КОМБИНИРОВАНИЕ СПОСОБОВ ВЫЯВЛЕНИЯ ИНСАЙДЕРОВ БОЛЬШИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Буйневич М. В.[1], Власов Д. С.[2], Моисеенко Г. Ю.[3]

DOI: 10.21681/2311-3456-2024-3-2-13

Цель исследования: *изыскание направлений повышения эффективности противодействия инсайдерам в больших информационных системах за счет комбинирования способов их выявления.*

Методы исследования: *аналитический обзор релевантных научных публикаций, концептуальное моделирование, формализация, категориальный подход, экспертное и теоретическое комбинирование, синтез, алгоритмизация.*

Полученные результаты: *получен обобщенный список и разработана частично формализованная модель объединения качественно различных способов выявления инсайдеров в больших информационных системах; предложен экспертный прогноз 21 комбинации из 7 указанных способов, дана теоретическая оценка успешности их сочетания; синтезирован комбинированный способ выявления инсайдеров, алгоритм которого задан в виде псевдокода.*

Научная новизна работы *определяется авторским подходом к комбинированию способов на основе категориального пространства, которое имеет оси вдоль следующих пар антагонистических элементов: нормальное vs аномальное, статическое vs динамическое, субъект vs объект. Большинство комбинаций способов предложены впервые.*

Ключевые слова: *большие информационные системы, информационная безопасность, инсайдер, способ выявления, комбинация методов.*

METHODS COMBINING FOR IDENTIFYING OF INSIDERS IN LARGE INFORMATION SYSTEMS

Buinevich M. V.[4], Vlasov D. S.[5], Moiseenko G. Y.[6]

The goal of the investigation: *finding ways to improve the effectiveness of countering insiders in large information systems by combining methods of their detection.*

Research methods: *analytical review of relevant scientific publications, conceptual modeling, formalization, categorical approach, expert and theoretical combination, synthesis, algorithmization.*

Results: *a generalized list is obtained and a partially formalized model of combining qualitatively different methods of detecting insiders in large information systems is developed; an expert forecast of 21 combinations from 7 of these methods is proposed, a theoretical evaluation of the success of their combination is given; a combined method of detecting insiders is synthesized, the algorithm of which is given in the form of pseudo code.*

The scientific novelty *is determined by the author's approach to combining methods on the basis of a categorical space with axes along the following pairs of antagonistic elements: normal vs. abnormal, static vs. dynamic, subject vs. object. Most of the combinations of methods are proposed for the first time.*

Keywords: *large information system, information security, insider, detection method, combination of methods.*

1 Буйневич Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России, Санкт-Петербург. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru

2 Власов Дмитрий Сергеевич, начальник управления информационных технологий и связи Главного управления МЧС России по г. Санкт-Петербургу, Россия. ORCHID: http://orcid.org/0000-0003-2332-8431. E mail: prikerx@bk.ru

3 Моисеенко Григорий Юрьевич, руководитель направления Министерства обороны РФ, Москва, Россия. E-mail: mogreq@mail.ru

4 Mikhail V. Buinevich, Dr.Sc., Professor, Professor of Dep. Applied Mathematics and Information Technologies of Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint-Petersburg, Russia. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru

5 Dmitry S. Vlasov, Head of Information Technology and Communications Department EMERCOM of Russia Main Directorate in the St. Petersburg city, Saint-Petersburg, Russia. ORCHID: http://orcid.org/0000-0003-2332-8431. E-mail: prikerx@bk.ru

6 Grigory Y. Moiseenko, Head of direction, Ministry of Defense of the Russian Federation, Moscow, Russia. E-mail: mogreq@mail.ru

Введение

Согласно отчету «2023 Cost of Insider Threats: Global Report» [1], опубликованному Ponemon Institute, специализирующемуся на независимых исследованиях методов обеспечения конфиденциальности в сфере бизнеса и государственного управления, киберугрозы со стороны инсайдеров выросли за последний год на 47%. За тот же период расходы на раннее обнаружение инсайдеров и нейтрализацию их атак возросли на 31%. Отчет «Data Breach Investigations Report 2023» от компании Verizon [2], составленный на основе обработки свыше 16 000 зарегистрированных инцидентов безопасности и более 5000 подтвержденных случаев утечки данных на 6 континентах и в 20 отраслях, показал, что около трети всех случаев произошло вследствие инсайдерских атак.

Такая тенденция, в том числе, свидетельствует, что применяемые способы противодействия инсайдерской угрозе достигли некого предела своей эффективности. Ситуация усложняется следующими обстоятельствами. Во-первых, не все инсайдеры и «среды их обитания» одинаковы. Такие нарушители существенно различаются по мотивации (халатные сотрудники, злоумышленники, агенты влияния и т.д.) [3], поведению и подготовке, а в разных отраслях доминируют собственные инсайдерский атаки (например, здравоохранение – социальная инженерия, ИТ-сектор – ошибки привилегированных пользователей, сектор финансовых услуг – умышленная кража учетных записей). Отсюда следует, что конкретный способ выявления инсайдеров может быть максимально результативным только для сотрудников или компаний (организаций) определенного типа. Во-вторых, для инсайдерской угрозы время играет важную роль. В исследовании [2] указывается, что среднее время нейтрализации инсайдера составляет 77 дней, и только 13% инсайдеров нейтрализуются быстрее, чем за 30 дней. Кроме того, результаты исследования доказывают, что инциденты продолжительностью свыше 90 дней, обходятся компаниям примерно в 13,7 млн. долларов США в год, а менее 30 дней – примерно в 2 раза меньше. Соответственно, способ выявления инсайдеров должен быть максимально оперативным. И, в-третьих, на успешность атак оказывает влияние размер самой компании. Вполне естественно, что крупные организации, имеющие большие информационные системы, подвергаются большему количеству инсайдерских атак более многообразной этимологии (т.е. происхождения или природы). По данным [1] ежегодные расходы крупных организаций, владельцев больших информационных систем, на сдерживание инсайдеров составили в среднем 18,3 млн. долларов США против 7,68 млн. долларов США у компаний численностью менее 500 сотрудников. Поэтому способ выявления инсайдеров должен быть возможно более экономичным.

С учетом сложившихся обстоятельств рациональным решением для больших информационных систем представляется комбинирование способов выявления инсайдеров. И первыми шагами в этом направлении является их попарное сочетание с доказательством реализуемости комбинации через формализацию и последующий мыслительный эксперимент.

Обзор релевантных работ

Произведем обзор (в том числе и авторских) работ, в которых описываются подходы (или способы), применимые для комбинирования различных методов, моделей и инструментов выявления инсайдеров.

Работа [4] посвящена выявлению инсайдеров путем анализа сетевой активности сотрудников организации, основываясь на двух подходах к классификации каждого пользователя, как лояльного или злонамеренного. Суть первого заключается в применении строгих правил, созданных экспертом (или их группой); суть второго – в создании моделей машинного обучения по выборке сетевого трафика, полученной с помощью генератора сетевых атак. В качестве классификаторов машинного обучения применялись такие базовые как деревья решений, наивный байесовский классификатор, метод k-ближайших соседей и метод опорных векторов, а также их комбинация: голосование большинством, взвешенное и мягкое голосование, Adaboost. Поскольку каждый из подходов мог давать собственные результаты классификации пользователей, в т.ч. дополняющие или противоречащие друг другу, то для их комбинирования применялись 4 вариации: объединение, пересечение или выбор одного из вышеперечисленных.

В работе [5] описано решение задачи противодействия атакам на сервисы облачных вычислений со стороны инсайдеров, для чего комбинируется пара методов путем их наложения. Первый основан на классическом дереве атак, примененном к внутренней среде облачных сервисов; второй представляет собой, так называемую, цепочку уничтожения, вышедшую из концепции ведения боевых действий и заключающуюся в отслеживании степени продвижения атаки к заданным целям. Как результат, появляется возможность оценивать защищаемую систему на различных уровнях абстракции.

Работа [6] ссылается на 2 метода противодействия инсайдерам: на основе анализа внутренних угроз в организации и генерации данных, соответствующих человеческому поведению, его психологическим аспектам и контрразведывательной

деятельности. Как результат, второй метод дополняет первый, делая его более точным при фактическом обнаружении инсайдеров.

В [7] описывается способ, где сначала производится сбор данных с устройств сотрудников (телефоны, ноутбуки, персональные компьютеры и пр.) для создания профиля каждого из пользователей. А затем, с применением методов машинного обучения в части поиска аномалий выделяются те профили, которые имеют существенное отличие от профилей других сотрудников. Идея, предлагаемая в статье, основана на том, что инсайдеры будут иметь «концентрацию» данных, отличную от тех, которая есть на устройствах у коллег. Таким образом, предлагаемая система основана на объединении инструментов сбора и обработки данных, которые были подвергнуты определенному упрощению. Как результат, удается обнаруживать инсайдеров, профили которых отличаются не только от профилей других коллег, но и от собственных, но на более раннем периоде. Второй случай, очевидно, означает факт превращения лояльного сотрудника в нарушителя, что позволяет лучше понять причины такого превращения и негативные предпосылки этого для организации.

Работа [8] аналогична [7] в части подхода к выявлению инсайдерской деятельности – через выявление сотрудников, поведение которых имеет существенные отличия от остальных. Однако в исследовании подчеркивается, что современные инсайдеры стремятся быть похожими на лояльных пользователей. Таким образом, для их выявления может потребоваться анализ нескольких источников информации, в интересах чего авторы предлагают комбинировать консенсусную кластеризацию (позволяющую оценить влияние небольших возмущений в наборах данных на состав кластера) и обнаружение аномалий. Основная идея заключается в поиске аномальных признаков типовой активности сотрудников, когда действия инсайдера внешне неотличимы от действий лояльных пользователей; это достигается каскадным применением методов машинного обучения.

В работе [9] предлагается способ предупреждения инсайдерских атак, объединяющий сразу 3 метода риск-менеджмента – основанный на поведении злоумышленника и учитывающие компьютерные и психо-социальные риски. В первом методе выделяются такие риски, как недовольный сотрудник, принятие критики, управление гневом, невовлеченность в «жизнь» организации, игнорирование правил, производительность, стресс, конфронтация, личные проблемы, эгоцентризм, надежность, прогулы. Ко второму методу относятся следующие риски: неудачный вход в систему, подозрительное общение, сбор данных, установка и использование «нештатного» программного обеспечения, удаленный вход, несанкционированный доступ, удаление логов. Для третьего метода характерны такие риски, как проблемы с деньгами, недавний разрыв или потеря, чрезмерная депрессия, патологическое отыгрывание (игромания), расстройство адаптации (т.е. чрезмерное реагирование на стресс) и проблемы с тревогой (т.е. бессознательное развитие тревожной для человека ситуации). Для моделирования инсайдерской деятельности используется системная динамика (направление в изучении сложных систем). Как результат, с применением продукта Vensim строится модель, связывающая вероятностное поведение человека и детерминированное поведение системы.

В работе [10] описываются две модели, работающие по качественно разным признакам выявления инсайдеров. Первая предназначена для распознавания лица пользователя и сравнение его с занесенным в базу данных при регистрации, для чего используется OpenCV (*аббр. от англ.* Open Source Computer Vision, *пер. на русск.* открытая библиотека для работы с алгоритмами компьютерного зрения). Вторая отслеживает поведение пользователей и классифицирует их на 4 следующих: легитимный, возможно легитимный, возможно нелегитимный, нелегитимный. Эта модель реализуется на базе алгоритма k-ближайших соседей (из области машинного обучения). Обе модели объединяются в одну метамодель, которая собственно и лежит в основе способа обнаружения инсайдеров.

Анализ результатов обзора релевантных работ позволяет сделать следующие выводы. Во-первых, существует достаточно малое количество исследований, направленных на объединение разнородных способов выявления инсайдеров. Во-вторых, наблюдается тенденция применения машинного обучения [7, 8, 10], хотя оно и подходит только для определенных способов поиска, имеющих возможность получения формализованной Best Practices. И, в-третьих, объединение способов, относящихся к разным областям организаций (например, сетевое поведение пользователей и их психоэмоциональное состояние) является существенной проблемой, не нашедшей полноценного решения; частично решения предлагаются в [6, 10]. Можно отметить работу [9], где подобная попытка предпринята путем применения системно-динамического моделирования. Однако какого-либо полноценного подхода для объединения всех способов или их большей части на данный момент не обнаружено.

Способы выявления инсайдеров

Систематизируем и обобщим способы выявления инсайдеров в больших информационных системах с учетом их списков, составленных авторами ранее [11, 12].

Способ 1 – Анализ динамики обычной жизни, основанный на учете событий и ситуаций сотрудников, в том числе и вне организации. Так, повышение финансовых трат и большое количество взятых кредитов может привести к тому, что сотрудник станет продавать конфиденциальную информацию «третьим лицам».

Способ 2 – Выявление аномалий в типовых сценариях работы пользователей, основанное на модели IDES (*аббр. от англ.* Intrusion Detection Expert System, *пер. на русск.* экспертная система обнаружения вторжений) и подразумевающее некоторые отклонения в действиях потенциального нарушителя по сравнению с поведением большинства других – лояльных. Например, резкое повышение отправленного сетевого трафика от сотрудника на внешний Интернет-ресурс может сигнализировать о потенциальной угрозе нарушения конфиденциальности информации.

Способ 3 – Предотвращение накопления критической конфиденциальной информации, заключающееся в отслеживании объема и/или охвата данных, к которым получил доступ сотрудник. Так, если кем-либо, в нарушение должностных обязанностей и превышение полномочий, в организации была собрана по частям достаточно полная клиентская база, то это может считаться подозрительным и сигнализировать о целенаправленной инсайдерской деятельности.

Способ 4 – «Ловля на живца» (*в англ. лит.* – Honeypot, Honeynet, Honeytoken и пр., *досл. пер. на русск.* «медовая ловушка»), суть которой заключается в оставлении «приманок» для злоумышленника, которые не имеют особой ценности и существенной защиты, но получение доступа к которым будет говорить о злонамеренной деятельности. Например, если к хранимому в условно свободном доступе документу с лже-финансовой отчетностью будут осуществляться попытки доступа (с целью хищения или уничтожения), то это может сигнализировать о заинтересованности сотрудника-инсайдера в неправомерных действиях.

Способ 5 – Выявление потенциального нарушителя психодиагностическими методами, которое основано на изучении психологии сотрудников и определения среди них тех, кто является или может стать инсайдером. Так, сотрудники с высоким желанием самоутвердиться, придерживающиеся асоциальных и деструктивных взглядов, а также падкие на получение быстрой прибыли в случае финансовых затруднений могут в числе первых заняться инсайдерством.

Способ 6 – Анализ защищенности пользователей информационных систем от атак с применением социальной инженерии. Так, близкие личностные связи двух сотрудников могут позволить внешнему нарушителю воздействовать на второго (например, администратора сети) через первого (например, члена группы поддержки). Как результат, оба этих сотрудника могут непреднамеренно стать инсайдерами.

Способ 7 – Оценка потенциала сотрудника для реализации атаки, которая позволяет выявить обладающих критериями, подходящими для ведения инсайдерской деятельности. Например, высокий уровень технической подготовленности, участие в Pentest-проектах (т.е. в качестве «белого хакера») и предыдущая работа в неблагонадежных организациях (в частности, замешанных в преступной деятельности) может считаться признаками, характеризующими сотрудника как способного к успешному совершению неправомерных действий.

Модель комбинирования

Согласно вышеприведенному краткому описанию способов, каждый из них строится на собственных функциональных элементах, т.е. описывается в их терминах, точно совпадающих или обобщаемых в более абстрактное понятие. Например, Способы 5 и 7 строятся на элементе «тестирование» применительно к сотрудникам – тем самым, функциональные элементы этих способов совпадают. Аналогично, Способ 1 основывается на «событиях в жизни», а Способ 6 учитывает взаимодействие «личности» с «обществом» – все эти элементы могут быть обобщены в понятие «социума». Таким образом, логично было бы характеризовать все способы на основе одного набора элементов, т.е. в едином базисе. Тогда комбинация способов также будет работать на этом базисе, что может считаться специальной *моделью комбинирования*.

Одной из основных проблем синтеза новых базисов является их корректность в виде ортогональности – так, чтобы каждый базис не являлся бы комбинацией других. Для этого воспользуемся аппаратом категориального деления, обозначаемого vs (*аббр. от лат.* versus, *пер. на русск.* против), хорошо зарекомендовавшим себя для подобного рода методологических задач [13]. Для этого выделим 3 философские категориальные пары антагонистов, обозначаемые P (*аббр. от лат.* pair, *пер. на русск.* пара), отражающих подходы к выявлению инсайдеров. Именно эти категории и будут набором базисов, создавая тем самым 3-мерное категориальное пространство – XYZ. Каждая же точка в этом пространстве будет характеризовать принцип работы одного из 7 способов – она может быть задана набором 3-х элементов-антагонистов каждой из пар.

Авторский опыт, поверенный авторитетными публикациями других ученых-специалистов [14, 15], позволил выбрать следующие категориальные пары, характеризующие способы выявления инсайдеров и отвечающие на вопросы:

1) выявляет ли способ отклонения (***A***, *аббр. от англ.* Anormal) от нормы (***N***, *аббр. от англ.* Normal) по признакам – пара ***PX***: Нормальный (X_N) ***vs*** Аномальный (X_A);
2) анализирует ли способ постоянные (***S***, *аббр. от англ.* Static) или изменяющиеся во времени (***D***, *аббр. от англ.* Dynamic) признаки – пара ***PY***: Статический (Y_S) ***vs*** Динамический (Y_D);
3) получает ли способ признаки непосредственно от людей (***H***, *аббр. от англ.* Human) или же объектов (***O***, *аббр. от англ.* Object), с которыми они взаимодействуют – пара ***PZ***: Субъект (Z_H) ***vs*** Объект (Z_O).

Таким образом, характеристика каждого способа (*Method*) может быть записана точкой (X,Y,Z) в категориальном пространстве:

$$\begin{cases} Method \longrightarrow (X,Y,Z) \\ X \in \{X_N, X_A\} \\ Y \in \{Y_S, Y_D\} \\ Z \in \{Z_H, Z_O\} \end{cases} \quad ((1)$$

Так, например, Способ 1 основан на анализе событий в жизни сотрудника и построен из следующих функциональных элементов: «жизнь сотрудников», «события в жизни», «пребывание вне организации», «взаимодействие с миром». С этой позиции он может быть описан элементами категориальных пар: «нормальная деятельность» + «динамический анализ» + «признаки субъекта» – т.е. возникающие события в жизни сотрудника. Таким образом, Способу 1 соответствует точка: (X_N,Y_D,Z_H). Аналогичным образом, запишем в таком категориальном пространстве каждый из способов через его функциональные элементы в табличном виде (Таблица 1).

Анализ Таблицы 1 позволяет сделать вывод, что практически все способы хотя и имеют свою точку в категориальном пространстве, однако могут иметь отдельные одинаковые координаты категориальных пар и тождественные (или даже общие) функциональные элементы; что может быть использовано в дальнейшем для оценки их совместимости при комбинировании. Лишь два способа совпадают в категориальном пространстве с этой позиции (имеют единую точку) Способ 1 и Способ 5; что является закономерным, поскольку способы подобным образом анализируют изменение состояния человека при взаимодействии с внешним миром на предмет перехода в группу инсайдеров.

Экспертное комбинирование

Приведем далее все возможные комбинации пар способов и дадим их экспертную оценочную интерпретацию; очевидно, что 7 способов создадут 21 пару.

Способ 1 + Способ 2

Техническое противодействие инсайдерам затруднено тем, что, как правило, эти сотрудники компании хорошо знают, какое программное обеспечение

Таблица 1

Функциональные элементы и точки в категориальном пространстве способов выявления инсайдеров

Условное название способа	Функциональные элементы	Точка в категориальном пространстве
Способ 1. Анализ событий в реальной жизни	жизнь сотрудников, события в жизни, пребывание вне организации, взаимодействие с миром	(X_N,Y_D,Z_H)
Способ 2. Выявление аномалий в типовых сценариях работы пользователей	сценарии работы, типовое поведение, аномальное поведение, должностные обязанности	(X_A,Y_D,Z_O)
Способ 3. Предотвращение накопления критической конфиденциальной информации	сбор информации, объем информации, критичный объем, содержимое данных	(X_A,Y_S,Z_O)
Способ 4. «Ловля на живца» («Honeypot»)	«привлекательный» объект, отслеживание доступа, размещение ресурсов, пост-анализ	(X_N,Y_S,Z_O)
Способ 5. Выявление инсайдера психодиагностическими методами	психология человека, критерии нарушителя, мотивация сотрудника, тестирование сотрудника	(X_N,Y_D,Z_H)
Способ 6. Анализ защищенности пользователей от социальных атак	внешний нарушитель, социальная инженерия, общество, личность	(X_N,Y_S,Z_H)
Способ 7. Оценка потенциала пользователя для реализации атаки	потенциал сотрудника, критерии деятельности инсайдера, возможности сотрудника, тестирование сотрудника	(X_A,Y_S,Z_H)

и с какими уязвимостями используется [16, 17], а также, какие применяются политики безопасности. Именно поэтому в последнее время много внимания уделяется не только техническим средствам борьбы с инсайдерами, но и, например, анализу событий пользователей информационной системы в реальной жизни. Способ 1 схож со Способом 2, поскольку он также выделяет аномальное поведение, но не объектов, а субъектов информационной системы. Как результат, можно разработать комплекс программного обеспечения, который будет анализировать аномальные действия с объектами в организации [18] и поведение субъектов в реальной жизни, на основании чего и делать предсказания об инсайдерской деятельности.

Способ 1 + Способ 3

Экспертный анализ показал, что Способы 1 и 3 не имеют возможности работать в комплексе. Первый способ соответствует точке (X_A, Y_S, Z_O), а второй – точке (X_N, Y_D, Z_H) в категориальном пространстве. Таким образом, у них не совпадает ни один из элементов категориальной пары, что более формально подтверждает невозможность комбинирования.

Способ 1 + Способ 4

Инсайдеры – это не всегда пользователи информационной системы, которые вынашивают долгосрочный и точный план противоправной деятельности. Иногда это люди, которые попали в трудную финансовую ситуацию, разрешение которой возможно за передачу конфиденциальной информацию «третьим лицам» в обмен за вознаграждение. Подобного рода инсайдеров можно выявлять с помощью «подставных» предложений («Honeypot») от якобы «третьих лиц» в определенные трудные моменты их жизни, которые необходимо зафиксировать и учесть. Главным минусом данной комбинации однозначно является противоречие морально-этическим нормам.

Способ 1 + Способ 5

При выявлении инсайдеров психологическими методами создаются профили пользователей информационных систем с определенными показателями, которые могут указывать на склонность к инсайдерству. Одним из показателей может быть то, как сильно сложные жизненные ситуации способны подтолкнуть человека к передаче конфиденциальной информации «третьим лицам»; для определения этого возможно провести специализированное тестирование. В результате применения данной комбинации способов станет понятно, события в реальной жизни каких пользователей нужно отслеживать в первую очередь. Такой подход подобен моделям сетевых атак, но перенесенных в психологическую область. Как следствие, удастся сэкономить ресурсы, затрачиваемые на анализ поведения всех сотрудников, часть из которых в принципе не станут инсайдерами даже в тяжелых жизненных ситуациях.

Способ 1 + Способ 6

Для результативной работы Способа 6 необходимо наличие графа межличностных связей персонала с актуальной информацией, поскольку отношения между сотрудниками могут меняться на противоположные за недели или даже часы. В интересах этого необходимо постоянное обновление данного графа на основе событий, которые происходят в реальной жизни людей, работающих в организации; в этом и заключается комбинация Способов 1 и 6.

Способ 1 + Способ 7

Комбинация способов 1 и 7 может заключаться не в простом выявлении сотрудников, обладающих высоким потенциалом для совершения инсайдерских атак, а также и тех, для кого этот потенциал хотя и является условно средним, однако которым он все равно воспользуется в определенных жизненных ситуациях.

Способ 2 + Способ 3

Если пользователь информационной системы начинает собирать (и накапливать) информацию из системы хранения данных, то, следовательно, он воспроизводит аномальный сценарий работы. Таким образом, оба способа – 2 и 3 – работают на качественно едином принципе, но используя для этого разные подходы; их же объединение, очевидно, повысит общую результативность выявления инсайдеров.

Способ 2 + Способ 4

При выявлении аномалий в типовых сценариях работы пользователя можно столкнуться со сложностью отделения его нештатного поведения от обычных отклонений в работе лояльных сотрудников, связанными с определенными событиями в системе (например, ее сбой). В таком случае, для пользователей, чей профиль находится между типичным и атипичным поведением, можно устраивать дополнительную проверку в виде «ловли на живца».

Способ 2 + Способ 5

При выявлении инсайдера психологическими методами проводится ряд тестов с их последующим анализом и определением профиля пользователя информационной системы. Целесообразно до проведения такого тестирования производить анализ атипичного пове-дения или небольших отклонений в работе пользователя информационной системы.

Способ 2 + Способ 6

В Способе 6, заключающемся в анализе защищенности пользователей от социальных атак, строится граф межличностных связей персонала, в который можно занести профили нормального поведения,

как взаимодействия между некоторыми пользователями информационной системы; например, как часто один пользователь отправляет другому сообщения, содержащие конфиденциальные данные. Если поведение будет отличаться от типичного, это позволит предположить, что пользователь перешел (или может перейти) в разряд инсайдеров. Таким образом, несмотря на отсутствие у способов общих элементов категориальных пар, они все же могут быть скомбинированы, впрочем, не повысив существенно результативность обнаружения инсайдеров.

Способ 2 + Способ 7

Объединение способов аналогично комбинации Способов 1 + 7 с тем лишь отличием, что оно хотя и выявляет инсайдеров среди пользователей с потенциалом к проведению атак, но учитывает не их жизненные ситуации, а определенные события в рамках организации. Например, нарушитель может применить свои навыки лишь при возникновении определенных и крайне «удачных» условий в организации, таких, как, например, компрометация базы паролей.

Способ 3 + Способ 4

Если в системе применяется политика безопасности, основанная на предотвращении накапливания конфиденциальной информации, то потенциальному инсайдеру может оказаться сложно заполучить ее в полном объеме. Таким образом, чтобы его деятельность не была обнаружена, он будет искать иные пути достижения своей цели. В этом случае можно воспользоваться «ловлей на живца» путем предоставления ему возможности якобы получить недостающую информацию. Когда инсайдер попробует получить к ней доступ, сработает «медовая ловушка», и он будет детектирован.

Способ 3 + Способ 5

Экспертный анализ показал, что Способы 3 и 5 не имеют возможности работать в комплексе. Способ 3 соответствует точке (X_A, Y_S, Z_O), а Способ 5 – точке (X_N, Y_D, Z_H) в категориальном пространстве. Таким образом, у них не совпадает ни один из элементов категориальных пар, что более формально подтверждает невозможность комбинирования.

Способ 3 + Способ 6

Благодаря графу межличностных связей персонала становится понятно, какие пользователи и через каких работников компании могут быть подвергнуты атаке с использованием социальной инженерии. Тогда пользователям, которые особенно подвержены такому виду атак, можно ограничивать доступ к конфиденциальной информации и отслеживать накопление ими данных, чтобы при попытке передать ее «третьим лицам» не был нанесен ущерб организации.

Способ 3 + Способ 7

Аналогично комбинации Способов 3 и 6, на основании склонности поддаваться влиянию методов социальной инженерии, можно создать систему безопасности, которая также будет изолировать часть пользователей от конфиденциальной информации, но уже на основе их потенциала к реализации атак.

Способ 4 + Способ 5

Так как при выявлении инсайдера психологическими методами очень часто совершается ошибка II рода (отвергается гипотеза о том, что сотрудник – инсайдер, хотя он таковым является), то можно существенно усовершенствовать этот способ, добавив в него «ловлю на живца». В таком случае, при проведении психологического тестирования с последующим анализом результатов и определении пригодности кандидатур будут проводиться дополнительные тесты не только психологической природы, хотя и связанные с предыдущими результатами; например, системного администратора логичнее проверять на стремление к краже ключей доступа, а сотрудника бухгалтерии – на попытку разглашения финансовой информации.

Способ 4 + Способ 6

Представим, что в информационной системе существует Пользователь 1, у которого нет доступа к конфиденциальным данным, и Пользователь 2, имеющий к ним доступ. И если между такими субъектами устанавливаются тесные дружеские взаимоотношения, то становится возможным проведение атаки с использованием социальной инженерии на второго пользователя посредством первого. Иногда эту ситуацию можно решить, если предоставить Пользователю 1 мнимый доступ к информации, не предназначенной для него. В таком случае ему не придется воздействовать на Пользователя 2, а просто самому попробовать получить доступ к такой информации; в результате его инсайдерские действия будут детектированы.

Способ 4 + Способ 7

Интересным решением может стать добавление в тестирование на профпригодность при поступлении на работу механизма «ловли на живца», заключающегося в определении того, как будущий сотрудник в принципе реагирует на данные, оставленные без внимания. Так, если кандидат сходу видит бреши в системе безопасности, позволяющие ему заполучить конфиденциальную информацию, то он априори может быть опасен организации. Исключение составляют те кандидаты, которые изначально идут в отдел информационной безопасности и защиты информации и выявление подобного рода проблем входит в их компетенцию.

Способ 5 + Способ 6

Недостатком построения графа межличностных отношений персонала (Способ 6) является субъективность определения как самих связей сотрудников, так и силы их влияния. Повышение адекватности такой графовой модели (т.е. ее отражения реальной ситуации в организации) может быть осуществлено путем проведения дополнительных психодиагностических тестов (Способ 5).

Способ 5 + Способ 7

Совместное тестирование сотрудников, как с точки зрения психологии, так и с позиции потенциала для проведения атак позволит составить его более полный (и многоаспектный) «портрета, существенно повысив тем самым качество предсказания будущих инсайдеров. Так, например, признаки неуравновешенности и опыт хакерской деятельности сами по себе не будут говорить о потенциальном инсайдере, хотя их одновременное наличие у сотрудника будет крайне подозрительным, поскольку он может совершать неправомочные действия «на волне эмоций».

Способ 6 + Способ 7

Пользователи с высоким инсайдерским потенциалом вполне могут начать использовать свои социальные отношения с другими сотрудниками в целях получения через них конфиденциальной информации. Таким образом, сила связей в графе межличностных отношений может быть уточнена с учетом умения пользователей (т.е. узлов графа) проводить подобного рода атаки.

Задача комбинирования

Научно-обоснованная оценка возможности комбинирования является методологически сложной задачей. Однако для ее решения можно применить формулу (1), согласно которой каждому способу может быть поставлена в соответствие точка в категориальном пространстве. Воспользуемся для этого следующей логикой.

Во-первых, если точки способов покоординатно совпадают, это означает, что их подходы строятся на одинаковом базисе и, следовательно, способы имеют полную (*по англ.* Full) комбинируемость.

Во-вторых, если точки способов не совпадают ни по одной из координат, это означает, что их подходы строятся на абсолютно различном базисе и, следовательно, способы имеют низкую (*по англ.* Low) комбинируемость.

В-третьих, если точки способов совпадают хотя бы по одной из координат, это означает, что в их подходах совпадает один элемент категориальной пары и, следовательно, способы имеют среднюю (*по англ.* Medium) комбинируемость.

В-четвертых, если точки способов совпадают по двум координатам, это означает, что в их подходах не совпадает только один элемент категориальной пары и, следовательно, способы имеют высокую (*по англ.* High) комбинируемость.

И, в-пятых, если экспертный анализ ранее показал невозможность работы способов в комплексе, это значит, что их подходы считаются принципиально разными и, следовательно, у способов отсутствует (*по англ.* None) комбинируемость.

Исходя из введенных выше обозначений количества совпавших координат в категориальном пространстве, а также экспертного анализа комбинаций способов, дадим оценку успешности комбинирования пар; результат приведен в Таблице 2.

Табличный анализ (см. Таблицу 2) оценок возможности комбинирования способов позволяет сделать следующие выводы.

Во-первых, полная комбинируемость обнаружена для Способов 1 и 5, что закономерно, поскольку анализ жизненных событий сотрудников напрямую связан с их психоэмоциональным состоянием.

Таблица 2

Результат комбинирования пар способов выявления инсайдеров

	Способ 1	**Способ 2**	**Способ 3**	**Способ 4**	**Способ 5**	**Способ 6**	**Способ 7**
Способ 1		Medium	None	Medium	Full	High	Medium
Способ 2			High	Medium	Medium	Low	Medium
Способ 3				High	None	Medium	High
Способ 4					Medium	High	Medium
Способ 5						High	Medium
Способ 6							High
Способ 7							

Примечание. В Таблице 2 темно-серым фоном отмечены ячейки, комбинирование для которых не имеет смысла (поскольку комбинационная пара состоит из одного и того же способа). Светло-серым фоном отмечены ячейки, возможность комбинирования для которых уже указана, поскольку ячейки соответствуют таким же, но симметричным относительно диагонали. Остальные ячейки имеют следующий фон: белый для None – принципиальная невозможность комбинирования; желтый для Low – совпадение 0 координат; синий для Medium – совпадение 1-ой координаты; зеленый High – совпадение 2-х координат; красный для Full – совпадение 3-х координат.

Во-вторых, для трех следующих комбинаций способов отсутствуют совпадения их координат: Способ 1 + Способ 3, Способ 3 + Способ 5 и Способ 2 + Способ 6. При этом первые две пары не могут в принципе работать в комплексе; последняя будет иметь низкую комбинируемость, что закономерно – выявление аномалий при общении через социальные связи не принесет существенной пользы, поскольку методы социальной инженерии основаны на типовом общении людей, а не отличном от нормального.

И, в-третьих, статистика по комбинируемости имеет следующий вид: None – 2, Low – 1, Medium –10, High – 7, Full – 1. Таким образом, основная «масса» способов имеет среднюю успешность комбинирования.

Новый комбинированный «Способ 1 + 5»

Исходя из оценки возможности комбинирования способов обнаружения инсайдеров, наиболее удачной (см. Таблицу 2, значение Full) комбинацией является пара «Способ 1 + Способ 5», поскольку все их координаты в категориальном пространстве совпадают.

Суть совместной работы способов заключается в следующем. Во-первых, (следуя идее Способа 1) необходимо анализировать события в жизни сотрудников организации. Во-вторых, (следуя идее Способа 5), требуется непрерывное применение тестирования сотрудников на предмет изменений в их психологии, что может привести к совершению ими неправомерных действий (в данном случае – к инсайдерству).

Объединение идей способов позволит создать новый способ, основанный на некой модели атак на психику человека, целью которых является выведение его из лояльных сотрудников в инсайдеры. При этом источниками атак являются не инициаторы-субъекты (как в случае Способа 6), а внешние факторы. Такая модель психологических атак должна отражать особенности сотрудника, т.е. быть подстроена под него, а каждое новое событие (атака) может переводить его в следующее состояние. Достижение атакой финальной точки будет означать то, что сотрудник стал инсайдером (с психологической точки зрения).

Для обоснования работоспособности такого нового комбинированного способа приведем следующий пример. Предположим, что данная модель отражает некоторую взаимосвязь между следующими элементами: наличие дорогих гаджетов у его окружения, динамика цен на них (например, в виде графика выхода новых версий устройств), зависимость от чужого мнения и позиционирование своих интересов выше интересов компании. Очевидно, что сотрудник с высокими двумя последними показателями при повышении первых двух может попасть в ситуацию, когда резко понадобятся деньги на покупку новой версии популярного устройства. И это приведет к тому, что он с большой вероятностью попытается продать конфиденциальные данные компании третьим лицам – т.е. займется инсайдерской деятельностью.

Предложим алгоритм данной комбинации способов в формализованном виде с помощью следующего псевдокода.

```
Input:
 Environment – информация о физическом
               окружении сотрудника
 Persons[] –   информация о психологических
               особенностях всех сотрудников
 Events[] –    события, происходящие в окружении
               сотрудников
Output:
 Insiders[] –  индексы сотрудников, ставших
               инсайдерами
BEGIN
 1: VAR model = BuildModel(Environment)
 2: FOR_WITH_INDEX (person, index) IN Persons
 3:  model.SetPerson(person)
 4:  model.ApplyEvents(Events)
 5:  VAR attacks[] = model.Attacks
 6:  FOR attack IN attacks
 7:   IF attack.Rate == 100% THEN
 8:    Insiders.Add(index)
 9:    BREAK
 10:   END_IF
 11:  END_FOR
 12:  model.Reset()
 13: END_FOR_WITH_INDEX
 14: RETURN Insiders
END
```

Алгоритм на вход получает 3 параметра, определяющие психологические особенности сотрудника (Persons) и его окружения (Environment), а также динамику событий (Events) последнего.

В строке 1 по окружению (Environment) с помощью функции BuildModel строится модель (model) психологических атак (attack) на сотрудников организации.

В строке 2 начинается цикл по обходу информации о психологических особенностях каждого сотрудника (person из Persons), с указанием его индекса (index) в списке.

В строке 3 модель настраивается на текущего сотрудника (person) с помощью функции SetPerson.

В строке 4 к модели применяются произошедшие события (Events), позволяя тем самым отслеживать прогресс психологических атак (attack).

В строке 5 из модели возвращается список всех психологических атак (attack), воздействующих на сотрудника (person).

В строке 6 начинается цикл по обходу всех атак (attack из attacks) на текущего сотрудника (person).

В строке 7 проверяется диапазон (Rate) завершения текущей атаки (attack).

В строке 8, в случае завершения атак (attack) на 100% (условие в строке 7), в список инсайдеров (Insiders) с помощью функции Add() заносится

текущий индекс сотрудника (index of person), поскольку он потенциально перешел в разряд потенциальных нарушителей.

В строке 9 происходит выход из цикла по атакам (attacks), поскольку уже установлен факт инсайдерской деятельности текущего сотрудника (person).

В строке 10 завершается условие проверки завершенности атаки, начатое в строке 7.

В строке 11 завершается цикл по атакам, начатый в строке 6.

В строке 12 модель (model) с помощью функции Reset() инициализируется заново, чтобы можно было начать анализ психологического состояния следующего сотрудника (person из Persons).

В строке 13 происходит выход из цикла по сотрудникам (Persons), начатый в строке 2.

В строке 14 происходит выход из тела функции с возвратом индексов (index) всех инсайдеров (Insiders).

Таким образом, принцип работы алгоритма основан на построении общей модели психологических атак, которая считается инвариантной. Затем, для каждого сотрудника модель подстраивается под его особенности, а также производится моделирование психологических атак на основании событий, произошедших в окружении сотрудников. События могут отражать как общие изменения окружающего мира, так и события (в т.ч. и вещи), связанные с жизнью сотрудников компании. В случае если одна из атак достигла своей цели, это означает, что сотрудник потенциально перешел в разряд инсайдеров. Список таких сотрудников-инсайдеров и является результатом работы алгоритма.

Обсуждение результатов

Несмотря на очевидную, как теоретическую, так и практическую значимость проведенного исследования, сами результаты и процесс их получения обладают определенными недостатками.

Так, в работе содержится достаточно небольшое (по научным меркам) количество обзоров релевантных работ по теме комбинирования способов. Как результат, не все сделанные в секции выводы могут считаться до конца обоснованными. Однако это лишний раз подчеркивает новизну и актуальность текущей работы.

Отсутствует строгое обоснование того, что отсутствуют способы, кроме приведенных 7, или же что ни один способ не пересекается с другим. Для проверки (и в т.ч. обоснования) такой классификации можно применить уже упомянутый аппарат категориального деления. Суть аппарата заключается в том, что получаемые классы объектов обладают условием необходимости и достаточности – каждый способ будет отнесен к одному из классов, и может быть отнесен только к одному классу.

Предложенная модель комбинирования способов путем их представления в виде точки в категориальном пространстве может считаться достаточно простой (поскольку вряд ли настолько сложные способы могут быть описаны 3-мя бинарными значениями); тем не менее, это является первым шагом по формализации процесса совместимости и уже дает «строительный материал» для исследования проблем комбинирования способов [19].

Общие принципы комбинирования пар способов осуществлены, исходя из авторской точки зрения, хотя требуют более строгого (и, таким образом, научно обоснованного) подхода. Данная задача является крайне сложной и также требует дополнительного исследования. Так, например, формализация работы каждого способа и процесса их соединения в пару гипотетически позволит формализовать и итоговую комбинацию [20].

Более прагматичной, по сравнению с теоретической оценкой возможности комбинирования способов, основанной на точках в категориальном пространстве, может стать оценка и сравнение каждого из трех следующих показателей эффективности способа [21]: результативности – как меры выявления инсайдеров, оперативности – как длительности или этапа (до, во время или после атаки) их выявления, ресурсоэкономности – как объема затраченных способом ресурсов. Будем это также считать отдельно стоящей крупной задачей оценки, которая планируется к решению авторами в будущих исследованиях.

Авторы более детально описывает комбинацию Способов 1 и 5, которая по их экспертному мнению считается наиболее перспективной с позиции совместимости и величины итогового синергетического эффекта [22], что, безусловно, носит субъективный характер. Однако пример псевдокода для данной комбинации имеет определенную объективную составляющую, поскольку использует формальное описание алгоритма и основывается на строгом базисе категориальных пар.

Таким образом, несмотря на ряд недостатков (основным из которых является низкая степень формализации решений), все они имеют пути устранения.

Заключение

Первым научным результатом работы является модель комбинирования различных способов выявления инсайдеров. Новизна модели заключается в ее частичной формализации в 3-х мерном категориальном, поскольку другие способы комбинирования в основном полагаются на субъективное экспертное мнение.

Вторым научным результатом работы является экспертное и теоретическое комбинирование пар способов, позволившее получить оценки успешности такого комбинирования. Большинство комбинаций способов предложено впервые.

Третьим научным результатом работы является новый комбинированный способ, алгоритм которого задан в виде псевдокода. Аналогично, алгоритм комбинирования способов предложен впервые.

Совокупность полученных новых научных результатов позволяет сделать вывод о достижении цели исследования, а именно – сделан очередной шаг в направлении повышения эффективности противодействия инсайдерам в больших информационных системах за счет комбинаций способов их выявления.

Перспективными направлениями развития результатов настоящей работы авторы считают следующие.

1) Строгое доказательство состоятельности (необходимости и достаточности) декларированных способов выявления инсайдера за счет их классификации, полученной путем категориального деления. Не исключено, что она приведет к их агрегации с секвестрованием количества, или, наоборот – к расширению пула способов.
2) Также с научно-прогностической точки зрения интересным будет оценка возможности комбинирования всех 7 способов по аналогии с их парами. Так, одна координата каждого из способов равна примерно половине таких же координат всех остальных способов, следовательно, комбинирование всех способов имеет, по крайне мере, теоретическую вероятность.
3) Более глубокая формализация работы каждого способа, процесса их сочетания и получаемых комбинированных решений. Это позволит, с одной стороны, использовать при изучении предметной области не только эвристические, но и строго математические методы исследования, а с другой – передать комбинированное решение по выявлению инсайдеров на исполнение автомату (компьютерной программе).
4) Количественная оценка эффективности, как отдельных способов, так и комбинированных решений по критериям результативности, оперативности и ресурсоэкономности. Для этого, скорее всего, потребуется переход от мыслительных к полунатурным или имитационным экспериментам, сопровождаемым разработкой инновационных методик оценки [23].
5) Исследователи в области безопасности часто называют инсайдеров, связанных с облачными вычислениями, серьезной проблемой, но на сегодняшний день эта угроза тщательно не изучена, хотя и «озвучена» [24]. Экстраполяция полученных научных результатов в области выявления инсайдеров в больших информационных системах на цифровую облачную среду позволит по-новому ставить и решать вопросы безопасности, в том числе используя искусственный интеллект [25].

Литература

1. *Минаков С. С. Основные криптографические механизмы защиты данных, передаваемых в облачные сервисы и сети хранения 1. Ponemon Cost of Insider Threats: Global Report, 2023. URL: https://www.dtexsystems.com/resource-ponemon-insider-risks-global-report/ (дата доступа: 02.05.2024)*
2. *Verizon 2023 Data Breach Report: A Bulleted Summary. URL: https://rublon.com/blog/verizon-2023-data-breach-report-summary/ (дата доступа: 02.05.2024)*
3. *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.*
4. *Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders // The proceedings of 4th International Conference on Future Networks and Distributed Systems (New York, USA, 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442619*
5. *Duncan A., Creese S., Goldsmith M. A Combined Attack-Tree and Kill-Chain Approach to Designing Attack-Detection Strategies for Malicious Insiders in Cloud Computing // The proceedings of International Conference on Cyber Security and Protection of Digital Services (Oxford, UK, 2019). IEEE, 2019, PP. 1–9. DOI: 10.1109/CyberSecPODS.2019.8885401*
6. *Kammüller F., Probst C. W. Combining Generated Data Models with Formal Invalidation for Insider Threat Analysis // The proceedings of Security and Privacy Workshops (San Jose, CA, USA, 2014). 2014. PP. 229–235. DOI: 10.1109/SPW.2014.45*
7. *Garfinkel S. L. Beebe N. Liu L. Maasberg M. Detecting threatening insiders with lightweight media forensics // The proceedings of International Conference on Technologies for Homeland Security (Waltham, MA, USA, 2013). IEEE, 2013. PP. 86-92. DOI: 10.1109/THS.2013.6698981*
8. *Liu A. Y., Lam D. N. Using Consensus Clustering for Multi-view Anomaly Detection // The proceedings of Symposium on Security and Privacy Workshops (San Francisco, CA, USA, 2021). IEEE, 2012. PP. 117–124. DOI: 10.1109/SPW.2012.18*
9. *Ackerman D., Mehrpouyan H. Modeling human behavior to anticipate insider attacks via System Dynamics // The proceedings of Symposium on Theory of Modeling and Simulation (Pasadena, CA, USA, 2016). 2016. PP. 1–6. DOI: 10.23919/TMS.2016.7918809*
10. *Sarma M. S., Srinivas Y., Abhiram M., Ullala L., Prasanthi M. S., Rao J. R. Insider Threat Detection with Face Recognition and KNN User Classification // The proceedings of International Conference on Cloud Computing in Emerging Markets (Bangalore, India, 2017), IEEE, 2017. PP.* 39–44, DOI: 10.1109/CCEM.2017.16.
11. *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*
12. *Власов Д. С. Мультикритериальная модель систематизации способов обнаружения инсайдера // Вопросы кибербезопасности. 2024. № 2 (60). С. 66–73. DOI: 10.21681/2311-3456-2024-2-66-73*
13. *Буйневич М. В., Израилов К. Е., Матвеев В. В., Покусов В. В. Способ вариативной классификации уязвимостей в программном коде. Часть 1. Стратификация и категориальное деление // Автоматизация в промышленности. 2021. № 11. С. 42–49. DOI: 10.25728/avtprom.2021.11.09*
14. *Нашивочников Н. В. Выявление отклонений в поведенческих паттернах пользователей корпоративных информационных ресурсов с использованием топологических признаков // Вопросы кибербезопасности. 2023. № 4 (56). С. 12–22. DOI: 10.21681/2311-3456-2023-4-12-22.*

15. *Лебедев Д. В., Васильев Н. В. Метод выделения семантически согласованных групп пользователей социальных медиа-платформ // Техника средств связи. 2021. № 4 (156). С. 20–33.*
16. *Buinevich M., Izrailov K., Vladyko A. Metric of vulnerability at the base of the life cycle of software representations // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. PP. 1–8. URL: https://ieeexplore.ieee.org/document/8323940.*
17. *Buinevich M., Izrailov K., Vladyko A. Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices // The proceedings of 19th International Conference on Advanced Communication Technology (Pyeongchang, South Korea, 2017). IEEE, 2017. PP. 408–414. URL: https://ieeexplore.ieee.org/document/7890122*
18. *Поляничко М. А. Методика обнаружения аномального взаимодействия пользователей с информационными активами для выявления инсайдерской деятельности // Труды учебных заведений связи. 2020. Т. 6. № 1. С. 94–98. DOI: 10.31854/1813-324X-2020-6-1-94-98*
19. *Man D., Wang Y., Yang W., Wang W. A Combined Prediction Method for Network Security Situation // The proceedings of International Conference on Computational Intelligence and Software Engineering (Wuhan, China, 10-12 December 2010). 2010. PP. 1–4. DOI: 10.1109/CISE.2010.5676911*
20. *Lim S.-H., Yun S., Lim J., Yi O. Formalizing the design, evaluation, and analysis of quality of protection in wireless networks // Journal of Communications and Networks(). 2009. Vol. 11. No. 6. PP. 634-644. DOI: 10.1109/JCN.2009.6388417*
21. *Yu J., Oh H., Kim M., Jung S. Unusual Insider Behavior Detection Framework on Enterprise Resource Planning Systems Using Adversarial Recurrent Autoencoder // IEEE Transactions on Industrial Informatics. Vol. 18. No. 3. PP. 1541–1551. DOI: 10.1109/TII.2021.3090362*
22. *Jeridi W., Benabdallah S., Hamdi M., Boudriga N. Dynamic expert weighing for Security Risk Analysis team synergy // The proceedings of Second International Conference on Engineering System Management and Applications (Arab Emirates, 30 March 2010 - 01 April 2010). 2010. PP. 1–8.*
23. *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. 2017. С. 227–228.*
24. *Mescheryakov S., Shchemelinin D., Izrailov K., Pokussov V. Digital cloud environment: present challenges and future forecast // Future Internet. 2020. Vol. 12. Iss. 5. PP. 82. DOI: 10.3390/fi12050082*
25. *Мадиева К. З. Искусственный интеллект и социотехнические угрозы безопасности информации // Журнал высоких гуманитарных технологий. 2024. № 1 (4). С. 38–45.*