# МУЛЬТИКРИТЕРИАЛЬНАЯ МОДЕЛЬ СИСТЕМАТИЗАЦИИ СПОСОБОВ ОБНАРУЖЕНИЯ ИНСАЙДЕРА

*Власов Д. С.*[1]

**DOI:** 10.21681/2311-3456-2024-2-66-73

***Цель исследования:*** *систематизация способов обнаружения инсайдеров в организации для защиты ее информационных ресурсов.*

***Методы исследования:*** *анализ научных публикаций, системный анализ, критериальное сравнение, синтез новых способов.*

***Полученные результаты:*** *сделан обзор научных публикаций со способами обнаружения инсайдеров и выделения в них используемых признаков инсайдера, а также логики и параметров алгоритма обнаружения; произведена систематизация существующих способов обнаружения инсайдеров в таблицу согласно трем критериями признаков нарушителя и двум критериям алгоритмов обнаружения; синтезированы потенциально новые способы обнаружения.*

***Научная новизна*** *работы определяется сбором и сведением всех существующих способов обнаружения инсайдера в единый список, а также получением оригинальной совокупности критериев, подходящей для идентификации каждого из способов.*

***Ключевые слова:*** *информационная безопасность, организация, инсайдер, способы обнаружения, мультикритериальная модель.*

# MULTICRITERIA MODEL FOR SYSTEMATIZING METHODS FOR DETECTING AN INSIDER

*Vlasov D. S.*[2]

***The goal of the investigation:*** *systematization of methods for detecting insiders in an organization to protect its information resources.*

***Research methods:*** *analysis of scientific publications, system analysis, criterion comparison, synthesis of new methods.*

***Results:*** *a review of scientific publications was made with methods for detecting insiders and highlighting the insider features used in them, as well as the logic and parameters of the detection algorithm; existing methods for detecting insiders were systematized into a table according to three criteria for signs of an intruder and two criteria for detection algorithms; Potentially new detection methods have been synthesized.*

***The scientific novelty*** *of the work is determined by collecting and combining all existing methods of identifying an insider into a single list, as well as obtaining an original set of criteria suitable for identifying each of the methods.*

***Keywords:*** *information security, organization, insider, detection methods, multi-criteria model.*

## Введение

Противодействие информационным угрозам в любой организации является основной миссией специалистов по защите информации и осуществляется по-разному в различных плоскостях в зависимости от направления (вектора) атак на ее ресурсы. Одной из такой плоскостей является сфера деятельности сотрудников самой организации, которые в этом случае выступают в качестве потенциальных инсайдеров. Особенность последних, упрощающая проведение атак, заключается в нахождении нарушителей уже внутри охраняемого периметра вследствие выполнения своих должностных обязанностей [1]. Обнаружение же инсайдеров (с последующим их контролированием и недопущением реализации

1 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

2 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

угроз) является одной из актуальнейших задач обеспечения информационной безопасности ресурсов любой организации.

Однако при анализе Best Practices по ее решению обнаруживается следующее научное противоречие. С одной стороны, требуется применение всего спектра возможных способов обнаружения инсайдера (включая достижения в области машинного обучения [2]), поскольку инсайдер является не простой уязвимостью в программной системе (зачастую, хорошо формализуемой [3, 4]), а представляет собой сложную разумную сущность с интеллектуальными подходами и множеством вариативных действий для проведения атак и своей маскировки под легальных сотрудников [5]. С другой стороны, существующие (по крайне мере те, которые были найдены автором) способы не охватывают весь возможный спектр, поскольку созданы без использования системного подхода – эволюционно, на основании экспертных мнений, с перекрыванием и/или пропуском функционалов, учитывая при этом не все многогранные признаки инсайдера [6].

В качестве частичного разрешения данного противоречия, а точнее, первого шага на пути к этому, далее будет произведен обзор существующих способов обнаружения инсайдеров, в которых будут выделены основополагающие элементы (как некоторые критерии), которые лягут в основу единой модели систематизации всех возможных способов. Тем самым модель отразит не только существующие из них, но еще и позволит спрогнозировать, а в перспективе и синтезировать потенциально новые. Тем самым будет сформирован весь спектр способов, являющийся «краеугольным камнем» существования вышеупомянутого противоречия.

### Обзор способов

Произведем аналитический обзор 10 способов обнаружения инсайдеров, как составленных автором ранее (первые 7) на основании опубликованной работы [7], так и дополненных им в текущем исследовании (последние 3). Также, в котором будем кратко указывать следующие их свойства:

- признак (инсайдера), отражающий особенности сотрудника, которые используются для обнаружения в нем нарушителя;
- логика (алгоритма метода), указывающая основные шаги его работы;
- параметр (алгоритма метода), задающий особенности его применения.

Таким образом, каждый способ можно описать по следующему шаблону: «Способ работает по [Логике], настраивается заданными ему [Параметрами] и оперирует [Признаками] сотрудника».

**Способ_1. Анализ событий в реальной жизни**

Способ заключается в анализе поведения сотрудников организации в среде, отличной от информационной (обусловленной сетевыми потоками, программными сбоями, DoS-атаками и т.п.) – т.е. в реальной жизни [8]. В частности, переход между событиями определяется различными возникающими факторами. Так, если у сотрудника резко ухудшилось финансовое благополучие, то он может перейти из нормального состояния в то, когда ему потребуется дополнительный заработок, что очевидно, может «сподвигнуть» его к краже корпоративных секретов для продажи.

Признаки: связанные с сотрудником основные события (внутри организации и за ее пределами);

Логика: сбор событий, переходы между состояниями, сравнение с инсайдерскими;

Параметры: заданные правила переходов между состояниями, их отнесение к инсайдерским.

**Способ_2. Выявление аномалий в типовых сценариях работы сотрудника**

Способ заключается в выявлении аномальных действий сотрудников или продуцируемых ими событий, происходящих в организации [9]. Для этого, в частности, может осуществляться сравнение деятельности сотрудников с типовыми (т.е. безопасными) профилями поведения, которые могут строиться как автоматическими, так и экспертными методами. Так, если в некоторый момент времени сотрудник стал осуществлять доступ к информации, которая для других сотрудников на такой же должности не была «интересна», то, возможно, он стремится совершить с ней незаконные действия.

Признаки: связанные с сотрудником основные события в организации;

Логика: выявление аномалий;

Параметры: типовые профили (автоматические или экспертные).

**Способ_3. Фиксирование накопления критичной конфиденциальной информации**

Способ заключается в отслеживании осведомленности сотрудников с некоторым множеством информации, совокупность которой позволит получить из нее качественно новые знания [10]. Т.е. в организациях может существовать критический объем информации (включающий как количественную, так и качественную меру), обладание которой будет считаться потенциальной утечкой. Например, само по себе знание фамилий всех сотрудников и безымянного перечня их сотовых телефонов не так критично, как если оно будет дополнено сопоставлением элементов этих списков (т.е. с каждым сотрудником будет ассоциирован его телефон).

Признаки: собранная сотрудником информация в организации;

Логика: сравнение собранной информации с критической;

Параметры: критическая количественно/качественная мера информации.

**Способ_4. Ловля на живца («Honeypot»)**

Способ заключается в размещении в защищаемой информационной системе так называемых муляжей, по внешним признакам совпадающими с целями инсайдеров [11]; в частности, муляжи могут иметь разную природу – от простых документов до целых подсетей. В результате, злоумышленник потратит часть своих ресурсов на бесполезный для него информационный ресурс (или содержащую его информационную систему), при этом, в случае успешности такой «псевдо-атаки», выявит свое присутствие.

Признаки: попытка доступа сотрудником к информационному ресурсу организации;

Логика: отслеживание факта попытки доступа к муляжу;

Параметры: муляж информационного ресурса или системы.

**Способ_5. Обнаружение инсайдера психодиагностическими методами**

Способ заключается в тестировании сотрудников психологическими и иными инструментами, что позволит выявить если не самих инсайдеров, то тех, кто потенциально может ими стать [12]. В частности, результаты такого тестирования при поступлении на работу позволят выбрать наиболее подходящие должности кандидату, исходя не только из эффективности его работы, но и снижая вероятность последующих информационных угроз. Например, если будущий сотрудник является слабохарактерным, однако обладает навыками взлома компьютерных систем (что может быть актуально при проведении пентеста), то под воздействием внешнего влияния он может совершить взлом системы доступа к информационным ресурсам изнутри компании.

Признаки: психологические аспекты сотрудника;

Логика: сравнивает результаты теста с шаблоном, характерным для инсайдера;

Параметры: психодиагностические и прочие тесты.

**Способ_6. Анализ защищенности сотрудника от социальных атак**

Способ заключается в установлении, прогнозировании и анализе социальных связей между сотрудниками организации с целью обнаружения потенциальных инсайдеров (в особенности, неумышленных), на которых могут быть направлены социальные (или близких к ним) атаки [13]. Так, например, тесность связей администратора сети с сотрудниками, не обладающими особыми знаниями в области информационных технологий, позволит последним «по дружбе» получить доступ к конфиденциальной информации в компании и уже потом «по глупости» предоставить ее реальному злоумышленнику. В этом случае, оба сотрудника могут являться косвенными инсайдерами, даже не осознавая этого.

Признаки: социальные связи сотрудника (внутри организации и за ее пределами);

Логика: прогнозирование возможных манипуляций по модели;

Параметры: модель взаимоотношений сотрудников.

**Способ_7. Оценка потенциала сотрудника для реализации атаки**

Способ заключается в комплексной оценке возможностей сотрудников по проведению внутренних атак на информационную систему или ресурсы организации [14]. При этом учитываются как умения и знания самих сотрудников (т.е. их компетенции в области «хакинга»), а также их личностные характеристики, так и рабочее окружение, такое, как занимаемая должность, круг общения, доступ к данным и т.п. Например, сотрудник с богатым опытом в области взлома компьютерных систем, обладающий «показушными» наклонностями и находясь на должности, связанной с системным администрированием, может ради демонстрации своих умений друзьям взломать защищаемые информационные ресурсы организации изнутри и совершить неправомерные действия.

Признаки: умения, знания, личностная характеристика сотрудника;

Логика: сравнивает результаты теста с шаблоном, характерным для инсайдера;

Параметры: компетентностные и личностные тесты, сведения о занимаемой должности.

**Способ_8. Выявление фактов сговора сотрудников**

Способ ориентирован на инсайдерскую деятельность со стороны нескольких сотрудников, имеющих доступ к раздельным частям информационных ресурсов организации (в рамках должностных обязанностей или отдельных рабочих сессий). При этом обладание полным набором этих частей как раз и является целью деятельности. Данная ситуация характерна для банковской сферы, в которой один менеджер имеет доступ к данным клиентов для авторизации транзакций, а другой – к данным счетов и переводов. Так, несмотря на то, что согласно типовым политикам информационной безопасности (далее – ИБ) доступ одного менеджера ко всей такой информации запрещен, вследствие сговора она может быть собрана и использована в злонамеренных

целях. Для реализации способа могут применяться методы кластеризации и математической статистики [15].

Признаки: собранная группой сотрудников информация в организации;

Логика: определение степени накопления информации комбинациями сотрудников;

Параметры: критическая количественно/качественная мера информации, логика многопользовательской работы с информацией.

**Способ_9. Интеллектуальный анализ Big Data со сведениями о сотрудниках**

Способ частично повторяет (а точнее компенсирует) другие, поскольку предлагает анализ большого числа гетерогенных сведений о сотруднике (из реальной жизни, с места работы, из психологического портрета и т.п.) с помощью моделей и методов машинного обучения. Так, интеллектуальный анализ огромного потока операций с внутренним хранилищем компании позволит среди сотрудников (при этом, относящихся к разряду неблагонадежных) выявить тех, кто осуществляет инсайдерскую деятельность; особенностью способа будет то, что он способен учитывать небольшие отклонения от типового поведения, комбинация которых как раз и будет признаком злонамеренных действий [16]. Например, если из всех сотрудников только один дольше задерживался на работе, запрашивал больше излишней информации, реже участвовал в тимбилдингах, чаще высказывал недовольство руководством, то именно он может оказаться инсайдером.

Признаки: множество связанных с сотрудником частных событий (внутри организации и за ее пределами);

Логика: применение машинного обучения для классификации и «аномализации» инсайдерской деятельности;

Параметры: обучающая выборка действий легальных сотрудников, настройки параметров моделей машинного обучения.

**Способ_10. Аномальное изменение в темпоральном профиле сотрудника**

В отличие от Способа 2, данный основан не на сравнении профиля сотрудника с типовыми, а отслеживает изменение профиля одного инсайдера на предмет его аномальности [17]. Таким образом, профиль должен постоянно обновляться (т.е. быть темпоральным, имеющим временные метки), а его изменения анализироваться экспертными или интеллектуальными правилами на предмет «неестественной» активности. Например, если сотрудник постепенно увеличивал заинтересованность во внутренних документах организации (что можно определить по временному изменению его профиля, составленного по активности работы с внутренней базой данных), а затем его интерес за предыдущий отрезок времени вырос в несколько раз, то, возможно, что именно в этот момент у него проявилась инсайдерская деятельность (или же его аккаунт был взломан).

Признаки: действия и события сотрудника в организации;

Логика: построение профилей за промежутки времени и выявление в них аномальных изменений;

Параметры: параметры темпоральных профилей.

Следуя сделанным обзорам, уже сейчас можно выявить то, что часть результатов в них достаточно близка друг к другу; так, например, тестирование в 5-м и 7-м способах в том числе оценивает личностные характеристики сотрудников, а анализ данных в 9-м способе лишь интеллектуализирует 10-й способ, а также явно указывает на работу с Big Data.

### Модель систематизации способов обнаружения инсайдера

В интересах систематизации всех существующих (а точнее найденных в научных публикациях) способов [18] выделим 5 следующих их критериев, первые 3 из которых относятся к признакам инсайдера (начинаются с аббревиатуры «КП», от Критерий Признака), а последние 2 – к алгоритмам способа (начинаются с аббревиатуры «КА», от Критерий Алгоритма):

а) КП_1 – Признак с позиции учета в нем временных изменений (его темпоральность): **С**татический (т.е. разовое или постоянное значение) или **Д**инамический (т.е. согласно изменению значения);

б) КП_2 – Признак с позиции отражения в нем взаимоотношений с другими людьми (т.е. его социальность): **П**ерсональный (т.е. отражающий особенности одного человека) или **О**бщественный (т.е. учитывающий особенности взаимодействий человека с окружающими);

в) КП_3 – Признак с позиции учета в нем специфики организации (его специализация): **Ч**астный (т.е. определяемый конкретной организацией) или **Г**лобальный (т.е. не зависящий от организации);

г) КА_1 – Алгоритм с позиции соотношения признаков сотрудника с известными данными (предопределенность его шаблонов): **К**лассификация (т.е. сравнение с известными классами) или **А**номализация (т.е. определение отклонений от нормы);

д) КА_2 – Алгоритм с позиции возможности точного обнаружения инсайдера (его надежность): **З**аконы (т.е. строгое сравнение с конкретными значениями) или **В**ероятность (т.е. нестрогое использование статистических данных).

Таким образом, по каждому критерию любой способ может принимать одно из двух альтернативных значений – т.е. производится бинарное разбиение. Систематизация всех возможных способов, определяемые комбинацией значений их критериев, общим числом $2^5 = 32$ приведена в Таблице. Для лучшей понятности записи, заголовок каждого столбца (из последних) для критерия записан с помощью вариации первых букв его значений (которые выше были указаны с прописной буквы жирным шрифтом) через символ «/», т.е. КП_1 – «С/Д», КП_2 – «П/О», КП_3 – «Ч/Г», КА_1 – «К/А», КА_2 – «З/В»; ячейка таблицы с зеленым фоном соответствует первому значению критерия, с белым – второму.

В Таблице, помимо 1-го столбца с нумерацией комбинаций критериев, присутствует столбец «Способы» с 3 следующими подзаголовками и содержащимися в столбцах элементах: «Существующие» – способы из 10 рассмотренных выше комбинаций критериев (ячейки с синим фоном); «Расширенные» – возможное и достаточно логичное первоочередное развитие способов путем соответствия новым критериям (ячейки также с синим фоном, значения с префиксом «*» к базовому способу); «Новые» – те способы, которые ранее не применялись и не имеют очевидного получения из существующих (ячейки с желтым фоном, значения с номером способа после префикса «N»). Используя введенные сокращения столбцов для критериев, каждый из способов может кодироваться с помощью последовательности 5 битов или что более читаемо – 5-ю буквами по первым значениям критериев (которые изначально были выбраны не совпадающими друг с другом); например, Способ_4 имеет код [ДПЧКЗ].

Согласно вышеизложенному, таблица представляет собой общую мультикритериальную модель систематизации способов обнаружения инсайдера, состоящую из двух частных – модели классификации признаков инсайдера (критерии КП_1, КП_2 и КП_3) и модели классификации алгоритмов его обнаружения (критерии КА_1 и КА_2).

Проанализируем полученную систематизацию способов обнаружения инсайдера.

Во-первых, количество комбинаций критериев, которым соответствует более одного способа, равно 4, что достаточно логично, поскольку способы являются пересекающимися или входящими друг в друга, а отличия носят частный характер; например, Способ_5 близок к Способу_7, поскольку в обоих производится тестирование особенностей и способностей сотрудников с точки зрения ИБ для организации, определяя при этом тех, кто подходит под заранее заданные шаблоны инсайдера.

Во-вторых, непосредственно существующие способы соответствуют 11 комбинациям критериев, что составляет $\frac{11}{32} = 34\%$ от общего числа вариантов. Таким образом, существующие способы (а точнее, их некоторые реализации) в явном виде составляют треть из всех возможных.

В-третьих, логичное развитие способов увеличивает количество задействованных комбинаций до 21, что составляет $\frac{21}{32} = 66\%$ – или две трети.

В-четвертых, следуя из предыдущего вывода, количество принципиально новых и неприменяемых ранее способов составляет 11 или 34% – или треть.

Общий вывод, который можно сделать из анализа Таблицы, заключается в достаточной точности полученной модели, поскольку 2/3 существующих и логично развиваемых способов могут быть отнесены к одной или нескольким комбинациям критериев.

Поскольку новые (т.е., по сути, синтезированные из модели) способы являются достаточно важным с научной и практической точки зрения результатом решения задачи обнаружения инсайдеров, дадим краткую интерпретацию каждого из них и приведем пример обнаруженных нарушителей. При этом комбинацию значений признаков КП_2 и КП_3 – «Персональный + Частный» и «Персональный + Глобальный» будем интерпретировать следующим образом. Первая комбинация отражает персональные особенности и возможности сотрудника, определяемые организацией – т.е. в соответствии с ее внутренними требованиями, которые будем называть корпоративными стандартами. Вторая же комбинация отражает аналогичные особенности и возможности сотрудника, но существующие и без организации – т.е. в соответствии с инвариантными к ней требованиями, которые будем называть общепринятыми стандартами.

Способ_N1 [СПЧКВ] – вероятностное отнесение результатов тестирования сотрудника по корпоративным стандартам к шаблону, считающемуся небезопасным; например, нахождение сотрудника на низкооплачиваемой должности, критичное отношение к руководству и проявление слабохарактерности согласно статистике организации может привести к вандализму в отношении внутренних информационных ресурсов без какой-либо его коммерческой выгоды;

Способ_N2 [СПЧАЗ] – строгое превышение результатов тестирования сотрудника по корпоративным стандартам предельных значений, говорящее о его подверженности инсайдерской деятельности; например, недостаточное количество участий сотрудника в корпоративах и тимбилдингах (т.е. слабая сплоченность с коллективом [19]) при чрезмерном (т.е. сверх меры) общении с внешними партнерами (т.е. с потенциальными конкурентами) может

*Таблица*

*Мультикритериальная модель систематизации способов обнаружения инсайдера*

| № | Способы | | | Критерии и их альтернативные значения | | | | |
|---|---|---|---|---|---|---|---|---|
| | Существующие | Расширенные | Новые | КП_1 | КП_2 | КП_3 | КА_1 | КА_2 |
| | | | | С/Д | П/О | Ч/Г | К/А | З/В |
| 1 | Способ_7 | | | С | П | Ч | К | З |
| 2 | | | Способ_N1 | С | П | Ч | К | В |
| 3 | | | Способ_N2 | С | П | Ч | А | З |
| 4 | | | Способ_N3 | С | П | Ч | А | В |
| 5 | Способ_5<br>Способ_7 | | | С | П | Г | К | З |
| 6 | | | Способ_N4 | С | П | Г | К | В |
| 7 | | Способ_5* | | С | П | Г | А | З |
| 8 | | | Способ_N5 | С | П | Г | А | В |
| 9 | Способ_6 | Способ_7* | | С | О | Ч | К | З |
| 10 | | | Способ_N6 | С | О | Ч | К | В |
| 11 | | Способ_6* | | С | О | Ч | А | З |
| 12 | | | Способ_N7 | С | О | Ч | А | В |
| 13 | Способ_6 | Способ_7* | | С | О | Г | К | З |
| 14 | | | Способ_N8 | С | О | Г | К | В |
| 15 | | Способ_6* | | С | О | Г | А | З |
| 16 | | | Способ_N9 | С | О | Г | А | В |
| 17 | Способ_1<br>Способ_3<br>Способ_4 | | | Д | П | Ч | К | З |
| 18 | Способ_9 | Способ_3* | | Д | П | Ч | К | В |
| 19 | Способ_2<br>Способ_3<br>Способ_10 | Способ_1* | | Д | П | Ч | А | З |
| 20 | Способ_9<br>Способ_10 | Способ_2*<br>Способ_3* | | Д | П | Ч | А | В |
| 21 | Способ_1 | | | Д | П | Г | К | З |
| 22 | | Способ_9* | | Д | П | Г | К | В |
| 23 | | Способ_1*<br>Способ_2* | | Д | П | Г | А | З |
| 24 | | Способ_2*<br>Способ_9* | | Д | П | Г | А | В |
| 25 | Способ_8 | Способ_4* | | Д | О | Ч | К | З |
| 26 | | Способ_8* | | Д | О | Ч | К | В |
| 27 | Способ_8 | Способ_10* | | Д | О | Ч | А | З |
| 28 | | Способ_8*<br>Способ_10* | | Д | О | Ч | А | В |
| 29 | | | Способ_N10 | Д | О | Г | К | З |
| 30 | | | Способ_N11 | Д | О | Г | К | В |
| 31 | | Способ_10* | | Д | О | Г | А | З |
| 32 | | Способ_10* | | Д | О | Г | А | В |

DOI: 10.21681/2311-3456-2024-2-66-73

привести к его переходу в другую организацию с кражей коммерческой информации;

Способ_N3 [СПЧАВ] – вероятностный выход результатов тестирования сотрудника по корпоративным стандартам из допустимых значений, говорящий о его подверженности инсайдерской деятельности; например, непризнание сотрудником важности защиты коммерческой тайны организации при наличии аномально высоких оценок в тестах на должность пентестера согласно статистике организации может привести к взлому и краже внутренних информационных ресурсов;

Способ_N4 [СПГКВ] – вероятностное отнесение результатов тестирования сотрудника по корпоративным стандартам к шаблону, считающемуся небезопасным; например, сотрудник с низкой ИБ-грамотностью и необходимостью работать удаленно (в частности, по состоянию здоровья) статистически может быть отнесен к группе людей, через плохо защищенный (по небрежности, безграмотности и т.п.) VPN-доступ которых реальный нарушитель сможет проникнуть во внутреннюю сеть организации.

Способ_N5 [СПГАВ] – вероятностный выход результатов тестирования сотрудника по корпоративным стандартам из допустимых значений, говорящий о его подверженности инсайдерской деятельности; например, полное отсутствие у сотрудника ИБ-грамотности при синдроме трудоголика с большой вероятностью приведет к утечке конфиденциальных данных (поскольку, будет стремление к работе с информацией организации при непонимании потребности и возможности обеспечения ее безопасности).

Способ_N6 [СОЧКВ] – вероятностное отнесение результатов тестирования сотрудника по взаимодействию с коллегами к шаблону, считающемуся небезопасным; например, наличие близких знакомств сотрудника как с коллегами из числа админов (т.е. ответственными за управления правами доступа), так и с новыми сотрудниками (среди которых могут быть «шпионы» от конкурентов), может, следуя статистике, отнести его к неблагонадежному промежуточному звену коммуникации, поскольку это позволит использовать его для проведения социальных атак.

Способ_N7 [СОЧАВ] – вероятностный выход результатов тестирования сотрудника по взаимодействию с коллегами из допустимых значений, говорящий о его подверженности инсайдерской деятельности; например, нахождение сотрудника на низкооплачиваемой должности (т.е. не замотивированный для процветания организации) при близких родственных отношениях с менеджером высшего звена (т.е. ставшего частью и продолжателем идей организации), может привести к проведению им социальной атаки для получения несанкционированного доступа к информационным ресурсам для их кражи или самоутверждения.

Способ_N8 [СОГКВ] – вероятностное отнесение результатов тестирования сотрудника по взаимодействию с окружающим социумом (вне организации) к шаблону, считающемуся небезопасным; например, высокая степень социальной связи сотрудника с людьми, связанными с зарубежными организациями (например, по информации из анкеты о родственниках и предыдущих местах работы), в ряде государственных служб может привести к его отнесению к потенциальному шпиону из-за возможности проведения внутренних атак по заказу спецслужб иностранных государств.

Способ_N9 [СОГАВ] – вероятностный выход результатов тестирования сотрудника по взаимодействию с окружающим социумом (вне организации) из допустимых значений, говорящий о его подверженности инсайдерской деятельности; например, существенная «неприживчивость» в других организациях (следуя предыдущим местам работы) при сильнейшем желании выделиться среди окружающих (согласно наличию и содержимому его аккаунтов из социальных сетей) может привести к уничтожению конфиденциальной информации в организации с целью получения славы или «хайпа» (эффект Герострата).

Способ_N10 [ДОГКЗ] – строгое отнесение результатов анализа поведения сотрудника в социуме к шаблону, считающемуся небезопасным; например, заведение сотрудником за короткий промежуток времени профессиональных контактов с маргинальными специалистами по взлому, а также обращение в молодежных компаниях, связанных с употреблением наркотических средств, отнесет его к группе «неблагонадежных хакеров», что в конечном итоге может привести к появлению наркотической зависимости и необходимости взлома защиты организации изнутри для кражи и продажи коммерческой информации или самоутверждения.

Способ_N11 [ДОГКВ] – вероятностное отнесение результатов анализа поведения сотрудника в социуме к шаблону, считающемуся небезопасным; например, заведение сотрудником дружеских, профессиональных и иных контактов с вступлением в различные субкультуры (в том числе, связанные с информационными технологиями, такие, как «Фидонет» [20]), комбинация которых согласно статистике правонарушений приводит к осуществлению компьютерных преступлений, в организации может трактоваться как крайне неблагонадежный фактор для устройства на некоторые должности.

Интерпретация новых 11 способов, сопровождаемая примерами обнаружения (потенциальных) инсайдеров, позволяет сделать вывод, что все они как имеют право на существование в реальной практике, так и являются лишь дополнительным развитием существующих.

### Заключение

Работа посвящена задаче обнаружения инсайдеров в организации с защищаемыми информационными ресурсами. Для этого опубликованный ранее [7] список из 7 способов обнаружения актуализирован – дополнен еще 3; в каждом обзоре используемый признак инсайдера, логика обнаружения и ее параметры. Исходя из этого, получены критерии, определяющие каждый из способов и его вариации.

Основным научным результатом работы является мультикритериальная модель систематизации способов обнаружения (в виде матрицы или таблицы), состоящая из подмоделей признаков инсайдера и алгоритма его обнаружения.

Теоретическая значимость исследования заключается в систематизации всех способов обнаружения инсайдера в единую табличную модель.

Практическая значимость состоит в возможности синтезировать новые способы (общим количеством 11), имеющие иную (гипотетические более высокую) эффективность по сравнению с существующими (за счет использования новых комбинаций факторов).

Продолжением работы должно стать объединение всех способов в единый (на базе полученной модели), работающий со всеми признаками инсайдера и согласованно применяющий весь спектр алгоритмов его обнаружения.

### Литература


1. *Корниенко С. В., Пантюхина А. В. Методика выявления потенциальных внутренних нарушителей информационной безопасности // Интеллектуальные технологии на транспорте. 2023. № 2 (34). С. 50–57. DOI: 10.24412/2413-2527-2023-234-50-57.*
2. *Стрижков В. А. Применение методов машинного обучения для противодействия инсайдерской угрозе информационной безопасности // Вопросы безопасности. 2023. № 4. С. 152–165. DOI: 10.25136/2409-7543.2023.4.68856.*
3. *Израилов К. Е. Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 1. Схема жизненного цикла // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 75–93. DOI:10.31854/1813-324X-2023-9-1-75-93.*
4. *Израилов К. Е. Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 2. Аналитическая модель и эксперимент // Труды учебных заведений связи. 2023. Т. 9. № 2. С. 95–111. DOI:10.31854/1813-324X-2023-9-2-95-111.*
5. *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.*
6. *Буйневич М. В., Власов Д. С. Аналитическим обзор моделей инсайдеров информационных систем // Информатизация и связь. 2020. № 6. С. 92–98.*
7. *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*
8. *Бычков И. В., Веденеев В. С. Алгоритмы поиска инсайдеров в корпоративных компьютерных системах // Информация и безопасность. 2013. Т. 16. № 2. С. 179–184.*
9. *Denning D. An Intrusion Detection Model // IEEE Transactions on Software Engineering. 1987. V. SE-13. № 1. Pp. 222–232.*
10. *Мартьянов Е. А. Возможность выявления инсайдера статистическими методами // Системы и средства информатики. 2017. Т. 27. № 2. С. 41–47. DOI: 10.14357/08696527170204*
11. *Веденеев В. С., Бычков И. В. Средства поиска инсайдеров в корпоративных информационных системах // Безопасность информационных технологий. 2014. Т. 21. № 1. С. 9–13*
12. *Белов С. В., Садыкова У. В. Разработка информационной системы выявления потенциальных нарушителей информационной безопасности на основе психодиагностических методик // Научные труды Кубанского государственного технологического университета. 2018. № 3. С. 106–115.*
13. *Абрамов М. В., Азаров А. А., Фильченков А. А. Распространение социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей // Международная конференция по мягким вычислениям и измерениям. 2015. Т. 1. С. 329–331.*
14. *Сычев В. М. Формализация модели внутреннего нарушителя информационной безопасности // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия: Приборостроение. 2015. № 2 (101). С. 92–106.*
15. *Грушо А. А., Забежайло М. И., Смирнов Д. В., Тимонина Е. Е., Шоргин С. Я. Методы математической статистики в задаче поиска инсайдера // Информатика и ее применения. 2020. Т. 14. № 3. С. 71–75. 10.14357/19922264200310.*
16. *Смирнов Д. В. Методы поиска признаков инсайдера в Big Data: : дис. ... канд. техн. наук: 05.13.19. Москва, 2021.144 с.*
17. *Быстров И. С., Котенко И. В. Классификация подходов к построению моделей поведения пользователей для задачи обнаружения кибер-инсайдеров // Информационная безопасность регионов России (ИБРР-2021): материалы XII Санкт-Петербургской межрегиональной конференции (Санкт-Петербург, 27–29 ноября 2021 года). 2021. С. 70–72.*
18. *Власов Д. С. Анализ и систематизация инсайдерских угроз в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021): сборник научных статей (Санкт-Петербург, 24-25 февраля 2021 года). Т. 4. 2021. С. 399–403.*
19. *Гладышев П. С. Тимбилдинг как эффективный инструмент в управлении трудовой адаптацией в организации // Психология человека и общества. 2020. № 2 (19). С. 5–9.*
20. *Гребенкина А. Ю. Суть и значение локальных и глобальных компьютерных сетей // Научные исследования XXI века. 2023. № 2 (22). С. 27–29.*