Automated Log Parsing / Zhu J. et al. // IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). 2019. P. 121–130.

5. Ефимова Ю. В., Гаврилов А. Г. Моделирование системы информационной безопасности на основе анализа системных журналов // Инженерный вестник Дона. 2019. № 6 (57). С. 40.

6. Моделирование идентификации профиля кибератак на основе анализа поведения устройств в сети провайдера телекоммуникационных услуг / И. П. Болодурина, Д. И. Парфёнов, Л. С. Забродина и др. // Вестник Южно-Уральского гос. университета. 2019. № 4. С. 48–59.

7. Drain: an online log parsing approach with fixed depth tree / P. He, J. Zhu, Z. Zheng, M. R. Lyu // Proc. of the International Conference on Web Services (ICWS). 2017. IEEE. P. 33–40.

8. Reidemeister T., Jiang M., Ward P. A. Mining unstructured log files for recurrent fault diagnosis // Proc. of the Int. Symp. on Integrated Netw. Mgmt. IEEE. 2011. P. 377–384.

9. Сидорова Д. Н., Пивкин Е. Н. Алгоритмы и методы кластеризации данных в анализе журналов событий информационной безопасности // Безопасность цифровых технологий. 2022. № 1 (104). С. 41–60.

10. Juvonen A., Sipola T., Hamalainen T. Online anomaly detection using dimensionality reduction techniques for http log analysis // Computer Networks. 2015. No. 91. P. 46–56.

11. Incremental clustering for semi-supervised anomaly detection applied on log data / M. Wurzenberger, F. Skopik, M. Landaueret al. // Proc. of the 12th International Conference on Availability, Reliability and Security. ACM. 2017. P. 31:1–31:6.

12. One graph is worth a thousand logs: uncovering hidden structures in massive system event logs / M. Aharon, G. Barash, I. Cohen, E. Mordechai // Proc. of the Joint Eur. Conf. on Machine Learning and Knowledge Discovery in Databases. Springer. 2009. P. 227–243.

13. Logsed: anomaly diagnosis through mining time-weighted control flow graph in logs / T. Jia, L. Yang, P. Chen et al. // Proc. of the 10th Int. Conf. on Cloud Comp. (CLOUD). IEEE. 2017. P. 447–455.

14. Kononov D., Isaev S. Analysis of the dynamics of Internet threats for corporate network web services // CEUR Workshop Proceedings. The 2nd Siberian Scientific Workshop on Data Analysis Technologies with Applications 2021. 2021. Vol. 3047. P. 71–78.

15. Analysis of Web Security Using Open Web Application Security Project 10 / M. A. Helmiawan, E. Firmansyah, I. Fadil et al. // 8th International Conference on Cyber and IT Service Management (CITSM). 2020. P. 1–5.

16. OWASP ModSecurity Core Rule Set [Электронный ресурс]. URL: https://owasp.org/www-project-modsecurity-core-rule-set/ (дата обращения: 13.05.2022).

References

1. Landauer M., Skopik F., Wurzenberger M., Rauber A. System log clustering approaches for cyber security applications: A survey. *Computers & Security*. 2020, Vol. 92, P. 101739.

2. He P., Zhu J., He S., Li J. et al. Towards Automated Log Parsing for Large-Scale Log Data Analysis. *IEEE Transactions on Dependable and Secure Computing.* 2017, Vol. 15, No. 6, P. 931–944.

3. Moh M., Pininti S., Doddapaneni S., Moh T. Detecting Web Attacks Using Multi-stage Log Analysis. *IEEE 6th International Conference on Advanced Computing (IACC)*. 2016, P. 733–738.

4. Zhu J. et al. Tools and Benchmarks for Automated Log Parsing. *IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP).* 2019, P. 121–130.

5. Efimova Yu. V., Gavrilov A. G. [Modeling an information security system based on the analysis of system logs]. *Inzhenernyi vestnik Dona*. 2019, No. 6 (57), P. 40 (In Russ.).

6. Bolodurina I. P., Parfenov D. I., Zabrodina L. S. et al. [Modeling the identification of a cyber attack profile based on the analysis of the behavior of devices in the network of a telecommunications service provider]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta*. 2019, No. 4, P. 48–59 (In Russ.).

7. He P., Zhu J., Zheng Z., Lyu M. R. Drain: an online log parsing approach with fixed depth tree. *Proc. of the International Conference on Web Services (ICWS).* IEEE, 2017, P. 33-40.

8. Reidemeister T., Jiang M., Ward P. A. Mining unstructured log files for recurrent fault diagnosis. *Proc. of the Int. Symp. on Integrated Netw. Mgmt.* IEEE, 2011, P. 377–384.

9. Sidorova D. N., Pivkin E. N. [Algorithms and methods of data clustering in the analysis of information security event logs]. *Bezopasnost' tsifrovykh tekhnologii*. 2022, No. 1 (104), P. 41–60 (In Russ.).

10. Juvonen A., Sipola T., Hamalainen T. Online anomaly detection using dimensionality reduction techniques for http log analysis. *Computer Networks.* 2015, No. 91, P. 46–56.

11. Wurzenberger M., Skopik F., Landauer M., Greitbauer P., Fiedler R., Kastner W. Incremental clustering for semi-supervised anomaly detection applied on log data. *Proc. of the 12th International Conference on Availability, Reliability and Security,* ACM (2017), P. 31:1–31:6.

12. Aharon M., Barash G., Cohen I., Mordechai E. One graph is worth a thousand logs: uncovering hidden structures in massive system event logs. *Proc. of the Joint Eur. Conf. on Machine Learning and Knowledge Discovery in Databases.* Springer, 2009, P. 227–243.

13. Jia T., Yang L., Chen P., Li Y., Meng F., Xu J. Logsed: anomaly diagnosis through mining time-weighted control flow graph in logs. *Proc. of the 10th Int. Conf. on Cloud Comp. (CLOUD).* IEEE, 2017, P. 447–455.

14. Kononov D., Isaev S. Analysis of the dynamics of Internet threats for corporate network web services. *CEUR Workshop Proceedings. The 2nd Siberian Scientific Workshop on Data Analysis Technologies with Applications 2021.* 2021, Vol. 3047, P. 71–78.

15. Helmiawan M. A., Firmansyah E., Fadil I., Sofivan Y., Mahardika F. and Guntara A. Analysis of Web Security Using Open Web Application Security Project 10. *8th International Conference on Cyber and IT Service Management (CITSM).* 2020, P. 1–5.

16. OWASP ModSecurity Core Rule Set. Available at: https://owasp.org/www-project-modsecurity-core-rule-set/ (accessed: 13.05.2022).

© Исаев С. В., Кононов Д. Д., 2022

Исаев Сергей Владиславович – кандидат технических наук, доцент, заведующий отделом информационно-телекоммуникационных технологий; Институт вычислительного моделирования СО РАН. E-mail: si@icm.krasn.ru.

Кононов Дмитрий Дмитриевич – научный сотрудник; Институт вычислительного моделирования СО РАН. E-mail: ddk@icm.krasn.ru.

Isaev Sergey Vladislavovich – Cand. Sc., associate professor, head of the Department of Information and Telecommunication Technologies; Institute of Computational Modeling SB RAS. E-mail: si@icm.krasn.ru.

Kononov Dmitry Dmitrievich – scientific researcher; Institute of Computational Modeling SB RAS. E-mail: ddk@icm.krasn.ru.