УДК 004.6 DOI 10.37468/2307-1400-2024-1-35-45

К ВОПРОСУ О ПРИЗНАКАХ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

Власов Дмитрий Сергеевич [1]

[1] Главное управление МЧС России по г. Санкт-Петербургу, г. Санкт-Петербург, Россия

АННОТАЦИЯ

В работе ставится задача выявления инсайдерской деятельности в организациях, приводящей к угрозам информационной безопасности, одним из первых шагов чего должен стать обзор научных публикаций предметной области и выделение основных признаков инсайдеров. Цель работы заключается в систематизации основных признаков инсайдеров, используемых при работе соответствующих способов; для этого применялись следующие научные методы: обзор научных публикаций, выделение признаков инсайдеров, их анализ и систематизация. Новизна исследования определяется тем, что в отличие от отдельных групп признаков, используемых существующими способами обнаружения инсайдеров, в данной работе представлен их набор из 15 элементов, подходящий для всего множества решений; а именно следующий: жадность, биография, психология, личность, коммутация, предиспозиционность, профессиональность (рабочая), аномальность поведения, распространение информации, изменения файлов, сбор информации (избыточной), телефонные переговоры, лояльность, физигномичность, нелегальные действия. Теоретическая значимость заключается в том, что получен единый набор признаков инсайдеров, включающий все частные, используемые в существующих способов. Практическая значимость состоит в получении признаков инсайдеров, на базе которых может быть построен единый мета-способ, учитывающий преимущества существующих.

Ключевые слова: информационная безопасность, инсайдер, организация, обзор, систематизация, признаки.

ON THE QUESTION OF SIGNS OF INSIDER ACTIVITY

Vlasov Dmitry S. [1]

[1] EMERCOM of Russia Main Directorate in the St. Petersburg city, Saint-Petersburg, Russia

ABSTRACT

The work sets the task of identifying insider activities in organizations that lead to threats to information security, one of the first steps of which should be a review of scientific publications in the subject area and identifying the main characteristics of insiders. The purpose of the work is to systematize the main characteristics of insiders used in the work of the corresponding methods; For this purpose, the following scientific methods were used: review of scientific publications, identification of insider characteristics, their analysis and systematization. The novelty of the research is determined by the fact that, in contrast to individual groups of features used by existing methods for detecting insiders, this work presents their set of 15 elements, suitable for the entire set of solutions; namely the following: greed, biography, psychology, personality, switching, predispositional, professional (working), abnormal behavior, dissemination of information, file changes, collection of information (redundant), telephone conversations, loyalty, physiognomy, illegal actions. The theoretical significance lies in the fact that a single set of insider attributes has been obtained, including all private ones used in existing methods. The practical significance lies in obtaining the characteristics of insiders, on the basis of which a unified meta-method can be built, taking into account the advantages of existing ones.

Keywords: information security, insider, organization, review, systematization, signs.

Введение

Информация уже достаточно давно стала основой функционирования современного мира. Как следствие, актуализировались информационные угрозы, влияющее не только на отдельных людей и организации любого размера и профиля, но даже и на целые государства [1-6]. В результате вопросам защиты информации стало уделяться еще более существенное внимания.

Однако, если программно-технические средства и могут обеспечить некоторый удовлетворительный уровень защиты, то человеческий фактор продолжает играть ключевую роль в информационной безопасности. Так, наличие такого феномена, как *инсайдерство*, может свести на нет даже самые сложные и продуманные системы, поскольку они в основном учитывают угрозы со стороны объекта физического мира со строгими алгоритмами действия (даже, если источником и является изощренный злоумышленник), не всегда принимая во внимание его противоположность (в соответствии с подходом категориального деления [7]) – субъекта, обладающего разумом и крайне недетерминированным (а, следовательно, не предсказуемым) поведением. Таким образом, задача выявления инсайдеров в организациях является актуальной, требующей отдельного глубокого изучения.

В данной статье производится обзор научных публикаций (продолжая предыдущие исследования автора [8]), посвященных или частично затрагивающих существующие способы выявления инсайдеров на предмет используемых ими признаков. Это позволит как совершенствовать существующие способы, так и создавать новые, гипотетические более совершенные за счет более всестороннего учета особенностей инсайдерской деятельности.

Обзор научных работ

Приведем точки зрения научной общественности на различные способы обнаружения инсайдеров в организациях и используемые для этого признаки.

В [9] производится обзор методов поиска инсайдеров в компьютерной сети с выделением следующих из них: использование DLP-систем, обеспечивающих анализ информации определенного формата, в том числе, на основе цифровых отпечатков; контроль передачи ее по сети; скачивание документов на различные носители и их печать; использование SIEM-систем для фиксирования аномального поведения сотрудников; детектирование логических бомб; нахождение дефектов в коде [10, 11]; привлечение нарушителя с помощью муляжа части системы (т.е. применение HoneyPot); контроль найма сотрудников.

Согласно [12], предлагается такой способ обнаружения инсайдера, как биометрическая аутентификация. При этом она позволяет выявить нарушителя на ранней стадии, что могут предложить далеко не все способы, например, такие, как DLP-системы. Выделяют такие методы биометрии, как распознавание по отпечаткам пальцев, радужной оболочке глаза, геометрии лиц в статике и динамике. Взаимная однозначность биометрических данных и сотрудника позволяет эффективно бороться с нарушителями еще до момента совершения киберпреступлений.

В работе [13] описаны способы вычисления инсайдера в банковской системе. В качестве основных и организационных способов выделено выявление инсайдера по психологическим признакам среди действующих сотрудников и при найме, определение потенциальных нарушителей, выявление аномального скрытного поведения. К техническим способам относят контроль подозрительной активности, сбор информации, не соответствующей должностным обязанностям, активное заметание следов.

Статья [14] приводит ряд технических способов обнаружения инсайдеров, а именно следующих: перехват информации, передаваемой сотрудником, с помощью средств DLP-систем; привлечение внимания инсайдера с помощью систем HoneyPot (муляжа части информационной системы) и HoneyToken (информационной обманки с возможностью слежения за ее перемещением при хищении); использование SIEM-систем для анализа данных и оповещения о инцидентах в реальном времени; отслеживание изменений в конфигурационных и прочих файлах с помощью программ tripwire [15].

В [16] производится анализ основных способов обнаружения инсайдеров в корпоративной информационной системе. Среди них выделяют следующие: перехват информации от пользователя с помощью средств DLP-систем, передаваемой по сети и на различные носители и периферийные устройства; привлечения внима-

ния нарушителя с помощью HoneyPot или их сети HoneyNet, а также HoneyToken (информации-приманки в виде псевдо-важного файла, пары логин или пароль и т.п. с отслеживанием перемещений); выявление аномальной активности сотрудника и его отклонений от заданного режима работы; обнаружение логических бомб и backdoor средствами SIEM-систем. Также одним из способов является применение программы tripwire, отслеживающей изменения в системных файлах.

Статья [17] описывает такой способ выявления инсайдера, как проверка лояльности сотрудников на полиграфе. Также предлагается дополнительный способ обнаружения для повышения эффективности проверки – программное распознавание физиогномических особенностей или, иными словами, анализ микровыражений человека.

В исследовании [18] предлагается такой способ выявления инсайдеров, как комплексная лингвистическая оценка опасности попадания анализируемого человека в «инсайдеры». Сюда входит сбор и анализ информации о личной жизни и проблемах сотрудника, о прошлой работе, составление психологического портрета и анализ особенностей поведения.

В статье [19] в качестве способа обнаружения инсайдера рассматривается система UBA, которая производит анализ поведения пользователя и выявляет потенциального нарушителя. Также описываются методы поиска поведенческих аномалий на основе пространственной кластеризации.

Исследователи в сборнике статей по итогам конференции [20] в качестве одного из способов поиска инсайдера рассматривается система поведенческого поведения UEBA, которая решает огромный список задач, связанных с ИБ-аналитикой – она способна анализировать большой поток данных обо всех действиях пользователей и идентифицировать угрозы. Однако данное решение на данный момент применимо лишь в комплексе с другими методами.

Работа [21] описывает подход к выявлению внутренних нарушителей на основе анализа различных показателей рисков. Различают такие показатели инсайдера, как психологические (черты характера, состояние), личностные (наличие зависимостей, семейное положение, заболевания), контекстные (факты биографии), скрининговые и технические (исследование на наличие аномального поведения и деятельности).

В [22] приводится метод выявления инсайдера с помощью анализа сотрудников по определенным группам показателей. К ним относят стационарные (психологические и коммуникативные показатели), периодические (личностные показатели, поведенческие, скрининговые или данные полиграфа и контекстные показатели), а также динамические, в состав которых входят данные о деятельности пользователя от различных систем комплексного обеспечения информационной безопасности (DLP, SIEM, IDS и т.п.).

Ученые в [23] рассматривают такие способы обнаружения инсайдеров, как мониторинг и контроль распространения данных по сети с помощью DLP-систем, а также выявление поведенческих аномалий. В работе указываются проблем применения различных решений для обеспечения информационной безопасности.

Работа [24] описывает реализацию метода идентификации сотрудников на основе клавиатурной подписи. Данный метод основан на том, что у пользователя вырабатывается индивидуальный устойчивый навык набора идентификационных данных, что может служить дополнительным биометрическим показателем. Применение данного метода позволяет повысить эффективность обнаружения инсайдера еще до совершения киберпреступления.

В статье [25] приводится способ выявления инсайдера статистическими методами. Приводится математическая модель поиска инсайдера на основе факта регулярного сбора избыточной информации нарушителем. Данная модель позволяет его обнаружить за конечное число шагов.

Результаты исследований [26] содержат описание проекта информационной системы, способной обнаружить потенциального внутреннего

нарушителя путем тестирования сотрудников. Анализируются качества личности потенциального инсайдера, производится подбор психодиагностических тестов и порядок обработки результатов тестирования.

Работа [27] рассматривает следующие методы поиска инсайдеров: организационные (анализ психологических типов работников, оценка благонадежности кандидатов) и технические (контроль трафика и активности сотрудников с помощью SIEM-систем, использование DLP-систем для перехвата информации, Honeypot-системы для привлечения инсайдера).

В [28] описывается метод выявления инсайдеров на основе показателей личностной предиспозиции к подобному виду деятельности. Рассмотрены частные показатели личности внутреннего нарушителя. Приведен пример опроса для оценки сотрудников.

Материалы научной конференции [29] рассматривают подход к выявлению инсайдера на основе различных показателей, к которым относятся следующие: данные об аутентификации, сетевая активность, факт получения доступа к ресурсам и печать документов, скачиваемая информация, поисковые запросы и использование браузера. Производится оценка рисков инсайдерской деятельности с учетом профессиональных и личностных качеств работника, а также текущего уровня мотивации.

Способ выявления инсайдеров, такой, как мониторинг и анализ телефонных переговоров, приводится в [30]. Наглядно демонстрируется применение контрольных звонков для проверки сотрудников на предрасположенность к нарушениям. Также описана система «Словоискатель», позволяющая выявить в аудиозаписях телефонных разговоров факт разглашения конфиденциальных данных.

В [31] описываются принципы работы систем Skype и ICQ, а также основные методы обнаружения инсайдерской деятельности в этих системах. К таким методам относится применение программ tripwire, систем обнаружения поведенческих аномалий, средств обнаружения утечек данных и SIEM, а также, анализ психологического состояния сотрудников в течение рабочего сеанса.

Признаки инсайдеров

Анализ публикаций позволяет синтезировать следующие признаки инсайдеров, используемые способами их обнаружения (номер перед признаком будем считать его идентификатором):

1) жадность – реагирование инсайдера на так называемые «муляж» или «живца» в виде визуально полезного ресурса, не имеющего реальной ценности (HoneyPot, HoneyNet, HoneyToken);

2) биография – события из истории жизни сотрудника для предсказания его злонамеренных действий;

3) психология – аспекты человека, как некоторого субъекта, способного к злонамеренным действиям;

4) личность – аспекты сотрудника, косвенно связанные их его потенциальными инсайдерскими действиями, такие, как семейное состояние, заболевания, финансовые потребности и т.п.;

5) коммутация – социальные связи между сотрудниками (общительность, коммуникацию и пр.), позволяющие ему совершать информационные нарушения;

6) предиспозиционность – предрасположенность сотрудника к информационным преступлениям;

7) профессиональность (рабочая) – собственные способности сотрудника к нарушениям внутри организации (уровень подготовки, осведомленность, опыт в работе системами безопасности и т.п.);

8) аномальность поведения – поведение сотрудника, качественно отличающееся от типового;

9) распространение информации – факт передачи конфиденциальной информации по каналам связи;

10)изменения файлов – критические изменениях в файлах, потенциально связанные их с инсайдерской деятельностью;

11)сбор информации (избыточной) – превышение количества и качества собираемой

сотрудником вне должностных обязанностей информации некоторого критического предела;

12) телефонные переговоры – факты разглашение конфиденциальной информации в процессе телефонных переговоров (как внутри компании, так и при общении с лицами вне ее);

13) лояльность – результаты тестирования на полиграфе касательно верности сотрудника компании, ее целям, правилам и т.п.;

14) физигномичность – результаты анализа микровыражений человека, связанные с возможностью осуществления инсайдерской деятельности;

15) нелегальные действия – действия сотрудника, которые изначально считаются нарушениями (например, попытка подбора пароля).

Для обоснования полученного списка приведем участие составляющих его признаков инсайдеров к каждому из рассмотренных в публикациях способу (см. Таблица 1). Используются следующие обозначения: «+» – непосредственное использование признака в способе (1 балл); «+/–» – потенциальная возможность использования признака (0.5 балла); «∑» (последняя строка) – суммирование баллов; столбец «№» содержит ссылку на соответствующую публикацию.

Таблица 1 – Участие признаков инсайдера в способах на основе анализа научных публикаций

№	Идентификатор признака														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
[9]	+					+/–		+		+	+/–		+/–		+/–
[12]								+						+/–	+/–
[13]			+					+			+				
[14]	+							+/–	+	+/–		+			+/–
[16]	+							+	+	+					+/–
[17]													+	+	
[18]		+/–	+			+/–		+/–							
[19]								+							+/–
[20]								+/–	+/–	+/–					+/–
[21]		+	+	+				+	+/–	+/–					
[22]			+	+	+			+/–	+/–	+/–			+		
[23]								+	+						
[24]								+/–							+
[25]											+				
[26]			+	+											
[27]	+		+					+/–	+	+/–					+/–
[28]				+/–		+									
[29]				+			+	+/–	+/–		+/–				+
[30]					+/–	+			+/–			+			
[31]			+		+/–				+	+		+/–			
∑	4	1.5	7	4.5	2	3	1	10.5	7.5	5.5	3	2.5	2.5	1.5	5.5

Анализ систематизированных признаков инсайдеров по способам из обзора исследований (см. Таблица 1) позволяет сделать следующие выводы:

Во-первых, наиболее используемым признаком (как непосредственно, так и потенциально) являются аномалии в поведении (10.5 баллов), за которым идет распространение конфиденциальной информации (7.5 балла) и модификация критических файлов (5.5 балла).

Во-вторых, наиболее редкими признаками с этой позиции являются учет профессиональных способностей сотрудников совершить нарушение (1 балл), а также биография и физигномичность (по 1.5 балла).

И, в-третьих, ни один из способов не учитывает более половины всех признаков, поскольку их наибольшее используемое количество равно 7 из 15 (для [9] и [22]).

Также необходимо отметить, что наблюдается тенденция применения методов машинного обучения для решения поставленной задачи (аномализация, классификация, кластеризация [32]), что, безусловно, приносит свои плоды для обеспечения информационной безопасности организаций.

Заключение

Анализ и обзор 20 научных исследований на тему способов выявления инсайдеров позволил выделить и систематизировать 15 признаков, используемых данными способами. Таким образом, признаки могут считаться некоторым базисом моделей, на которых строятся все существующие (или, по крайней мере, отраженные в публикациях) способы. Логичным развитием направления по выявлению инсайдеров в организациях должно стать создание новых способов, учитывающих (совместно, а не по отдельности) указанное многообразие признаков, повышая тем самым итоговую эффективность. Естественно, учет всех признаков в едином способе является технически труднодостижимой задачей, тем не менее это может считаться некоторым идеалом, само по себе стремление к которому позволит сделать качественный скачок на пути противодействия инсайдерству.

Список литературы

1. *Буйневич М.В., Васильева И.Н., Воробьев Т.М., Гниденко И.Г., Егорова И.В., Еникеева Л.А и др.* Защита информации в компьютерных системах: монография. – СПб.: СПГЭУ, 2017. – 163 с. – ISBN 978-5-7310-4070-9. – EDN YLGBGO.

2. *Уткин О.В., Власов Д.С., Ильин А.В., Ефременков Е.Ю.* Методика оценки деятельности должностного лица ЦУКС МЧС России // Подготовка кадров в системе предупреждения и ликвидации последствий чрезвычайных ситуаций: материалы международной научно-практической конференции, Санкт-Петербург, 1 июня 2017 года. – СПб.: Санкт-Петербургский университет ГПС МЧС России, 2017. – С. 227–228. – EDN XXYGLJ.

3. *Власов Д.С.* Задачи построения системы обеспечения информационной безопасности типового объекта МЧС России // Актуальные проблемы инфотелекоммуникаций в науке и образовании: Сборник научных статей V международной научно-технической и научно-методической конференции, Санкт-Петербург, 10–11 марта 2016 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – С. 281-285. – EDN WZILPD.

4. *Израилов К.Е.* Анализ состояния в области безопасности программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании: II Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 27–28 февраля 2013 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2013. – С. 874-877. – EDN SMCVQZ.

5. *Буйневич М.В., Щербаков О.В., Владыко А.Г., Израилов К.Е.* Архитектурные уязвимости моделей телекоммуникационных сетей // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2015. – № 4. – С. 86-93. – EDN VHNSTB.

6. *Mescheryakov S., Shchemelinin D., Izrailov K., Pokussov V.* Digital cloud environment: present

challenges and future forecast // Future Internet. – 2020. – Vol. 12, No. 5. – P. 82. – DOI 10.3390/FI12050082. – EDN HSNQNI.

7. *Буйневич М.В., Израилов К.Е.* Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. – 2016. – Т. 4, № 3. – С. 95-106. – EDN XXDTSN.

8. *Буйневич М.В., Власов Д.С.* Сравнительный обзор способов выявления инсайдеров в информационных системах // Информатизация и связь. – 2019. – № 2. – С. 83-91. – DOI 10.34219/2078-8320-2019-10-2-83-91. – EDN GCIDKY.

9. *Пименов А.П., Бутиков З.Э.* Анализ методов и алгоритмов поиска инсайдеров в компьютерной сети // Моделирование и анализ сложных технических и технологических систем: сборник статей Международной научно-практической конференции, Магнитогорск, 01 декабря 2018 года. – Магнитогорск: Общество с ограниченной ответственностью «Аэтерна», 2018. – С. 15-19. – EDN YQQIGL.

10. *Буйневич М.В., Израилов К.Е.* Обобщенная модель статического анализа программного кода на базе машинного обучения применительно к задаче поиска уязвимостей // Информатизация и связь. – 2020. – № 2. – С. 143-152. – DOI 10.34219/2078-8320-2020-11-2-143-152. – EDN ISHFGR.

11. *Буйневич М.В., Израилов К.Е.* Аналитическое моделирование работы программного кода с уязвимостями // Вопросы кибербезопасности. – 2020. – № 3(37). – С. 2-12. – DOI 10.21681/2311-3456-2020-03-02-12. – EDN CQFGPI.

12. *Королева Е.В., Жарова О.Ю.* Применение технологии распознавания лиц для предотвращения инсайдерских атак // Электронный журнал: наука, техника и образование. – 2019. – № 4(27). – С. 58-63. – EDN WFCLDK.

13. *Терёшкин М.В.* Борьба с внутренними угрозами. Выявление инсайдера в банке // Теоретические и прикладные вопросы комплексной безопасности: материалы I Международной научно-практической конференции, Санкт-Петербург, 28 марта 2018 года. – СПб: Петровская академия наук и искусств, 2018. – С. 198-200. – EDN XNKPVJ.

14. *Хлестова Д.Р., Попов К.Г.* Средства поиска инсайдеров // Актуальные проблемы социального, экономического и информационного развития современного общества: Всероссийская научно-практическая конференция, посвящённая 100-летию со дня рождения первого ректора Башкирского государственного университета Чанбарисова Шайхуллы Хабибулловича, Уфа, 20 мая 2016 года / Башкирский государственный университет. Том Часть 2. – Уфа: Общество с ограниченной ответственностью «Аэтерна», 2016. – С. 169-172. – EDN WLHVGH.

15. *Spafford E.* Tripwire: Pioneering Integrity Scanning for Cybersecurity // In proceedings of Annual Computer Security Applications Conference, 5–9 December 2022, Austin, Texas. 2022. URL: https://api.semanticscholar.org/CorpusID:254520122.

16. *Веденеев В.С., Бычков И.В.* Средства поиска инсайдеров в корпоративных информационных системах // Безопасность информационных технологий. – 2014. – Т. 21, № 1. – С. 9-13. – EDN TOLNST.

17. *Кудрявцев Д.А., Кузнецов М.В., Светличная М.А.* Разработка модуля распознавания микровыражений «Face Mode» для повышения достоверности выявления инсайдера // Инфокоммуникационные технологии. – 2013. – Т. 11, № 2. – С. 87-90. – EDN RVMIVZ.

18. *Снегуров А.В., Кравченко А.Д., Ткаченко Е.А.* Подход к повышению эффективности выявления инсайдеров при обеспечении информационной безопасности организации // Восточно-Европейский журнал передовых технологий. – 2011. – Т. 2, № 9(50). – С. 17-20. – EDN OMSNQW.

19. *Савенков П.А., Трегубов П.С.* Поиск поведенческих аномалий в деятельности сотрудников при помощи методов пространственной кластеризации, основанных на плотности // Известия Тульского государственного университета. Технические науки. – 2020. – № 9. – С. 250-259. – EDN AFTSKZ.

20. *Пузанков А.М.* Системы поведенческого анализа (User and Entity Behavior Analytics, UEBA)

// Общетеоретические и отраслевые проблемы науки и пути их решения: Сборник статей по итогам Международной научно-практической конференции, Волгоград, 28 мая 2019 года. Том 1. – Волгоград: Агентство международных исследований, 2019. – С. 70-73. – EDN ARKZPE.

21. *Поляничко М.А.* Выявление инсайдерских угроз в транспортных организациях // Интеллектуальные технологии на транспорте. – 2018. – № 3(15). – С. 33-37. – EDN YRMQPJ.

22. *Корниенко А.А., Поляничко М.А.* Метод обнаружения инсайдерской деятельности в организации // Программные системы и вычислительные методы. – 2019. – № 1. – С. 30-41. – DOI 10.7256/2454-0714.2019.1.29048. – EDN ZUPYEX.

23. *Поляничко М.А., Пунанова К.В.* Основные проблемы практического применения человеко-ориентированного подхода к обеспечению информационной безопасности // Фундаментальные и прикладные разработки в области технических и физико-математических наук: сборник научных статей по итогам работы третьего международного круглого стола, Казань, 31 июля 2018 года. – Казань: Общество с ограниченной ответственностью «КОНВЕРТ», 2018. – С. 57-60. – EDN UVBLME.

24. *Вепрев С.Б., Гончаров П.И.* Скрытый метод выявления утечек инсайдерской информации // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2014. – № 4. – С. 152-155. – EDN TNUGXX.

25. *Мартьянов Е.А.* Возможность выявления инсайдера статистическими методами // Системы и средства информатики. – 2017. – Т. 27, № 2. – С. 41-47. – DOI 10.14357/08696527170204. – EDN YPJBAZ.

26. *Белов С.В., Садыкова У.В.* Разработка информационной системы выявления потенциальных нарушителей информационной безопасности на основе психодиагностических методик // Электронный сетевой политематический журнал «Научные труды КубГТУ». – 2018. – № 3. – С. 106-115. – EDN OSWTTH.

27. *Кабанов А.С., Лось А.Б.* Причины, профилактика и методы противодействия инсайдерской деятельности // Безопасность бизнеса. – 2016. – № 3. – С. 28-35. – EDN WFVZAL.

28. *Поляничко М.А.* Показатели личностной предиспозиции к инсайдерской деятельности // Международный научно-исследовательский журнал. – 2018. – № 10-1(76). – С. 43-46. – DOI 10.23670/IRJ.2018.76.10.008. – EDN YLRSUP.

29. *Поляничко М.А.* Подход к оценке рисков информационной безопасности на основе определения актуальности инсайдерских угроз // Региональная информатика и информационная безопасность : Сборник трудов, Санкт-Петербург, 23–25 октября 2019 года. Том Выпуск 7. – СПб: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2019. – С. 111-114. – EDN QZPYWQ.

30. *Гаранин Н.Б.* Выявление инсайдеров в системе обеспечения информационной безопасности предприятия // Ресурсам области - эффективное использование: XV Ежегодная научная конференция студентов Финансово-технологической академии: Сборник материалов, Королёв, 22 апреля 2015 года. Том Часть 1. – Королёв: Общество с ограниченной ответственностью «Научный консультант», 2015. – С. 59-64. – EDN TZNQAL.

31. *Пескова О.Ю., Тимкова О.Ю., Тимков А.Е.* Программы мгновенного обмена сообщениями и инсайдерские атаки // Информационное противодействие угрозам терроризма. – 2014. – № 23. – С. 132-142. – EDN THAWVZ.

32. *Kotenko I., Izrailov K., Buinevich M.* Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. – 2022. – Vol. 22, No. 4. – DOI 10.3390/s22041335. – EDN XEOLHD.

References

1. *Buinevich M. V., Vasilyeva I. N., Vorobyov T. M., Gnidenko I. G., Egorova I. V., Enikeeva L. A, etc.* Information protection in computer systems: monograph. – St. Petersburg: SPGEU, 2017. – 163 p. – ISBN 978-5-7310-4070-9. – EDN YLGBGO.

2. *Utkin O.V., Vlasov D.S., Ilyin A.V., Efremenkov E.Yu.* Methodology for assessing the activities of an

official of the Central Control Center of the Ministry of Emergency Situations of Russia // Personnel training in the system of warning and liquidation of consequences of emergency situations: materials of international scientific- practical conference, St. Petersburg, June 1, 2017. – St. Petersburg: St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia, 2017. – pp. 227–228. – EDN XXYGLJ.

3. *Vlasov D.S.* Tasks of building a system for ensuring information security of a standard object of the Ministry of Emergency Situations of Russia // Current problems of information telecommunications in science and education: Collection of scientific articles of the V international scientific-technical and scientific-methodological conference, St. Petersburg, March 10–11, 2016 of the year. Volume 1. – St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2016. – pp. 281-285. – EDN WZILPD.

4. *Izrailov K.E.* Analysis of the state of affairs in the field of software security // Current problems of information telecommunications in science and education: II International Scientific, Technical and Scientific Methodological Conference, St. Petersburg, February 27–28, 2013. – St. Petersburg: St. Petersburg State University of Telecommunications named after. prof. M.A. Bonch-Bruevich, 2013. – pp. 874-877. – EDN SMCVQZ.

5. *Buinevich M.V., Shcherbakov O.V., Vladyko A.G., Izrailov K.E.* Architectural vulnerabilities of telecommunication network models // Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". – 2015. – No. 4. – P. 86-93. – EDN VHNSTB.

6. *Mescheryakov S., Shchemelinin D., Izrailov K., Pokussov V.* Digital cloud environment: present challenges and future forecast // Future Internet. – 2020. – Vol. 12, No. 5. – P. 82. – DOI 10.3390/FI12050082. – EDN HSNQNI.

7. *Buinevich M.V., Izrailov K.E.* Categorical synthesis and technological analysis of options for safe import substitution of software for telecommunication devices // Information technologies and telecommunications. – 2016. – T. 4, No. 3. – P. 95-106. – EDN XXDTSN.

8. *Buinevich M.V., Vlasov D.S.* Comparative review of methods for identifying insiders in information systems // Informatization and Communication. – 2019. – No. 2. – P. 83-91. – DOI 10.34219/2078-8320-2019-10-2-83-91. – EDN GCIDKY.

9. *Pimenov A.P., Butikov Z.E.* Analysis of methods and algorithms for searching for insiders in a computer network // Modeling and analysis of complex technical and technological systems: collection of articles of the International Scientific and Practical Conference, Magnitogorsk, December 01, 2018. – Magnitogorsk: Limited Liability Company "Aeterna", 2018. – pp. 15-19. – EDN YQQIGL.

10. *Buinevich M.V., Izrailov K.E.* A generalized model of static analysis of program code based on machine learning in relation to the problem of searching for vulnerabilities // Informatization and Communication. – 2020. – No. 2. – P. 143-152. – DOI 10.34219/2078-8320-2020-11-2-143-152. – EDN ISHFGR.

11. *Buinevich M.V., Izrailov K.E.* Analytical modeling of the operation of program code with vulnerabilities // Issues of cybersecurity. – 2020. – No. 3(37). – P. 2-12. – DOI 10.21681/2311-3456-2020-03-02-12. – EDN CQFGPI.

12. *Koroleva E.V., Zharova O.Yu.* Application of facial recognition technology to prevent insider attacks // Electronic journal: science, technology and education. – 2019. – No. 4(27). – pp. 58-63. – EDN WFCLDK.

13. *Tereshkin M.V.* Combating internal threats. identifying an insider in a bank // Theoretical and applied issues of integrated security: materials of the I International Scientific and Practical Conference, St. Petersburg, March 28, 2018. – St. Petersburg: Petrovskaya Academy of Sciences and Arts, 2018. – P. 198-200. – EDN XNKPVJ.

14. *Khlestova D.R., Popov K.G.* Tools for searching for insiders // Current problems of social, economic and information development of modern society: All-Russian scientific and practical conference dedicated to the 100th anniversary of the birth of the first rector

of the Bashkir State University Chanbarisov Shaikhulla Khabibullovich , Ufa, May 20, 2016 / Bashkir State University. Volume Part 2. - Ufa: Limited Liability Company "Aeterna", 2016. - P. 169-172. – EDN WLHVGH.

15. *Spafford E.* Tripwire: Pioneering Integrity Scanning for Cybersecurity // In proceedings of Annual Computer Security Applications Conference, 5–9 December 2022, Austin, Texas. 2022. URL: https://api.semanticscholar.org/CorpusID:254520122. Vedeneyev V. S., Bychkov I. V. Sredstva poiska insayderov v korporativnykh informatsi-onnykh sistemakh // Bezopasnost' informatsionnykh tekhnologiy. 2014. T. 21. № 1. S. 9–13.

16. *Vedeneev V.S., Bychkov I.V.* Tools for searching for insiders in corporate information systems // Security of information technologies. – 2014. – T. 21, No. 1. – P. 9-13. – EDN TOLNST.

17. *Kudryavtsev D.A., Kuznetsov M.V., Svetlichnaya M.A.* Development of a micro-expression recognition module "Face Mode" to increase the reliability of identifying an insider // Infocommunication technologies. – 2013. – T. 11, No. 2. – P. 87-90. – EDN RVMIVZ.

18. *Snegurov A.V., Kravchenko A.D., Tkachenko E.A.* An approach to increasing the efficiency of identifying insiders while ensuring the information security of an organization // East European Journal of Advanced Technologies. – 2011. – T. 2, No. 9(50). – pp. 17-20. – EDN OMSNQW.

19. *Savenkov P.A., Tregubov P.S.* Search for behavioral anomalies in the activities of employees using spatial clustering methods based on density // News of Tula State University. Technical science. – 2020. – No. 9. – P. 250-259. – EDN AFTSKZ.

20. *Puzankov A. M.* Systems of behavioral analysis (User and Entity Behavior Analytics, UEBA) // General theoretical and sectoral problems of science and ways to solve them: Collection of articles based on the results of the International Scientific and Practical Conference, Volgograd, May 28, 2019. Volume 1. – Volgograd: Agency for International Research, 2019. – pp. 70-73. – EDN ARKZPE.

21. *Polyanichko M.A.* Identification of insider threats in transport organizations // Intelligent technologies in transport. – 2018. – No. 3(15). – pp. 33-37. – EDN YRMQPJ.

22. *Kornienko A.A., Polyanichko M.A.* Method for detecting insider activity in an organization // Program systems and computational methods. – 2019. – No. 1. – P. 30-41. – DOI 10.7256/2454-0714.2019.1.29048. – EDN ZUPYEX.

23. *Polyanichko M.A., Punanova K.V.* Main problems of practical application of a human-oriented approach to ensuring information security // Fundamental and applied developments in the field of technical and physical and mathematical sciences: a collection of scientific articles based on the results of the third international round table , Kazan, July 31, 2018. – Kazan: Limited Liability Company "CONVERT", 2018. – pp. 57-60. – EDN UVBLME. Mart'yanov Ye. A. Vozmozhnost' vyyavleniya insaydera statisticheskimi metodami // Si-stemy i sredstva informatiki. 2017. T. 27. № 2. S. 41–47.

24. *Veprev S.B., Goncharov P.I.* Hidden method for identifying leaks of insider information // Bulletin of the Russian New University. Series: Complex systems: models, analysis and control. – 2014. – No. 4. – P. 152-155. – EDN TNUGXX.

25. *Martyanov E.A.* Possibility of identifying an insider using statistical methods // Systems and means of informatics. – 2017. – T. 27, No. 2. – P. 41-47. – DOI 10.14357/08696527170204. – EDN YPJBAZ.

26. *Belov S.V., Sadykova U.V.* Development of an information system for identifying potential violators of information security based on psychodiagnostic techniques // Electronic network polythematic journal "Scientific works of KubSTU". – 2018. – No. 3. – P. 106-115. – EDN OSWTTH.

27. *Kabanov A.S., Los A.B.* Reasons, prevention and methods of counteracting insider activity // Business Security. – 2016. – No. 3. – P. 28-35. – EDN WFVZAL.

28. *Polyanichko M.A.* Indicators of personal predisposition to insider activity // International scientific research journal. – 2018. – No. 10-1(76). – pp. 43-46. – DOI 10.23670/IRJ.2018.76.10.008. – EDN YLRSUP.

Polyanichko M.A. An approach to assessing information security risks based on determining

the relevance of insider threats // Regional informatics and information security: Collection of proceedings, St. Petersburg, October 23–25, 2019. Volume Issue 7. – St. Petersburg: Regional public organization "St. Petersburg Society of Informatics, Computer Science, Communication and Control Systems", 2019. – P. 111-114. – EDN QZPYWQ.

29. *Garanin N.B.* Identification of insiders in the system of ensuring information security of an enterprise // Regional resources - effective use: XV Annual Scientific Conference of Students of the Financial and Technology Academy: Collection of materials, Korolev, April 22, 2015. Volume Part 1. - Korolev: Limited Liability Company "Scientific Consultant", 2015. - P. 59-64. – EDN TZNQAL.

30. *Peskova O.Yu., Timkova O.Yu., Timkov A.E.* Instant messaging programs and insider attacks // Information counteraction to terrorist threats. – 2014. – No. 23. – P. 132-142. – EDN THAWVZ.

31. *Kotenko I., Izrailov K., Buinevich M.* Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. – 2022. – Vol. 22, No. 4. – DOI 10.3390/s22041335. – EDN XEOLHD.

Статья поступила в редакцию 25 сентября 2023 г.
Принята к публикации 12 декабря 2023 г.

Ссылка для цитирования: Власов Д.С. К вопросу о признаках инсайдерской деятельности // Национальная безопасность и стратегическое планирование. 2024. № 1(45). С. 35-45. DOI: https://doi.org/10.37468/2307-1400-2024-1-35-45

For citation: Vlasov D.S. On the question of signs of insider activity // National security and strategic planning. 2024. № 1(45). pp. 35-45. DOI: https://doi.org/10.37468/2307-1400-2024-1-35-45

Сведения об авторах:

ВЛАСОВ ДМИТРИЙ СЕРГЕЕВИЧ – *начальник управления информационных технологий и связи Главного управления МЧС России по г. Санкт-Петербургу, г. Санкт-Петербург, Россия*
ORCID: http://orcid.org/0000-0003-2332-8431
SPIN-код: 2739-2000
e-mail: prikerx@bk.ru

Information about authors:

VLASOV DMITRY S. – *Head of Information Technology and Communications Department EMERCOM of Russia Main Directorate in the St. Petersburg city, St. Petersburg, Russia*
ORCID: http://orcid.org/0000-0003-2332-8431
SPIN-код: 2739-2000
e-mail: prikerx@bk.ru