УДК 681.322.067

А.В. Павлычев, К.С. Солдатов, В.А. Сказин

Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения

Разработан алгоритм поиска и выявления сетевых аномалий в системных журналах операционной системы Microsoft Windows с применением методов машинного обучения. Проведены предобработка, кластеризация и визуализация исследуемых данных. Предложенный алгоритм подтвердил свою эффективность, выявив в исследуемом наборе данных события, являющиеся признаками работы вредоносного программного обеспечения.
Ключевые слова: аудит безопасности, системные журналы Windows, машинное обучение, кластеризация, сетевые аномалии.
DOI: 10.21293/1818-0442-2021-24-4-27-32

В современном цифровом мире на передний план выходят задачи обеспечения целостности, доступности и конфиденциальности информации, обрабатываемой в государственных и иных информационных системах.

Согласно отчетам крупнейших аналитических центров, одной из наиболее заметных в 2020 и 2021 гг. угроз в области кибербезопасности является использование так называемых вирусов-шифровальщиков (Ransomware) [1, 2]. Деятельность различных хакерских группировок направлена на получение несанкционированного сетевого доступа в целевую информационную инфраструктуру с целью похищения информации ограниченного распространения с дальнейшим шифрованием пользовательских данных и требованием финансового выкупа как за расшифровку данных, так и за нераспространение конфиденциальной информации [3].

Ввиду изменения ландшафта киберугроз изменяются и подходы к обеспечению информационной безопасности. Сегодня основная цель организации состоит в правильной оценке киберрисков, а также разработке системы адекватных мер реагирования [4, 5].

Выявление сетевых аномалий представляет собой важную задачу в рамках построения превентивной системы обеспечения информационной безопасности и эффективного противодействия несанкционированному доступу. Особенно данная задача актуальна для объектов критической информационной инфраструктуры [6].

Одним из способов выявления сетевых аномалий является исследование файлов журналов различных информационных систем, в том числе системных журналов операционной системы [7].

В настоящий момент Windows – самая популярная операционная система в мире. По данным аналитического агентства StatCounter по состоянию на сентябрь 2021 г., данная операционная система установлена на 76,13% всех компьютеров, в России данный показатель составляет 78,34%. Если рассматривать конкретные версии операционной системы Windows, по состоянию на август 2021 г. самой популярной в мире версией является Windows 10 (78,34%), за ней следуют Windows 7 (15,98%), Windows 8.1 (3,62%), Windows 8 (1,15%). В России места распределены следующим образом: Windows 10 (75,79%), Windows 7 (16,74%), Windows 8.1 (3,79%), Windows 8 (2,29%) [8].

В операционной системе Windows ведутся журналы, которые регистрируют пользовательские события и работу системных и прикладных программ на компьютере.

Журналы событий Windows содержат ряд дескрипторов, позволяющих объединять события в такие категории, как «информационные» и «критические». Отдельные идентификаторы указывают на конкретные типы событий, а последние версии Windows имеют отдельные файлы журналов событий для различных приложений и служб [9].

Несмотря на имеющиеся во встроенном приложении для работы с журналами варианты фильтрации, специалисту по информационной безопасности зачастую сложно найти интересующее его событие среди большого объема хранимых данных. Особенно задача усложняется при необходимости расследования компьютерного инцидента, в ходе которого требуется изучить большое количество взаимосвязанных событий, которые могут находиться в разных журналах [10].

Журнал событий представляет собой бинарный файл специального формата (с расширением EVTX), схожий с файлом базы данных. Журнал включает в себя следующие данные:

1. Уровень. Указывает, к какому типу относится событие:

1.1. Предупреждение – некритичное событие, которое указывает на возможность возникновения более серьезных ошибок в будущем. Предупреждением считается восстановление приложения без утраты данных или потери функциональности.

1.2. Ошибка – событие, которое указывает на значительную проблему, например на потерю функциональности или утрату данных.

1.3. Сведения – события, которые описывают успешную работу службы, драйвера или приложения. Например, целесообразно создать информационное событие в случае успешной загрузки сетевого драйвера.

1.4. Аудит успеха – событие, которое фиксирует проверенную успешную попытку доступа к функционалу безопасности. К таким событиям можно отнести успешную попытку пользователя войти в систему.

1.5. Аудит отказа – событие, которое фиксирует проверенную неудачную попытку доступа к функционалу безопасности. Например, событие будет создано, если пользователь попытается получить доступ к диску, который не будет предоставлен.

2. Дата и время регистрации события.

3. Источник события – это имя программного обеспечения, которое регистрирует событие. Часто это имя приложения или имя подкомпонента приложения, если оно большое.

4. Категории. Помогают объединять события, чтобы программа просмотра событий могла их фильтровать. Каждый источник событий может определять свои собственные пронумерованные категории и текстовые строки, в которые они отображаются. Категории должны быть пронумерованы последовательно, начиная с номера 1. Могут храниться в отдельном файле сообщений или в файле, который содержит сообщения других типов.

5. Идентификаторы событий. Однозначно идентифицируют конкретное событие. Каждый источник событий может определять свои собственные пронумерованные события и строки описания, с которыми они отображаются в своем файле сообщений.

6. Пользователь. Содержит имя пользователя, от которого выполнялись процессы. Многие события связаны с конкретными пользователями, имена которых указаны в данном поле.

7. Компьютер. Указывает имя компьютера, на котором произошла регистрация события.

Аудит безопасности является инструментом, который необходимо использовать для поддержания целостности системы. Базовая политика аудита определяет категории связанных с безопасностью событий, указанные для проверки. Когда Windows впервые устанавливается, все категории аудита отключены. Включая различные категории событий аудита, появляется возможность реализовать политику аудита, которая соответствует установленным требованиям безопасности.

Журнал безопасности записывает каждое событие в соответствии с политиками аудита, которые устанавливаются для каждого объекта. В аудит могут быть добавлены следующие категории событий:

1) аудит событий входа;
2) аудит доступа к объектам;
3) аудит отслеживания процессов;
4) аудит доступа к службе каталогов;
5) аудит событий входа в аккаунт;
6) аудит управления учетными записями;
7) изменение политики аудита;
8) использование привилегий аудита;
9) аудит системных событий.

Методология поиска аномалий в системных журналах

Алгоритм выявления аномалий состоит из пяти основных этапов: сбор файлов системных журналов, предварительная обработка данных, снижение размерности и визуализация, кластеризация данных и поиск аномалий.

Сбор файлов системных журналов: стандартное приложение «Просмотр событий» позволяет выгружать события в формате *.csv. На первом этапе производится выгрузка содержимого системного журнала Security (журнал безопасности) в csv-файл. Данный журнал содержит события, относящиеся к безопасности компьютера, например, вход/выход пользователя, доступ к объектам, изменение политик и т.д.

Предварительная обработка данных: выгружаемый csv-файл зачастую содержит данные в плохо структурированной форме и представленные в некорректном формате. Цель предварительной обработки – удаление событий или признаков, в дальнейшем не используемых в алгоритме. Также на этом этапе производится приведение данных к однообразному виду для лучшей кластеризации.

Снижение размерности и визуализация: алгоритмы снижения размерности широко применяются в визуализации данных в пространстве большой размерности. Визуализация данных критически важна для понимания и интерпретации структуры больших наборов данных [11]. Наиболее популярным алгоритмом на сегодняшний день является алгоритм t-SNE.

t-SNE представляет собой итерационный алгоритм визуализации многомерных данных путем сопоставления точек данных в двух- или трехмерном пространстве. Он создает единую карту, которая показывает внутренние структуры в многомерном наборе данных, включая тенденции, закономерности и выбросы, с помощью метода нелинейного уменьшения размеров [12]. Рассмотрим математическую модель алгоритма.

Если дан набор из N объектов высокой размерности x_i, …, x_j, то для набора объектов вычисляются вероятности $P(i|j)$, которые пропорциональны похожести объектов x_i и x_j:

$$P_{i|j} = \frac{\exp\left(\frac{-\left|x_i - x_j\right|^2}{2\sigma_i^2}\right)}{\sum_{k \neq j}^{n} \exp\left(\frac{-\left|x_i - x_k\right|^2}{2\sigma_i^2}\right)}, \quad (1)$$

σ_i – дисперсия в точке данных x_i, x_j в качестве соседа выбирает x_j, основываясь на пропорции его гауссовой плотности вероятности с центром в точке x_i:

$$P_{ij} = \frac{P_{j|i} + P_{i|j}}{2n}. \quad (2)$$

Для близлежащих точек $P(i|j)$ плотность будет высокой, а для точек, расположенных далеко друг от друга, $P(i|j)$ будет незначительной. Плотность распределения вероятности двух точек прямо пропорциональна сходству этих точек.

На следующем шаге работы алгоритм стремится получить отображение $y_1, \ldots, y_n$ в d-мерное пространство, которое отражает, насколько это возможно, похожести $P(i|j)$. Для этого алгоритм измеряет похожесть $q(i|j)$ между двумя точками y_i и y_j:

$$q_{ij} = \frac{\left(1+\left\|y_i - y_j\right\|^2\right)^{-1}}{\sum_{k\neq 1}\left(1+\left\|y_k - y_i\right\|^2\right)^{-1}}. \quad (3)$$

Затем для того, чтобы непохожие объекты расположить далеко друг от друга, происходит измерение похожести между точками в пространстве низкой размерности.

Расположение точек y_i в пространстве малой размерности определяется минимизацией расстояния Кульбака–Лейблера распределения Q от распределения P, т.е.

$$KL\left(P\|Q\right) = \sum_{(i\neq j)} P_{ij} \log \frac{p_{ij}}{q_{ij}}. \quad (4)$$

Минимизация расстояния Кульбака–Лейблера к точкам y_i осуществляется с помощью градиентного спуска. Результатом оптимизации является отображение, которое отражает похожесть между объектами пространства высокой размерности.

Также необходимо использовать кластеризацию, т.е. решить задачу разделения всех данных на группы (кластеры) таким образом, чтобы объекты с разных групп отличались друг от друга, а объекты в одной группе были «похожи» друг на друга [13, 14]. В данной работе рассматривается метод DBSCAN. Данный алгоритм имеет ряд преимуществ:

- не требует спецификации числа кластеров;
- умеет находить кластеры произвольной формы;
- имеет понятия шума и устойчивости к выбросам;
- требует всего два параметра и нечувствителен к порядку точек в базе данных.

Рассмотрим математическую модель данного алгоритма.

Для множества объектов X задана метрическая функция расстояния ρ, minOb_j – минимальное количество соседних объектов, необходимых для образования одного кластера, а ε – максимальное расстояние между соседними объектами.

Объект $p \in X$ будет являться кластерным, если в ε-окрестности точки p находятся minOb_j объектов (включая сам объект p). Такие объекты называются прямо достижимыми из p. Объект $q \in X$ называется достижимым из p, если существует такой путь $p_1, \ldots, p_n$, где $p_1 = p$ и $p_n = q$, а каждый объект $p_i + 1$ достижим из p_i. Отсюда следует, что все объекты в пути, кроме объекта q, должны быть кластерными. Все объекты, которые не достижимы ни из одного другого объекта, считаются выбросами (шумом). Соответственно, кластером является множество кластерных объектов, достижимых друг из друга, а также граничные объекты, которые достижимы из любой другой точки кластера [15].

Расстояние ρ между двумя объектами кластеризуемого множества вычисляется с использованием метрики Евклида:

$$Q(p,q) = \sqrt{(p_1-q_1)^2 + (p_2-q_2)^2 + \ldots (p_n-q_n)^2} = \\ = \sqrt{\sum_{k=1}^{n}(p_k-q_k)^2}. \quad (5)$$

В данной работе в качестве аномалий считаются данные, находящиеся в кластере «–1». В данный кластер заносятся данные, которые алгоритм считает выбросами (шумом).

Результаты

На первом этапе с тестового компьютера осуществлена выгрузка файла журнала «Security.evtx». Содержимое журнала импортировано в csv-файл для дальнейшей обработки. Выбор компьютера обусловлен зафиксированной на нем вредоносной активностью в течение продолжительного периода времени.

На втором этапе в ходе предобработки в итоговый набор данных выбраны следующие поля:

«TimeWritten» – время создания события;

«EventID» – идентификатор события;

«EventType» – идентификатор типа события;

«EventCategory» – идентификатор категории события.

На третьем этапе применяем алгоритм визуализации и снижения размерности итогового набора данных t-SNE (рис. 1).

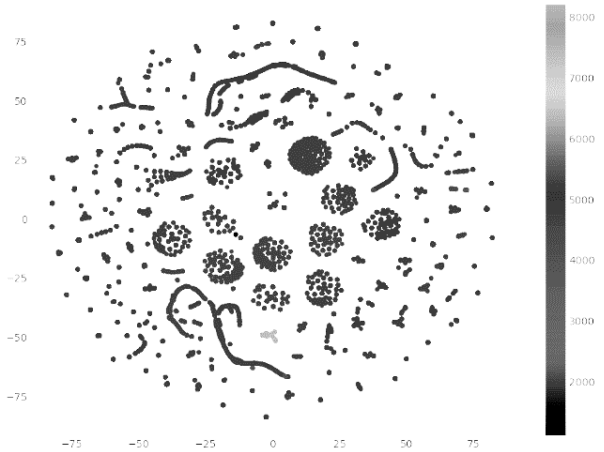

Рис. 1. Результат применения алгоритма t-SNE

На четвертом этапе итоговый набор данных кластеризован с помощью алгоритма DBSCAN. Коэффициент максимального расстояния между соседними объектами и коэффициент минимального количества соседних объектов, необходимых для образования кластера, определялись путем перебора.

На рис. 2 звездочками выделены аномальные выбросы нашего набора данных.

Последним этапом с помощью ранее описанного метода кластеризации выявляются выбросы (шумы). Результатом работы кластеризации является

csv-файл, содержащий информацию об аномальном событии: идентификатор события и время его возникновения. Для выявления вредоносной активности необходимо в исходном файле журнала событий найти выявленное «аномальное» событие и проверить соседние события, предшествующие или наступившие после возникновения «аномального» события.

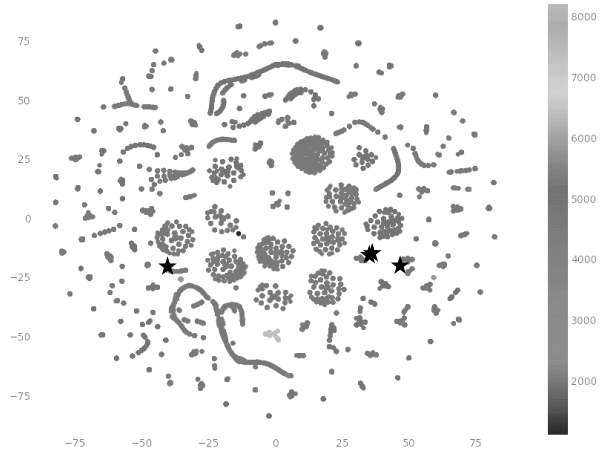

Рис. 2. Результат кластеризации DBSCAN

В результате работы алгоритм выделил в качестве аномалий следующие события (EventID):

4624: пользователь успешно вошел в систему. Может быть признаком несанкционированных действий при выполнении дополнительных условий, например вход в систему во внерабочее время;

4672: особые привилегии, назначенные новому входу в систему. Событие генерируется для входа в новую учетную запись, если для нового сеанса входа в систему назначены какие-либо особые привилегии;

4657: изменено значение реестра. Является одним из ключевых событий в системе, поскольку целью большинства вредоносных программ – является модификация пользовательских или системных данных;

4663: попытка доступа к объекту. Может иметь важное значение при копировании «тела» вируса или создании скрипта для последующего исполнения.

При проверке исходных файлов журналов выявлено, что события 4624 и 4672 следуют друг за другом. Событие 4624 (пользователь успешно вошел в систему) зафиксировало использование NTLM пакета аутентификации и тип входа – 3 (пользователь или компьютер вошел на этот компьютер из сети). Отличие легитимного соединения NTLM – использование пароля. Следовательно, в случае, если данный вход осуществлялся пользователем, события в журнале должны быть следующие:

4768: запрошен билет проверки подлинности Kerberos (TGT);

4769: запрошен билет службы Kerberos (TGS);

4648: попытка входа в систему с использованием явных учетных данных;

4624: учетная запись была успешно авторизована.

В исходном файле журнала после события 4624 зафиксировано событие 4672 (особые привилегии, назначенные новому входу в систему), что может свидетельствовать об успешно проведенной атаке типа pass-the-hash. Данная атака направлена на обход механизма авторизации по протоколу NTLM.

События 4663 и 4657 фиксируются через короткий промежуток времени и также следуют друг за другом. Событие 4663 (попытка доступа к объекту) фиксирует создание файла «mmkt.exe» в директории «%System Root%\Users\All Users», а событие 4657 (изменено значение реестра) – добавление ранее созданного исполняемого файла в ключе автозапуска системного реестра ([HKCU\Software\Microsoft\Windows\CurrentVersion\Run]).

Использование техники pass-the-hash с дальнейшим закреплением на атакуемой машине может являться индикацией заражения устройства.

Дальнейшая проверка данного устройства антивирусом выявила ВПО, классифицируемое как «Trojan.Win32.MIMIKATZ.AEG».

В результате описанной процедуры было обработано 4 000 событий (N). Каждое из событий было отдельно изучено и промаркировано. При применении рассмотренного алгоритма неправильно были отнесены к аномальным 22 события (FP), неправильно были распознаны в качестве неаномальных 4 события (FN).

Проведем расчет точности (6), уровня ошибок первого рода (7) и уровня ошибок второго рода (8):

$$Acc = \left(1 - \frac{FN + FP}{N}\right) \times 100\%, \quad (6)$$

$$P_1 = \frac{FP}{N}, \quad (7)$$

$$P_2 = \frac{FN}{N}. \quad (8)$$

В результате расчетов получим следующие значения: точность – 99,35%, уровень ошибок первого рода – $5{,}5 \cdot 10^{-3}$, уровень ошибок второго рода – 10^{-3}.

Заключение

В ходе исследования был разработан способ выявления сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения. Предложенный алгоритм подтвердил свою эффективность, выявив в исследуемом наборе данных события, являющиеся признаками работы вредоносного программного обеспечения.

Литература

1. Solar JSOC Security Report. Итоги 2020 года [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/ upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf, свободный (дата обращения: 02.12.2021).

2. Kaspersky Security Bulletin. Обзор активности APT-групп в 2020 году [Электронный ресурс]. – Режим доступа: https://securelist.ru/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99480, свободный (дата обращения: 02.12.2021).

3. Xin L. Awareness Education as the Key to Ransomware Prevention / L. Xin, Q. Liao // Information Systems Security. – 2012. – Vol. 16, No. 4. – P. 195–202.

4. Signature-less ransomware detection and mitigation / Y.S. Joshi, H. Mahajan, S.N. Joshi et al. // J. Comput Virol Hack Tech. – 2021. – No. 17. – P. 299–306.

5. Zavarsky P. Experimental analysis of ransomware on windows and android platforms: evolution and characterization / P. Zavarsky, D. Lindskog // Procedia Comput. Sci. – 2016. – Vol. 94. – P. 465–472.

6. Кибербезопасность 2020–2021. Тренды и прогнозы [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2020-2021/, свободный (дата обращения: 02.12.2021).

7. Berlin K., Slater D., Saxe J. Malicious Behavior Detection using Windows Audit Logs // In Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. Association for Computing Machinery, New York, NY, USA, 2015. – https://arxiv.org/pdf/1506.04200.pdf

8. Развитие информационных угроз во втором квартале 2021 года. Статистика по ПК [Электронный ресурс]. – Режим доступа: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/, свободный (дата обращения: 02.12.2021).

9. CIS Microsoft Windows Desktop Benchmarks: Securing Microsoft Windows Desktop an objective, consensus-driven security guideline for the Microsoft Windows Desktop Operating Systems [Электронный ресурс]. – Режим доступа: https://www.cisecurity.org/benchmark/microsoft_windows_desktop/, свободный (дата обращения: 02.12.2021).

10. Ring M., Schlör D., Wunderlich S., Landes D., Hotho A. Malware detection on windows audit logs using LSTMs // Computers&Security. – 2021. – Vol. 109. – P. 1–12.

11. Thomas T. Machine learning approaches in cyber security analytics / T. Thomas, A.P. Vijayaraghavan, S. Emmanuel. – Singapore: Springer, 2020. – 217 p.

12. Aldahoul N. Model fusion of deep neural networks for anomaly detection / N. Aldahoul, H.A. Karim, A. Wazir // J. of Big Data. – 2021. – No. 8. – P. 106.

13. Patcha A. An overview of anomaly detection techniques: Existing solutions and latest technological trends / A. Patcha, Jung-Min Park // Computer Networks. – 2007. – Vol. 51, Iss. – 12. – P. 3448–3470.

14. Kwon D., Kim H., Kim J. et al. A survey of deep learning-based network anomaly detection // Cluster Comput. – 2019. – No. 22. – P. 949–961.

15. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning / Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS-17). – 2017. – DOI 10.1145/3133956.3134015

Павлычев Алексей Викторович
Директор Центра информационной безопасности
Дальневосточного федерального ун-та (ДВФУ)
Аякс п., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-994-000-04-40
Эл. почта: pavlychev.av@dvfu.ru

Солдатов Константин Сергеевич
Канд. физ.-мат. наук, доцент
Департамента информационной безопасности ДВФУ
Аякс п., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-914-686-53-11
Эл. почта: soldatov_ks@dvfu.ru

Сказин Виктор Андреевич
Вед. специалист Центра информационной безопасности ДВФУ
Аякс п., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-968-142-59-50
Эл. почта: skazin_va@dvfu.ru

Pavlychev A.V., Soldatov K.S., Skazin V.A.

Network anomaly detection in the Microsoft Windows system logs using machine learning methods

An algorithm for network anomaly detection in the system security logs of the Microsoft Windows operating system with using machine learning methods was developed. Preprocessing, clustering, and visualization of the studied data were carried out. The proposed algorithm has confirmed its efficiency by identifying events in the studied dataset that indicate the operation of a malicious software.

Keywords: cybersecurity audit, Windows system journals, machine learning, clusterization, network anomaly.
DOI: 10.21293/1818-0442-2021-24-4-27-32

References

1. Solar JSOC Security Report. Results of 2020. Available at: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf, free (Accessed: December 02, 2021).

2. Kaspersky Security Bulletin [Overview of APT Group Activity in 2020]. Available at: https://securelist.ru/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99480, free (Accessed: December 02, 2021) (in Russ.).

3. Xin Luo, Qinyu Liao. Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, 2012, vol. 16, no. 4, pp. 195–202.

4. Joshi Y.S., Mahajan H., Joshi S.N. et al. Signature-less ransomware detection and mitigation. *Journal of Computer Virology and Hacking Techniques*, 2021, no. 17, pp. 299–306.

5. Zavarsky P., Lindskog D. et al. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 2016, vol. 94, pp. 465–472.

6. [Cybersecurity 2020-2021. Trends and Forecasts]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2020-2021, free (Accessed: December 02, 2021) (in Russ.).

7. Berlin K., Slater D., Saxe J. Malicious Behavior Detection using Windows Audit Logs. *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. Association for Computing Machinery*, New York, NY, USA (2015). https://arxiv.org/pdf/1506.04200.pdf

8. [Development of information threats in the second quarter of 2021. PC statistics]. Available at: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/, free (Accessed: December 02, 2021) (in Russ.).

9. CIS Microsoft Windows Desktop Benchmarks: Securing Microsoft Windows Desktop An objective, consensus-driven security guideline for the Microsoft Windows Desktop Operating Systems. Available at: https://www.cisecurity.org/benchmark/microsoft_windows_desktop/, free (Accessed: December 02, 2021).

10. Ring M., Schlör D., Wunderlich S., Landes D., Hotho A. Malware detection on windows audit logs using LSTMs. *Computers & Security*, 2021, vol. 109, pp. 1–12.

11. Thomas T., Vijayaraghavan A.P., Emmanuel S. *Machine Learning Approaches in Cyber Security Analytics*. Singapore: Springer, 2020, 217 p.

12. Aldahoul N., Karim H.A., Wazir A. Model fusion of deep neural networks for anomaly detection. *Journal of Big Data*, 2021, no. 8, pp. 106.

13. Animesh P., Jung-Min P. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 2007, vol. 51, iss. 12. P. 3448–3470.

14. Kwon D., Kim H., Kim J., Suh S.C., Kim I., Kim K.J. A survey of deep learning-based network anomaly detection. *Cluster Computing*, 2019, 22(1), P. 949–961.

15. Du Min, Li Feifei, Zheng Guineng, Srikumar Vivek. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (*CCS-17*), 2017. DOI 10.1145/3133956.3134015

Aleksey V. Pavlychev
Director, Cybersecurity Center,
Far Eastern Federal University (FEFU)
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-994-000-04-40
Email: pavlychev.av@dvfu.ru

Konstantin S. Soldatov
Candidate of Science in Physics and Mathematics,
Department of Information Security FEFU
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-914-686-53-11
Email: soldatov_ks@dvfu.ru

Viktor A. Skazin
Leading expert, Cybersecurity Center FEFU
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-968-142-59-50
Email: skazin_va@dvfu.ru