ТРУДЫ МОЛОДЫХ УЧЕНЫХ

Обзорная статья
УДК 004.056; DOI: 10.61260/2218-13X-2024-2-136-145

СРАВНИТЕЛЬНЫЙ ОБЗОР РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ РОССИЙСКИХ УЧЕНЫХ ПО ВЫЯВЛЕНИЮ ИНСАЙДЕРОВ В ОРГАНИЗАЦИЯХ

✉**Власов Дмитрий Сергеевич.**
Главное управление МЧС России по г. Санкт-Петербургу, Санкт-Петербург, Россия
✉***prikerx@bk.ru***

Аннотация. Работа посвящена задаче обнаружения инсайдеров в организации, повышая тем самым информационную безопасность ее ресурсов. Для этого проведен обзор результатов интеллектуальной деятельности (свидетельств о государственной регистрации программ и баз данных, патентов на полезные модели) российских ученых в РИНЦ по ключевым словам – «инсайдер» (7 публикаций) и «инсайдерский» (10 публикаций). Все найденные решения систематизированы в табличном виде по таким критериям, как год публикации, тип, язык программирования, международная патентная классификация и область применения. Сделан ряд следующих основополагающих выводов: востребованность в практических решениях, небольшой повышающийся тренд актуальности задачи, предпочтительность использования языков программирования «C++» и «C#», патентование в основном решений для сигнализации о кражах, основное применение в области оценивания личностных и поведенческих характеристик сотрудников.

Ключевые слова: информационная безопасность, инсайдер, обнаружение, обзор, интеллектуальная деятельность, систематизация

Для цитирования: Власов Д.С. Сравнительный обзор результатов интеллектуальной деятельности российских ученых по выявлению инсайдеров в организациях // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 136–145. DOI: 10.61260/2218-13X-2024-2-136-145.

Review article

COMPARATIVE REVIEW OF RESULTS INTELLECTUAL ACTIVITY OF RUSSIAN SCIENTISTS ON IDENTIFYING INSIDERS IN ORGANIZATIONS

✉**Vlasov Dmitry S.**
Main directorate of EMERCOM of Russia for Saint-Petersburg, Saint-Petersburg, Russia
✉***prikerx@bk.ru***

Abstract. The work is devoted to the task of detecting insiders in an organization, thereby increasing the information security of its resources. To do this, a review of the results of intellectual activity (certificates of state registration of programs and databases, patents for utility models) of Russian scientists in the Russian science citation indexwas carried out using the keywords «insider (as noun)» (7 publications) and «insider (as adjective)» (10 publications). All solutions found are systematized in tabular form according to criteria such as year of publication, type, programming language, international patent classification and scope. A number of the following fundamental conclusions have been made: demand for practical solutions, a slight increasing trend in the relevance of the problem, the preference for using the programming languages «C++» and «C#»,

© Санкт-Петербургский университет ГПС МЧС России, 2024

patenting mainly solutions for theft alarms, the main application in the field of assessing the personal and behavioral characteristics of employees.

Keywords: information security, insider, detection, review, intellectual activity, systematization

For citation: Vlasov D.S. Comparative review of results intellectual activity of russian scientists on identifying insiders in organizations // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 2. P. 136–145. DOI: 10.61260/2218-13X-2024-2-136-145.

Введение

Защита информационных ресурсов в любой организации является одной из первоочередных задач обеспечения ее безопасного и непрерывного функционирования. Помимо внешних угроз такого функционирования существуют и внутренние, исходящие непосредственно от сотрудников, которые в данном случае являются инсайдерами [1]. Так, последние, пользуясь своими должностными обязанностями, могут совершать неправомерные действия, такие как хищение коммерческой информации, ее модификация в собственных интересах или даже уничтожение из мести работодателю [2]. Сложность выявления такого рода нарушителей, в том числе, заключается в их слабо прогнозируемом поведении, близком к легальным сотрудникам [3]. Помимо научной стороны задачи обнаружения инсайдеров присутствует и практическая составляющая, заключающаяся в возможности доведения решений до практических работоспособных результатов [4]. Так, создание теоретических моделей и методов, которые не могут быть доведены до практики, имеет мало смысла в «боевых условиях». Именно в интересах практики далее будет произведен обзор результатов интеллектуальной деятельности (РИД) российских ученых по решению задачи обнаружения инсайдера – что является основной задачей текущего исследования (Задача).

Обзор работ

Произведём обзор работ с РИД российских ученых, ограничившись их содержанием в виде изобретений, патентов и свидетельств о государственной регистрации программ для ЭВМ, размещенных в РИНЦ. В качестве ключевого запроса для поиска использовалось слово «инсайдер», что позволило получить 13 публикаций, следующие семь из которых непосредственно относились к Задаче (в остальных шести подразумевались иные применения термина, например, для биржевой торговли); в конце каждого обзора будет указан используемый язык программирования или Международный патентный классификатор.

В работе [5] реализуется обнаружение инсайдеров в компьютерной сети, используемой множеством сотрудников организации. Для этого производится анализ сетевого трафика и его обработка методами машинного обучения – k-ближайших соседей и дерева решений. На входе программа принимает дамп сетевого трафика, а на выходе возвращает категории участников сети, а также визуализацию полученных кластеров. Программа [6] тех же авторов (точнее двух из них) решает подобную задачу, однако в процессе этого данные загружаются в базу данных OrientDB; также вместо машинного обучения применяются правила выявления инсайдеров, заданные экспертами вручную. Результат в работе [7] также является продолжением работы авторов путем применения кластера Apache Hadoop для распределенной обработки больших объемов данных. Язык программирования: Python.

Решение в работе [8] состоит из программной надстройки для «1С-Битрикс», а также агентов для персональных компьютеров и смартфонов. Решение предназначено для учета деятельности сотрудников организации с целью контроля за их работой; так, например, программа учитывает рабочую деятельность, делает скриншоты экрана, определяет некоторые нарушения трудового регламента и т.п. Основным назначением, помимо

управления эффективностью работы сотрудников со стороны руководителя, является повышение информационной безопасности в организации и расследование происходящих инцидентов. Программа в работе [9] того же автора обладает схожим функционалом (за исключением применения «1С-Битрикс») и, скорее всего, является развитием продукта. Языки программирования: PHP, JavaScript, Java, C++.

Назначением в работе [10] является имитация атак со стороны инсайдера, проводимая во внутренней сети организации. В качестве основного предназначения указан внутренний аудит информационной безопасности. Получаемые в итоге результаты подвергаются экспертному анализу. Язык программирования: Borland C++ Builder 6 Enterprise.

Полезная модель в работе [11] описывает средство регистрации (то есть устройство), предназначенное для скрытого контроля доступа в некоторую зону или к некоторому объекту, тем самым обнаруживая потенциально инсайдерскую деятельность в организации. Особенностью решения является схожесть средства с типовым бытовым изделием (ТБИ), скрывая тем самым его от злоумышленника. Международная патентная классификация: «G08B 13/00 – Сигнализация о краже, взломе и т.п.», «G11C 7/00 – Устройства для записи или считывания информации в цифровых запоминающих устройствах».

Исходя из достаточно малого количества качественно разных результатов, представленных в обзорах выше, поиск был продолжен с использованием ключевого слова «инсайдерский», что позволило дополнительно получить 20 публикаций, следующие 10 из которых непосредственно относились к Задаче.

Полезная модель в работе [12] описывает автоматизированное рабочее место (АРМ) для контроля за деятельностью сотрудников, что поможет выявить среди них инсайдеров. Для этого, в частности, предлагается сравнивать рабочие показатели сотрудников с шаблонными, при этом предоставляя гибкие возможности управления процессом. Международная патентная классификация: «G06Q 10/10 – Администрирование; менеджмент / офисная автоматизация, например, компьютерное управление электронной почтой или групповое программное обеспечение; управление временем, например, календари, устройства напоминания, учет встреч или времени», «G06F 17/10 – Оборудование или способы обработки данных или цифровых вычислений, специально предназначенные для особых функций / комплексные математические операции».

Программа в работе [13] предназначена для анализа деятельности пользователей информационных систем (от персональных станций и серверов до банкоматов) для выявления атак инсайдеров в сетях соответствующих организациях. Решение имеет клиент-серверную архитектуру и функционал, состоящий из контроля за файловой системой, доступом в интернет, устройствами, а также учет списка пользователей, прав доступа и т.п. Язык программирования: C++, C#.

Программа в работе [14], соавторов которой является автор настоящего исследования, предназначена для выдачи лабораторных работ обучающимся, загрузки их результатов в облачное хранилище на базе Google Drive, предоставления преподавателю возможности проверки выполнения, а также ведение статуса выполнения заданий. Важной функцией системы является возможность автоматической проверки загружаемых файлов с результатами выполнения на наличие вирусов, тем самым препятствуя потенциальным инсайдерским атакам со стороны обучающихся. Язык программирования: JavaScript, Google Script.

Программное решение в работе [15] практически идентично работе [13] по функционалу, хотя и имеет другого правообладателя. Язык программирования: C++, C#.

Два программных модуля в работах [16, 17], а также база данных в работе [18] выполнены в рамках научно-исследовательского проекта РФФИ №14-07-97014 «Разработка методов и моделей предотвращения инсайдерской активности и оценки эффективности работы персонала организации», суть которого заключается в оценке эффективности сотрудников организации, в том числе для выявления инсайдерской деятельности. Все решения входят в состав комплекса «Предотвращения инсайдерской активности и оценки

эффективности работы персонала организации» и имеют следующий функционал: первая программа собирает полную информацию о пользователе, включая его личностные количественные оценки; вторая программа сравнивает деятельность сотрудника с шаблонами, отклонения от которых будут сигнализировать о потенциальном инсайдере; база данных предоставляет анкеты для тестирования и выявления по ним различных особенностей сотрудников (профессиональных, биологических и иных). Язык программирования: C#.

Решение в работе [19] предназначено для выявления компьютерных атак, включая инсайдерские. Для этого предназначен богатый арсенал функционала, такой, как анализ инцидентов на сетевых узлах, определение применения инструментария злоумышленника, поиск по YARA-правилам, сбор и систематизация информации для доказательства нарушений и т.п. Таким образом, в решении совмещается, некоторым образом, как обработка информации от операционных систем (ОС), так и учет сетевой инфраструктуры. Язык программирования: Go, JavaScript.

В работе [20] предлагается снизить угрозу инсайдерской деятельности путем сканирования файлов АРМ на наличие в них персональных данных. Как результат, пользователь на основании полученного отчета сможет «подчистить» свое АРМ перед окончанием сеанса. Язык программирования: C#.

Полезная модель в работе [21], скорее всего, является развитием решения в работе [11], поскольку имеет близкое название, описание и частично тех же авторов. Однако в данной модели дается более четкое выделение двух частей – для имитации (внешне и внутренне) работы ТБИ и регистрации событий (за счет видеомодуля, микрофона, датчиков движения и т.п.). Международная патентная классификация: «G08B 13/00 – Сигнализация о краже, взломе и т.п.».

Сравнительный анализ

Произведем систематизацию всех 17 РИД, представленных в обзорах, в таблице, где введены следующие сокращения: «Название» – название публикации (с указанием ссылки на нее), «Тип» – тип РИД («Прог.» – программа, «Мод.» – полезная модель, «БД» – база данных); «Год» – год регистрации; «ЯП или МПК» – сокр. от «Язык программирования (для программы), Международная патентная классификация (для патента), «---» (для базы данных)»; «Область» – предлагаемая область применения (их расшифровка будет раскрыта далее).

Таблица

Систематизация РИД сделанных обзоров

Название	Тип	Год	ЯП или МПК	Область
Система обнаружения инсайдеров в корпоративной компьютерной сети с использованием технологий машинного обучения [5]	Прог.	2019	Python	Компьютерная сеть
Система обнаружения инсайдера в корпоративной компьютерной сети, используя алгоритмы, основанные на экспертных правилах [6]	Прог.	2019	Python	Компьютерная сеть
Компонент предобработки трафика в корпоративной компьютерной сети с использованием алгоритма Map Reduce в Hadoop кластере [7]	Прог.	2019	Python	Компьютерная сеть
«Инсайдер» – система мониторинга, контроля и комплексной оценки эффективности работы персонала [8]	Прог.	2021	PHP, JavaScript, Java, C++	Человеческие ресурсы

Название	Тип	Год	ЯП или МПК	Область
Insider cloud (инсайдер клауд) – система мониторинга работы сотрудников и автоматизации учета рабочего времени [9]	Прог.	2022	PHP, JavaScript, Java, C++	Человеческие ресурсы
Анализатор защищенности сетевых ресурсов от программно-технических воздействий [10]	Прог.	2014	C++ Builder	Компьютерная сеть
Скрытый регистратор доступа на объект [11]	Мод.	2009	G08B 13/00, G11C 7/00	Аппаратное обеспечение
АРМ для контроля эффективности работы персонала и предотвращения инсайдерских атак [12]	Мод.	2013	G06Q 10/10, G06F 17/10	Человеческие ресурсы
Система SoftControl для зашиты банкоматов, рабочих станций и серверов от вторжений и инсайдерских атак [13]	Прог.	2017	C++, C#	Операционная система
Программа для дистанционного приема лабораторных работ со встроенным модулем противодействия инсайдерской деятельности [14]	Прог.	2021	JavaScript, Google Script	Облачное хранилище
Программный комплекс SafenSoft SysWatch TPSecure для защиты банкоматов, рабочих станций и серверов от вторжений и инсайдерских инцидентов [15]	Прог.	2016	C++, C#	Операционная система
Программный модуль регистрации и ввода личностных характеристик пользователей [16]	Прог.	2015	C#	Человеческие ресурсы
Программный модуль оценки легитимности и эффективности работы пользователя [17]	Прог.	2016	C#	Человеческие ресурсы
Анкетирование пользователя для определения его личностных характеристик [18]	БД	2016	---	Человеческие ресурсы
Scanim Enterprise [19]	Прог.	2021	Go, JavaScript	Информационная система
Приложение для автоматического поиска персональной банковской информации в электронных документах [20]	Прог.	2020	C#	Операционная система
Скрытый регистратор несанкционированного доступа на объект или его локальные зоны [21]	Мод.	2010	G08B 13/00	Аппаратное обеспечение

Анализ систематизации РИД по сделанным обзорам (табл.) позволяет сделать следующие выводы.

Во-первых, из 17 работ в 14 регистрируется программа для ЭВМ, в двух – патент на полезную модель и в одной – база данных. Таким образом, преобладающая часть исследований и разработок доведена до программной реализации, что позволяет говорить о востребованности научной общественности в работоспособных решениях Задачи, готовых для непосредственного применения на практике (даже при учете относительной простоты оформления заявок на регистрацию программ по сравнению с патентами).

Во-вторых, первая регистрация РИД произведена в 2009 г., а последняя – в 2022 г., что гипотетически может говорить об инициализации Задачи только 15 лет назад (на момент написания статьи – в 2024 г.). Гистограмма распределения публикаций по годам представлена на рисунке; пометкой «Статьи с уникальными РИД» показано распределение при отнесении близких РИД к наиболее ранней из них без увеличения количества статей за год, то есть [5–7] к 2019 г.; [8, 9] к 2021 г.; [16–18] к 2015 г.

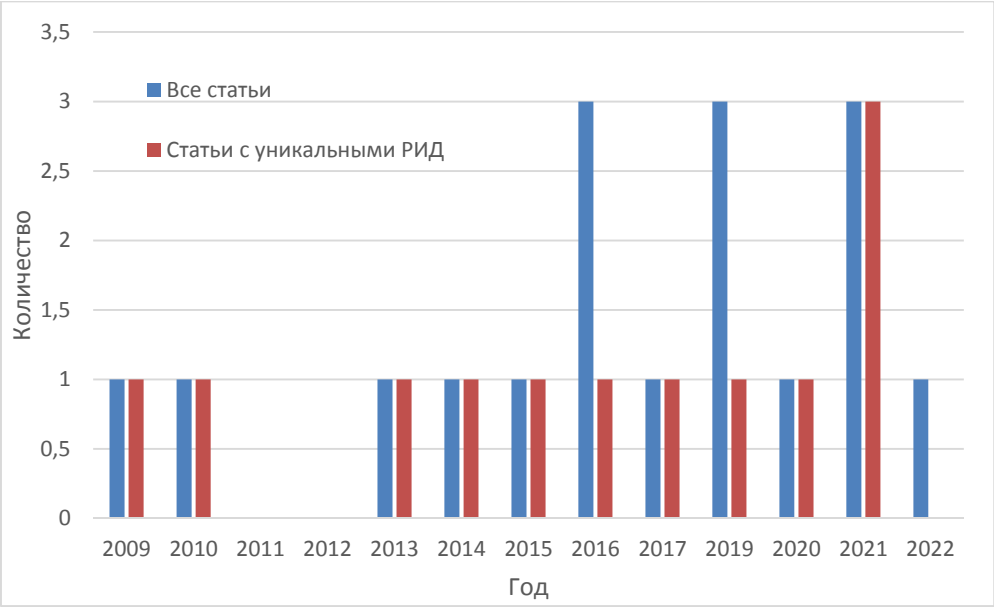

Рис. **Распределение публикаций РИД по годам**

Исходя из распределения публикаций с учетом совмещения «близких» РИД (рис., метка «Количество (общ.)»), можно сделать вывод о достаточно равномерном распределении активности интеллектуальной деятельности, направленной на реализацию решений по обнаружению инсайдеров. Аномальными тут являются лишь года 2011, 2012 и 2022, когда не было найдено ни одной публикации, и 2021 – где их было сразу три. Таким образом, с точки зрения актуализации Задачи и оперативного поиска практических решений (а не только теоретических «размышлений») можно предположить некоторый незначительный растущий тренд данной активности, а отсутствие регистраций в 2022 и 2023 гг. частично обосновать временными задержками при одобрении заявок и обновлении статистики, в особенности для патентов.

В-третьих, статистика использования языков программирования следующая (без учета того, что в одном РИД может использоваться их несколько): «C++» (включая «C++ Builder») и «C#» – по 5, «JavaScript» – 4, «Python» – 3, «Java» и «PHP» – по 2, «Google Script» и «Go» – по 1. Таким образом, разработка программных средств для решения Задачи получила наибольшее распространение на языках C-семейства (в широком смысле), за которым идет применение «JavaScript» для Web-части средств; популярный же среди научно-исследовательской аудитории язык «Python» расположен лишь на третьем месте.

С точки зрения Международной патентной классификации для «G08B 13/00» найдено две полезные модели, а для «G06F 17/10», «G06Q 10/10» и «G11C 7/00» – по одной. Таким образом, чаще всего РИДы, кроме программ, относятся к разряду сигнализации о кражах, что с точки зрения решения Задачи более отвечает противодействию угрозе нарушения конфиденциальности (с поправкой, что данные устройства могут реагировать на инсайдера, который, получив доступ к устройству хранения информации, способен ее модифицировать или уничтожать).

В-четвертых, распределение решений по областям применения оказалось следующим (включая их расшифровки):

– «Человеческие ресурсы» (различные характеристики и показатели сотрудников, определяемые как статически тестами, так и динамически по поведению, а также их сравнением с шаблонными): 6;

– «Компьютерная сеть» (обработка сетевой активности в организации, по которой можно судить о деятельности сотрудников): 4;

– «Операционная система» (обработка данных в рамках ОС на персональном компьютере для предотвращения инсайдерской деятельности): 3;

– «Аппаратное обеспечение» (обособленные программно-аппаратные решения для обнаружения инсайдеров; в сделанных обзорах – только патенты на полезную модель): 2;

– «Информационная система» (широкое применение различного функционала для обработки поведения сотрудников в информационной системе путем встраивания агентов в ОС, учете сетевой инфраструктуры и пр.): 1;

– «Облачное хранилище» (размещение решения в облаке, позволяя обнаруживать инсайдеров по их взаимодействию с внешними информационными ресурсами): 1.

Таким образом, основное применение предложенных в обзорах решений заключается в оценивании сотрудников по их личностным признакам и поведению. На втором месте идет «слежка» за сетевой активностью, а на третьем – за состоянием их АРМ. Остальные области применения можно считать достаточно специфичными, имеющими высокую эффективность лишь для отдельных сценариев и/или организаций.

Заключение

В работе произведен обзор практических РИД российских ученых по решению задачи обнаружения инсайдера путем сбора информации по свидетельствам о государственной регистрации программ для ЭМВ и баз данных, а также патентов на полезные модели. В результате их последующей систематизации и анализа был сделан ряд основополагающих выводов: востребованность в практических решениях, небольшой повышающийся тренд актуальности Задачи, предпочтительность использования языков программирования «C++» и «C#», патентование в основном решений для сигнализации о кражах и применение в области оценивания личностных и поведенческих характеристик сотрудников.

Основным результатом исследования является систематизация РИД в табличном виде по критериям: год, тип, язык программирования, международная патентная классификация и область применения. Новизна результата состоит в том, что впервые сделан обзор всех РИД предметной области, ограниченной ключевыми словами «инсайдер» и «инсайдерский» для базы РИНЦ.

Теоретическая значимость исследования заключается в систематизации всей предметной области (ограниченной указанными ключевыми словами), а практическая – в сборе и базовой формализации опыта о реализации решений Задачи (то есть, по сути, Best Practices), что может использоваться при создании РИД.

Продолжением исследования должно стать объединение преимуществ в рассмотренных решениях Задачи для синтеза собственного.

Список источников

1. Власов Д.С. К вопросу о мотивации инсайдера организации и способах его классификации // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 1. С. 128–147.

2. Буйневич М.В., Власов Д.С. Аналитическим обзор моделей инсайдеров информационных систем // Информатизация и связь. 2020. № 6. С. 92–98.

3. Буйневич М.В., Власов Д.С. Сравнительный обзор способов выявления инсайдеров в информационных системах // Информатизация и связь. 2019. № 2. С. 83–91.

4. Approach to combining different methods for detecting insiders / M. Buinevich [et al.] // ACM International Conference Proceeding Series: 4. 2020. P. 3442619. DOI: 10.1145/3440749.3442619.

5. Ушаков И.А., Котенко И.В., Твердохлебова Ю.В. Система обнаружения инсайдеров в корпоративной компьютерной сети с использованием технологий машинного обучения: св-во о гос. рег. программы для ЭВМ № 2019666738 от 5 дек. 2019 г.

6. Ушаков И.А., Котенко И.В., Пелевин Д.В. Система обнаружения инсайдера в корпоративной компьютерной сети, используя алгоритмы, основанные на экспертных правилах: св-во о гос. рег. программы для ЭВМ № 2019666959 от 5 дек. 2019 г.

7. Ушаков И.А., Котенко И.В. Овраменко Ю.А. Компонент предобработки трафика в корпоративной компьютерной сети с использованием алгоритма Map Reduce в Hadoop кластере: св-во о гос. рег. программы для ЭВМ № 2019666737 от 5 дек. 2019 г.

8. Голуб О.Я. «Инсайдер» – система мониторинга, контроля и комплексной оценки эффективности работы персонала: св-во о гос. рег. программы для ЭВМ № 2021618157 от 7 мая 2021 г.

9. Голуб О.Я. Insider cloud (инсайдер клауд) – система мониторинга работы сотрудников и автоматизации учета рабочего времени: св-во о гос. рег. программы для ЭВМ № 2022665589 от 1 авг. 2022 г.

10. Воробьев Г.Е. Анализатор защищенности сетевых ресурсов от программно-технических воздействий: св-во о гос. рег. программы для ЭВМ № 2015611323 от 10 дек. 2014 г.

11. Бугаенко О.В., Хотячук В.К., Хотячук К.М., Тимошкин В.С. Скрытый регистратор доступа на объект: патент на полезную модель № 86026 от 24 апр. 2009 г. URL: https://yandex.ru/patents/doc/RU86026U1_20090820?ysclid=lwsutshk94308307739 (дата обращения: 12.04.2024).

12. Свищева М.Н., Цыбулин А.М. Автоматизированное рабочее место для контроля эффективности работы персонала и предотвращения инсайдерских атак: патент на полезную модель № 135435 от 17 июля 2013 г. URL: https://yandex.ru/patents/doc/ /RU86026U1_20090820?ysclid=lwsutshk94308307739 (дата обращения: 23.04.2024).

13. Система SoftControl для защиты банкоматов, рабочих станций и серверов от вторжений и инсайдерских атак: с св-во о гос. рег. программы для ЭВМ № 2017614376 от 21 февр. 2017 г.

14. Власов Д.С., Вострых А.В., Буйневич М.В. Программа для дистанционного приема лабораторных работ со встроенным модулем противодействия инсайдерской деятельности: св-во о гос. рег. программы для ЭВМ № 2021668640 от 3 нояб. 2021 г.

15. Программный комплекс SafenSoft SysWatch TPSecure для защиты банкоматов, рабочих станций и серверов от вторжений и инсайдерских инцидентов: св-во о гос. рег. программы для ЭВМ № 2016660308 от 13 июля 2016 г.

16. Попов Г.А., Максимова Е.А., Витенбург Е.А., Корнева В.А. Программный модуль регистрации и ввода личностных характеристик пользователей: св-во о гос. рег. программы для ЭВМ № 2016611565 от 15 дек. 2015 г.

17. Попов Г.А., Максимова Е.А., Витенбург Е.А., Корнева В.А. Программный модуль оценки легитимности и эффективности работы пользователя: св-во о гос. рег. программы для ЭВМ № 2016612581 от 11 янв. 2016 г.

18. Витенбург Е.А., Максимова Е.А., Попов Г.А., Корнева В.А. Анкетирование пользователя для определения его личностных характеристик: св-во о гос. рег. базы данных № 2016620299 от 11 янв. 2016 г.

19. Scanim Enterprise: св-во о гос. рег. программы для ЭВМ № 2021614666 от 18 марта 2021 г.

20. Исмагилов И.Р., Коленченко Ю.В. Приложение для автоматического поиска персональной банковской информации в электронных документах: св-во о гос. рег. программы для ЭВМ № 2020667293 от 3 дек. 2020 г.

21. Лакеев В.А., Хотячук В.К., Тимошкин В.С. [и др.] Скрытый регистратор несанкционированного доступа на объект или его локальные зоны: патент на полезную модель № 104751 от 12 окт. 2010 г.

References

1. Vlasov D.S. K voprosu o motivacii insajdera organizacii i sposobah ego klassifikacii // Elektronnyj setevoj politematicheskij zhurnal «Nauchnye trudy KubGTU». 2022. № 1. S. 128–147.

2. Bujnevich M.V., Vlasov D.S. Analiticheskim obzor modelej insajderov informacionnyh sistem // Informatizaciya i svyaz'. 2020. № 6. S. 92–98.

3. Bujnevich M.V., Vlasov D.S. Sravnitel'nyj obzor sposobov vyyavleniya insajderov v informacionnyh sistemah // Informatizaciya i svyaz'. 2019. № 2. S. 83–91.

4. Approach to combining different methods for detecting insiders / M. Buinevich [et al.] // ACM International Conference Proceeding Series: 4. 2020. P. 3442619. DOI: 10.1145/3440749.3442619.

5. Ushakov I.A., Kotenko I.V., Tverdohlebova Yu.V. Sistema obnaruzheniya insajderov v korporativnoj komp'yuternoj seti s ispol'zovaniem tekhnologij mashinnogo obucheniya: sv-vo o gos. reg. programmy dlya EVM № 2019666738 ot 5 dek. 2019 g.

6. Ushakov I.A., Kotenko I.V., Pelevin D.V. Sistema obnaruzheniya insajdera v korporativnoj komp'yuternoj seti, ispol'zuya algoritmy, osnovannye na ekspertnyh pravilah: sv-vo o gos. reg. programmy dlya EVM № 2019666959 ot 5 dek. 2019 g.

7. Ushakov I.A., Kotenko I.V. Ovramenko Yu.A. Komponent predobrabotki trafika v korporativnoj komp'yuternoj seti s ispol'zovaniem algoritma Map Reduce v Hadoop klastere: sv-vo o gos. reg. programmy dlya EVM № 2019666737 ot zayavl. 5 dek. 2019 g.

8. Golub O.Ya. «Insajder» – sistema monitoringa, kontrolya i kompleksnoj ocenki effektivnosti raboty personala: sv-vo o gos. reg. programmy dlya EVM № 2021618157 ot 7 maya 2021 g.

9. Golub O.Ya. Insider cloud (insajder klaud) – sistema monitoringa raboty sotrudnikov i avtomatizacii ucheta rabochego vremeni: sv-vo o gos. reg.programmy dlya EVM № 2022665589 ot 1 avg. 2022 g.

10. Vorob'ev G.E. Analizator zashchishchennosti setevyh resursov ot programmno-tekhnicheskih vozdejstvij: sv-vo o gos. reg.programmy dlya EVM № 2015611323 ot 10 dek. 2014 g.

11. Bugaenko O.V., Hotyachuk V.K., Hotyachuk K.M., Timoshkin V.S. Skrytyj registrator dostupa na ob"ekt: patent na poleznuyu model' № 86026 ot 24 apr. 2009 g. URL: https://yandex.ru/patents/doc/RU86026U1_20090820?ysclid=lwsutshk94308307739 (data obrashcheniya: 12.04.2024).

12. Svishcheva M.N., Cybulin A.M. Avtomatizirovannoe rabochee mesto dlya kontrolya effektivnosti raboty personala i predotvrashcheniya insajderskih atak: patent na poleznuyu model' № 135435 ot 17 iyulya 2013 g. URL: https://yandex.ru/ patents/doc/RU86026U1_20090820? ?ysclid=lwsutshk94308307739 (data obrashcheniya: 23.04.2024).

13. Sistema SoftControl dlya za shchity bankomatov, rabochih stancij i serverov ot vtorzhenij i insajderskih atak: sv-vo o gos. reg. programmy dlya EVM № 2017614376 ot 21 fevr. 2017 g.

14. Vlasov D.S., Vostryh A.V., Bujnevich M.V. Programma dlya distancionnogo priema laboratornyh rabot so vstroennym modulem protivodejstviya insajderskoj deyatel'nosti: sv-vo o gos. reg. programmy dlya EVM № 2021668640 ot 3 noyab. 2021 g.

15. Programmnyj kompleks SafenSoft SysWatch TPSecure dlya zashchity bankomatov, rabochih stancij i serverov ot vtorzhenij i insajderskih incidentov: sv-vo o gos. reg. programmy dlya EVM № 2016660308 ot 13 iyulya 2016 g.

16. Popov G.A., Maksimova E.A., Vitenburg E.A., Korneva V.A. Programmnyj modul' registracii i vvoda lichnostnyh harakteristik pol'zovatelej: sv-vo o gos. reg. programmy dlya EVM № 2016611565 ot 15 dek. 2015 g.

17. Popov G.A., Maksimova E.A., Vitenburg E.A., Korneva V.A. Programmnyj modul' ocenki legitimnosti i effektivnosti raboty pol'zovatelya: sv-vo o gos. reg. programmy dlya EVM № 2016612581 ot 11 yanv. 2016 g.

18. Vitenburg E.A., Maksimova E.A., Popov G.A., Korneva V.A. Anketirovanie pol'zovatelya dlya opredeleniya ego lichnostnyh harakteristik: sv-vo o gos. reg. bazy dannyh № 2016620299 ot 11 yanv. 2016 g.

19. Scanim Enterprise: sv-vo o gos. reg.programmy dlya EVM № 2021614666 ot 18 marta 2021 g.

20. Ismagilov I.R., Kolenchenko Yu.V. Prilozhenie dlya avtomaticheskogo poiska personal'noj bankovskoj informacii v elektronnyh dokumentah: sv-vo o gos. reg. programmy dlya EVM № 2020667293 ot 3 dek. 2020 g.

21. Lakeev V.A., Hotyachuk V.K., Timoshkin V.S. [i dr.] Skrytyj registrator nesankcionirovannogo dostupa na ob"ekt ili ego lokal'nye zony: patent na poleznuyu model' № 104751 ot 12 okt. 2010 g.

Информация о статье:
Статья поступила в редакцию: 27.04.2024; одобрена после рецензирования: 27.05.2024;
принята к публикации: 29.05.2024
The information about article:
The article was submitted to the editorial office: 27.04.2024; approved after review: 27.05.2024;
accepted for publication: 29.05.2024

Информация об авторах:
Власов Дмитрий Сергеевич, начальник управления информационных технологий и связи Главного управления МЧС России по г. Санкт-Петербургу (190000, Санкт-Петербург, наб. реки Мойки, д. 85), e-mail: prikerx@bk.ru, http://orcid.org/0000-0003-2332-8431, SPIN-код: 2739-2000

Information about the authors:
Vlasov Dmitry S., head of information technology and communications department of the Main directorate of EMERCOM of Russia in the Saint-Petersburg city (190000, Saint-Petersburg, nab. reki Moyki, d. 85), e-mail: prikerx@bk.ru, http://orcid.org/0000-0003-2332-8431, SPIN: 2739-2000