УДК 004.6

Применение категориального деления для классификации мотивации инсайдерской деятельности

Власов Д. С.

Главное управление МЧС России по г. Санкт-Петербургу
Санкт-Петербург, 190000, Российская Федерация

***Постановка задачи**: выявление инсайдерской деятельности в организациях, приводящей к угрозам информационной безопасности, одним из первых шагов чего должно стать изучение мотивации, толкающей сотрудников к неправомерным действиям. **Целью работы** является синтез основных классов мотиваций инсайдеров; при этом они должны охватить всевозможные ситуации, а каждый из классов не должен пересекаться с другими. **Используемые методы**: категориальное деление для выделения классов и их практическое обоснование. **Новизна**: в отличие от существующих мотиваций инсайдеров, предложенная классификация соответствует критериям необходимости и достаточности, являясь тем самым изначально непротиворечивой и охватывая все случаи; при этом классы получены теоретически с применением строгой логики категориального деления. **Результат**: применение категориального деления выделило 3 пары категорий (Внутренний vs Внешний, Физический vs Психоэмоциональный, Польза или Благонамеренность vs Вред или Злонамеренность), что позволило сформировать по их комбинациям 8 уникальных классов мотиваций инсайдеров; приведена форма записи идентификаторов класса. Существование каждого из классов подтверждается наличием соответствующей ему публикации. **Теоретическая/практическая значимость**: получен соответствующий критериям необходимости и достаточности единый набор классов мотиваций инсайдеров, которые могут быть использованы для понимания причин такой неправомерной деятельности и, следовательно, для создания эффективных способов противодействия.*

***Ключевые слова:** информационная безопасность, инсайдер, организация, мотивация*

Введение

Любая организация, обладающая информационной системой, требует соответствующих мер защиты, направленных на препятствование нарушению конфиденциальности, целостности и доступности информации [1–7]. И если противодействие атакам (прямым и косвенным) по физическим или информационным каналам и имеет множество решений, то каналы, связанные с неправомерной деятельностью сотрудников (в этом случае называемых инсайдерами [8–12]) зачастую оставлены практически без внимания. Одной из причин этого является сложность прогнозирования поведения людей вследствие отсутствия сведений касательно их внутренних предпосылок к совершению тех или иных действий. Так, например, один сотрудник из-за финансовых трудностей может осуществить кражу и продажу коммерческой информации конкурирующей организации – нарушив ее конфиденциальность. Другой сотрудник может почув-

Библиографическая ссылка на статью:
Власов Д. С. Применение категориального деления для классификации мотивации инсайдерской деятельности // Информационные технологии и телекоммуникации. 2023. Т. 11. № 2. С. 47–56. DOI: 10.31854/2307-1303-2023-11-2-47-56

Reference for citation:
Vlasov D. Application of Categorical Division to Classify Motivation for Insider Activities. *Telecom IT*. 2023. Vol. 11. Iss. 2. PP. 47–56 (in Russian). DOI: 10.31854/2307-1303-2023-11-2-47-56

ствовать себя обиженным на руководство и сознательно испортить критически важные для компании данные – нарушив их целостность. Третий же сотрудник может выйти на работу сверхурочно и в результате перенапряжения удалить документ с важной информацией из-за банальной невнимательности – нарушив доступность данных в нем. Все три примера объединяет одно важное свойство – источником атаки стали сотрудники, изначально находящиеся внутри защищаемого периметра организации. Также можно сравнить проведенные атаки с позиции категориальной пары «субъект vs объект». Так, первый элемент пары, являясь разумным человеком, совершает свои шаги на основании заложенной в него мотивации – важнейшей характеристики любого сотрудника организации, толкающего его на совершение действий (в том числе и приступных) [13–15]. Второй же элемент пары, т. е. бессознательный автомат, действует согласно заданным правилам (хотя и зачастую заложенным другим человеком); отметим, что безопасность такого рода атак является отдельной областью исследования [16–18]. Все вышесказанное актуализирует необходимость понимания различных источников неправомерной деятельности сотрудников – т. е. их *мотивации*, первым шагом чего может быть непротиворечивая классификация таких источников. Как результат, это позволит разделить всех внутренних нарушителей на группы и выработать для них соответствующие способы обнаружения и противодействия.

Также, в случае теоретического выделения классов, каждый из них целесообразно обосновать с помощью корректной интерпретации и практические примеры; все это и будет осуществлено в статье далее.

Классы мотиваций

На авторский взгляд, одна из основных сложностей существующих классификаций инсайдеров и их характеристик заключается в несоответствии принципам, которые можно назвать как необходимость и достаточность деления [19]. Первая их часть утверждает о том, что выбрано необходимое количество классов – т. е. характеристика каждого инсайдера, относящаяся к некоторому классу, не может относиться к другому. Вторая же часть утверждает о том, что выбрано достаточное количество классов – т. е. характеристика любого инсайдера обязательно должна быть отнесена хотя бы к одному из классов. Совместное выполнение обеих частей приведет к гарантированному и однозначному отнесению мотивации инсайдера ровно к одному существующему классу.

Для получения классификации, удовлетворяющей принципам необходимости и достаточности, в ряде случаев оправданным оказывается применение категориального деления [20], суть которого заключается в следующем. Поскольку большое гетерогенное множество полностью поделить на близкие по мощности (или объему) подмножества (в нашем случае – классы мотивации инсайдеров) является не всегда тривиальной задачей, то имеет смысл производить постепенное деление множества на 2 части – по так называемой категориальной паре, каждая из которых с некоторой точки зрения является антагонистом к другой – например, как Положительный vs Отрицательный, Статический

vs Динамический, Человек vs Автомат и т. п. Выполнив одновременно N подобных делений, будет получено N пар, объединение элементов которых даст 2^N делений всего множества на непересекаемые подмножества – т. е. будет получена искомая классификация.

В интересах получения классов мотивации инсайдеров были выбраны следующие категориальные пары и их интерпретации (в скобках даны англоязычные термины для использования в будущих сокращениях):

а) Внутренний (*перев. на англ.* Internal) vs Внешний (*перев. на англ.* External) – расположение начальной точки (причины) мотивации, побудившей сотрудника на некоторые действия (по внутренним причинам человека или из-за внешних факторов);

б) Физический (*перев. на англ.* Physical) vs Психоэмоциональный (*перев. на англ.* Psycho-emotional) – расположение конечной точки (цели), на достижение которой направлена мотивация сотрудника (объект реального мира или лишь осознаваемое, чувствуемое человеком);

в) Польза или благонамеренность (*перев. на англ.* Good) vs Вред или злонамеренность (*перев. на англ.* Harm) – общий вектор (или окрас) мотивации с этической точки зрения (желание выполнить легальные действия или нанести вред организации);

Используя 3 указанные категориальные пары, будет получено $2 \times 3 = 8$ классов мотивации инсайдера, которые могут быть обозначены следующими последовательностями первых букв англоязычных названий элементов (кроме Psycho-emotional, где для отличия от Physical используется вторая буква – S): IPG, IPH, ISG, ISH, EPG, EPH, ESG, ESH.

Важно отметить, что все классы определяют именно причины действия инсайдеров, не говоря ни о способах проведения атак, ни о последствиях, ни об уровне подготовки инсайдера и т. п.

Признаки классов

Кратко интерпретируем далее каждый из классов мотивации инсайдеров, полученных с применением категориального деления, приведем пример реальной мотивации, а также дадим ее краткие характеристики (в соответствии с каждой категориальной парой). Также, для формализованной и лаконичной идентификации полученных классов воспользуемся важным следствием применения категориального деления, заключающимся в записи идентификаторов, как последовательности бинарных флагов, каждый из которых определяет элемент соответствующей категориальной пары:

$$\begin{cases} Identifier(Class) \equiv ID_{Class} \\ ID_{class} = \langle P_1, P_2, P_3 \rangle \\ Class \in [IPG, IPH, ISG, ISH, EPG, EPH, ESG, ESH] \\ P_1 \in [0,1] \\ P_2 \in [0,1] \\ P_3 \in [0,1] \end{cases},$$

DOI: 10.31854/2307-1303-2023-11-2-47-56
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_2/47-56.pdf

где оператор $Identifier()$ – получение идентификатора (ID) для заданного класса ($Class$); $\langle \dots \rangle$ – запись идентификатора (как кортеж), состоящая из трех компонент (соответствующих категориальным парам, определяющим антагонистические свойства классов): P_1, P_2 и P_3.

Согласно же введенным категориальным парам, компоненты записи идентификатора можно определить следующим образом (с использованием указанного ранее перевода на английский язык элементов пар):

а) для начальной причины мотивации инсайдера:

$$\begin{bmatrix} P_1 = 1 \text{ если } Class \in \text{Internal} \\ P_1 = 0 \text{ если } Class \in \text{External} \end{bmatrix};$$

б) для конечной цели мотивации инсайдера:

$$\begin{bmatrix} P_2 = 1 \text{ если } Class \in \text{Physical} \\ P_2 = 0 \text{ если } Class \in \text{Psycho} - \text{emotional} \end{bmatrix};$$

в) для общего вектора мотивации инсайдера:

$$\begin{bmatrix} P_3 = 1 \text{ если } Class \in \text{Good} \\ P_3 = 0 \text{ если } Class \in \text{Harm} \end{bmatrix}.$$

Важной особенностью предложенной идентификации является то, что при необходимости детализации классификации путем введения новой категориальной пары формальная запись классов будет изменена лишь добавлением новых компонентов: P_4, P_5 и т. д. При этом математический аппарат на базе старой классификации, примененный к новой, будет также работоспособным, поскольку в нем потребуется лишь не учитывать новые компоненты.

Класс IPG

К данному классу относится инсайдер, который из собственных побуждений и без злого умысла, при этом стремясь получить материальные блага, создал инцидент нарушения информационной безопасности в организации [21].

Так, например, сотрудник, легально выполняя все свои должностные обязанности, вышел подзаработать сверхурочные, переоценил свои возможности и из-за накопившейся усталости допустил ошибки при работе с конфиденциальной информацией, обеспечив ее попадание третьим лицам.

Класс мотивации характеризуется следующим: внутренние причины, стремление к материальному обогащению, отсутствие стремления к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 1,1,1 \rangle$.

Класс IPH

К данному классу относится инсайдер, который из собственных побуждений и со злым умыслом, при этом стремясь получить материальные блага, создал инцидент нарушения информационной безопасности в организации [22].

Так, например, сотрудник, стремясь самостоятельно незаконно обогатиться (как вариант, получить финансовую прибыль), в рамках должностных обязанностей совершил перевод денежных средств на личный счет.

Класс мотивации характеризуется следующим: внутренние причины, стремление к материальному обогащению, стремление к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 1,1,0 \rangle$.

Класс ISG

К данному классу относится инсайдер, который из собственных побуждений и без злого умысла, при этом стремясь получить психоэмоциональное удовлетворение, создал инцидент нарушения информационной безопасности в организации [23].

Так, например, сотрудник, легально выполняя все свои должностные обязанности, безответственно отнесся к изучению выданных материалов, недостаточно изучил инструкцию к программному обеспечению (т. е. потратил выделенное время на собственные нужды) и допустил уничтожение персональных данных сотрудников.

Класс мотивации характеризуется следующим: внутренние причины, стремление к психоэмоциональному обогащению, отсутствие стремления к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 1,0,1 \rangle$.

Класс ISH

К данному классу относится инсайдер, который из собственных побуждений и со злым умыслом, при этом стремясь получить психоэмоциональное удовлетворение, создал инцидент нарушения информационной безопасности в организации [24].

Так, например, сотрудник, стремясь получить эмоциональное удовольствие (как вариант, выместить злобу на руководство), в рамках должностных обязанностей совершил удаление проектной документации крупного заказчика.

Класс мотивации характеризуется следующим: внутренние причины, стремление к психоэмоциональному обогащению, стремление к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 1,0,0 \rangle$.

Класс EPG

К данному классу относится инсайдер, который из-за внешнего воздействия и без злого умысла, при этом стремясь получить материальные блага, создал инцидент нарушения информационной безопасности в организации [25].

Пример мотивации данного класса является достаточно специфическим, поскольку сотрудник должен с одной стороны получать материальные блага за счет своих действий, а с другой стороны не считать их злонамеренными; при этом, блага будут идти извне организации, что априори в большинстве случаев выглядит как подкуп – т. е. близко к злому умыслу. Если делать аналогию с классом IPG, то сотрудник должен выйти в сверхурочные за счет «внешнего

работодателя», допустив при этом халатность – что является мало реалистичным в современной практике. Тем не менее, примером может быть внешняя подработка сотрудником на рабочем месте, в результате которой он установил некорпоративное программное обеспечение (и, следовательно, непроверенное и потенциально содержащее уязвимости), которое привело к заражению как его компьютера, так и сети организации, в лучшем случае лишь замедлив работу бизнес-процессов (нарушив тем самым доступность информации).

Класс мотивации характеризуется следующим: внешние причины, стремление к материальному обогащению, отсутствие намерения к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 0,1,1 \rangle$.

Класс EPH

К данному классу относится инсайдер, который из-за внешнего воздействия и со злым умыслом, при этом стремясь получить материальные блага, создал инцидент нарушения информационной безопасности в организации [26].

Так, например, сотрудник, стремясь незаконно обогатиться (как вариант, получить финансовую прибыль), в рамках должностных обязанностей совершил кражу финансовых отчетов и передал ее конкурирующей организации за денежное вознаграждение.

Класс мотивации характеризуется следующим: внешние причины, стремление к материальному обогащению, стремление к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 0,1,0 \rangle$.

Класс ESG

К данному классу относится инсайдер, который из-за внешнего воздействия и без злого умысла, при этом стремясь получить психоэмоциональное удовлетворение, создал инцидент нарушения информационной безопасности в организации [27].

Так, например, сотрудник, легально выполняя все свои должностные обязанности, сильно подверженный определенной идеологии глобальной доступности информации (например, гипотетической, борющейся за доступность любых медиаданных абсолютно всем и абсолютно безвозмездно), выложил в открытый доступ ресурсы, обслуживаемые облачным сервисом организации и содержащие платную фильмотеку.

Класс мотивации характеризуется следующим: внешние причины, стремление к психоэмоциональному обогащению, отсутствие стремления к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 0,0,1 \rangle$.

Класс ESH

К данному классу относится инсайдер, который из-за внешнего воздействия и со злым умыслом, при этом стремясь получить психоэмоциональное удовлетворение, создал инцидент нарушения информационной безопасности в организации [28].

Так, например, сотрудник, являвшийся шпионом одной страны и внедренный в организацию другой страны (т. е. побуждаемый больше долгосрочным желанием победы в кибервойне, чем краткосрочными материальными благами), удалил базу данных с результатами работы других сотрудников.

Класс мотивации характеризуется следующим: внешние причины, стремление к психоэмоциональному обогащению, стремление к неправомерным действиям.

Запись идентификатора у класса следующая: $ID_{IPG} = \langle 0,0,0 \rangle$.

Противодействие инсайдерам

Важным применением полученной классификации может быть создание узконаправленных противодействий инсайдером путем нейтрализации соответствующих характеристик класса. Так, например, в случае класса IPG, препятствовать инсайдерской деятельности можно путем обеспечения высокой нравственной составляющей сотрудников (нейтрализуя внутренние факторы), увеличения размера заработной платы (снижая стремление к материальному обогащению) и усиления контроля за действиями сотрудников (предотвращая попытки неправомерных действий). Аналогично, для класса же ESG инсайдерской деятельности можно противодействовать путем ограничения контактов сотрудников с внешними, потенциально опасными лицами, обеспечивать психоэмоциональное насыщение сотрудников собственными мероприятиями и устраивая разъяснительные собрания касательно опасности чрезмерных инициатив, не носящих неправомерных действий, но потенциально ведущих к нарушениям информационной безопасности.

Заключение

В работе предлагается применение аппарата категориального деления для получения непротиворечивых классов мотиваций инсайдерской деятельности сотрудников организации с информационной системой (аналогично [29]). Для этого выделяется три следующие пары: Внутренний vs Внешний, Физический vs Психоэмоциональный, Польза vs Вред. Комбинация элементов пар позволяет получить 8 классов, для каждого из которых дается понятная интерпретация и практические пример.

Основным результатом работы являются 8 полученных классов мотивации сотрудников организации, что и определяет его теоретическую значимость в части расширения описательных характеристик инсайдера. Практическая значимость заключается в возможности обнаружения причин неправомерной инсайдерской деятельности и способов превентивного противодействия ей.

Продолжением исследования может стать создание способа (в том числе автоматизированного) классификации мотивации инсайдеров [30].

DOI: 10.31854/2307-1303-2023-11-2-47-56
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_2/47-56.pdf

Литература

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

2. Буйневич М. В., Израилов К. Е., Мостович Д. И., Ярошенко А. Ю. Проблемные вопросы нейтрализации уязвимостей программного кода телекоммуникационных устройств // Проблемы управления рисками в техносфере. 2016. № 3 (39). С. 81–89.

3. Власов Д. С. Задачи построения системы обеспечения информационной безопасности типового объекта МЧС России // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей V международной научно-технической и научно-методической конференции (Санкт-Петербург, 10–11 марта 2016 года). СПб.: СПбГУТ, 2016. С. 281–285.

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

5. Буйневич М. В., Израилов К. Е., Покусов В. В., Ярошенко А. Ю. Основные принципы проектирования архитектуры современных систем защиты // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58

6. Буйневич М. В., Васильева И. Н., Воробьев Т. М., Гниденко И. Г., Егорова И. В., Еникеева Л. А. и др. Защита информации в компьютерных системах. Монография. СПб.: СПГЭУ, 2017. 163 с.

7. Израилов К. Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети // Вестник ИНЖЭКОНа. Серия: Технические науки. 2012. № 8 (59). С. 150–153.

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

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

10. Давлетханов М. Г., Столяров Н. В. Защита от инсайдеров // Защита информации. Инсайд. 2006. № 3 (9). С. 52–56.

11. Морозова Е. А. Инсайдерство как преступление в сфере компьютерной информации // Аллея науки. 2019. Т. 1. № 1 (28). С. 725–729.

12. Alawneh M., Abbadi I. Defining and Analyzing Insiders and Their Threats in Organizations // Proceedings of 10th International Conference on Trust, Security and Privacy in Computing and Communications (Changsha, China, 16–18 November 2011). IEEE, 2011. PP. 785–794. DOI: 10.1109/TrustCom.2011.103

13. Пырьев Е. А. Эмоции в системе психического отражения и мотивации поведения человека // Вестник Оренбургского государственного университета. 2012. № 2 (138). С. 232–236.

14. Лэнгле А. Что движет человеком? экзистенциальная мотивация person // Эксперимент и инновации в школе. 2013. № 1. С. 48–58.

15. Камалова Р. Р., Ханнанова Т. Р. Управление трудом как мотивация деятельности человека // NovaInfo.Ru. 2014. № 22. С. 9–12.

16. Буйневич М. В., Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 115–130.

17. Израилов К. Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 86–104.

18. Израилов К. Е., Покусов В. В. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 104–121.

19. Виткова Л. А., Израилов К. Е., Чечулин А. А. Классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей IX Международной научно-технической и научно-методической конференции (Санкт-Петербург, 26–27 февраля 2020 года). СПб.: СПбГУТ, 2020. С. 253–258.

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

21. Помятилова Н. Н. Характерные типы инсайдеров в современных хозяйствующих организациях // Экономика и государство: эффективное управление и взаимодействие: сборник статей. М.: ООО "МАКС Пресс", 2019. С. 229–234.

22. Казакова И. И., Царегородцев А. В., Цацкина Е. П. Математическое и информационное обеспечение системы сценарного моделирования действий инсайдера // Огарёв-Online. 2017. № 13 (102). С. 2.

23. Незнамова З. А., Сибякин А. Е. Понятие и виды инсайдеров в законодательстве зарубежных стран // Электронное приложение к Российскому юридическому журналу. 2019. № 1. С. 47–53.

24. Маркова Т. И., Захарова К. В. Классификация инсайдеров // Вестник Волжского университета им. В. Н. Татищева. 2010. № 15. С. 29–34.

25. Мамочка Е. А. Типы личности преступника-инсайдера // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2016. Т. 8. № 3 (34). С. 70–78.

26. Зайцев А. С., Малюк А. А. Системно-динамическое моделирование угрозы кражи интеллектуальной собственности // Вестник РГГУ. Защита информации и информационная безопасность. 2015. № 12 (155). С. 70–91.

27. Ивутин В. В., Зайцев А. С. Разработка модели поведения немотивированного внутреннего нарушителя информационной безопасности // Безопасность информационных технологий. 2015. Т. 22. № 1. С. 83–85.

28. Bushuev A. Modern methods of protection against insider threats // Languages in professional communication: сборник материалов международной научно-практической конференции преподавателей, аспирантов и студентов (Екатеринбург, 28 мая 2020 года). Екатеринбург: ООО «Издательский Дом «Ажур», 2020. С. 458–461.

29. Курта П. А., Коломеец М. В. Обобщенная классификация интерфейсов транспортной инфраструктуры «Умного города» // Вестник кибернетики. 2020. № 4 (40). С. 6–13. DOI: 10.34822/1999-7604-2020-4-6-13

30. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders // Proceedings of ACM International Conference Proceeding Series: 4 (Saint-Petersburg, 26–27 November 2020). New York: Association for Computing Machinery, 2020. P. 3442619. DOI: 10.1145/3440749.3442619

Статья поступила 01 ноября 2023 г.
Принята к публикации 20 декабря 2023 г.

Информация об авторе

Власов Дмитрий Сергеевич – начальник управления информационных технологий и связи Главного управления МЧС России по г. Санкт-Петербургу. E-mail: prikerx@bk.ru

Application of Categorical Division to Classify Motivation For Insider Activities

Vlasov D.
EMERCOM of Russia Main Directorate in the St. Petersburg city
St. Petersburg, 190000, Russian Federation

Statement of the problem: *identifying insider activities in organizations that lead to threats to information security, one of the first steps of which should be the study of the motivation that pushes employees to illegal actions.* ***The purpose of the work*** *is to synthesize the main classes of insider motivations; at the same time, the classes must cover all possible situations, and each of the classes must not overlap with others.* ***Methods used:*** *categorical division to identify classes and their practical justification.* ***Novelty:*** *in contrast to the existing motivations of insiders, the proposed classification meets the criteria of necessity and sufficiency, thereby being initially sufficiently consistent and covering all cases; Moreover, all classes are obtained theoretically using the strict logic of categorical division.* ***Result:*** *the use of categorical division identified 3 pairs of categories (Internal vs External, Physical vs Psycho-emotional, Benefit or good intentions vs Harm or malicious intent), which made it possible to form 8 unique classes of insider motivations based on their combinations. The existence of each class is confirmed by the presence of a corresponding publication.* ***Theoretical relevance:*** *a unified set of insider motivation classes was obtained that meets the criteria of necessity and sufficiency.* ***Practical relevance:*** *the resulting classes of insider motivations can be used to understand the reasons for such illegal activities and, therefore, to create effective ways to counteract them.*

Keywords: *information security, insider, organization, motivation*

Information about Author

Vlasov Dmitry – Head of the Information Technology and Communications Department (EMERCOM of Russia Main Directorate in the St. Petersburg city).
E–mail: prikerx@bk.ru