Аналитическая статья
УДК 004.5; DOI: 10.61260/2218-13X-2024-4-89-102

ОБЗОР МОДЕЛЕЙ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ИНТЕРЕСАХ ПРОТИВОДЕЙСТВИЯ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ (ПО СОСТОЯНИЮ ОТЕЧЕСТВЕННОГО НАУЧНОГО СЕГМЕНТА)

✉**Буйневич Михаил Викторович.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия.
Моисеенко Григорий Юрьевич.
Министерство обороны Российской Федерации, Москва, Россия
✉***bmv1958@yandex.ru***

Аннотация. Работа посвящена противодействию инсайдерской деятельности, приводящей к угрозам безопасности информационным ресурсам организации. В качестве инсайдеров рассматривается их относительно новый тип – неумышленный, который не имеет злонамеренных мотивов и является следствием девиации в поведении человека как пользователя информационной системы. Дается общая методологическая схема предполагаемого научного исследования. На его первом этапе требуется разработка модели поведения пользователя (с учетом уязвимостей системы, информационных ресурсов, девиаций и т.п.), в интересах чего производится обзор топ-10 научных публикаций российских ученых. Систематизация работ в табличном виде с использованием критериев сравнения (год публикации, области применения, состояние решения, аналитическая форма, использование машинного обучения и отражение факта неумышленности) позволяет сделать ряд выводов относительно состояния предметной области, а также выдвинуть базовые предположения для создания необходимой модели поведения.

Ключевые слова: информационная система, информационная безопасность, пользователь, модель поведения, обзор

Для цитирования: Буйневич М.В., Моисеенко Г.Ю. Обзор моделей поведения пользователя информационной системы в интересах противодействия инсайдерской деятельности (по состоянию отечественного научного сегмента) // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 4. С. 89–102. DOI: 10.61260/2218-13X-2024-4-89-102.

Analytical article

THE INFORMATION SYSTEM USER BEHAVIOR MODELS REVIEW IN INTERESTS OF COUNTERACTING INSIDER ACTIVITY (BY THE STATE OF DOMESTIC SCIENTIFIC SEGMENT)

✉**Buinevich Mikhail V.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia.
Moiseenko Grigory Yu.
Ministry of defense of the Russian Federation, Moscow, Russia
✉***bmv1958@yandex.ru***

Abstract. The work is devoted to counteracting insider activity in organizations, leading to threats to its information resources. Insiders are considered to be a relatively new type of them – unintentional, which does not have malicious motives and is a consequence of deviation in human behavior as a user of an information system. A general methodological outline of the proposed scientific research are given. At its first stage, it is necessary to develop a model of user behavior (taking into account system vulnerabilities, information resources, deviations, etc.), for which a review of the top-10 scientific publications of Russian scientists is carried out. Systematization of works in tabular form using comparison criteria (year of publication, areas of application, state

of the solution, analytical form, use of machine learning and reflection of the fact of unintentionality) allows us to draw a number of conclusions regarding the state of the subject area, as well as put forward basic assumptions for creating the necessary behavior model.

Keywords: information system, information security, user, behavior model, review

For citation: Buinevich M.V., Moiseenko G.Yu. The information system user behavior models review in interests of counteracting insider activity (by the state of domestic scientific segment) // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 4. P. 89–102. DOI: 10.61260/2218-13X-2024-4-89-102.

Введение

Безопасность ресурсов информационной системы (ИС) является одной из первоочередных задач практически любой современной организации. При этом гетерогенность ее внутренней структуры и широкий спектр выполняемых задач, а также определенная открытость для внешней (то есть неконтролируемой) среды делают организацию подверженной большому количеству угроз, источники которых являются не только информационными и физическими, но и социальными или индивидуально человеческими [1]. Так, часть сотрудников, уже обладающих некоторыми правами на доступ к информационным ресурсам (например, исходя из своих должностных инструкций), могут передавать защищаемые документы третьим лицам, переходя тем самым в разряд инсайдеров [2]. Их выявление является достаточно нетривиальной комплексной задачей как с научной, так и с практической (в том числе организационной) точки зрения [3].

Ситуация усложняется тем, что сама инсайдерская деятельность может иметь не только злонамеренный характер, но и быть неумышленной, например, вследствие халатности сотрудника или его психо-эмоциональной усталости из-за большой рабочей нагрузки. Противодействие такого рода угрозам не всегда можно решить дисциплинарными способами, такими как объявление выговора или увольнение, поскольку у любого человека существуют вполне законные ограничения на безотказное выполнение инструкций, а в ряде областей с редкими высококвалифицированными сотрудниками поиск новых будет крайне затруднительным.

В интересах противодействия неумышленному инсайдингу авторами предлагается несколько отличный от классических подход, который заключается в следующем. Во-первых, одна из причин перехода легальных (или лояльных) сотрудников в разряд такого рода инсайдеров заключается в том, что они являются не алгоритмическими автоматами, строго выполняющими заданный порядок действий, а людьми, поведение которых может обладать слабо контролируемой девиацией.

Примечание: здесь именно девиация как отклонение от заданного направления движения (расчетной траектории), маршрута, технологической карты под влиянием каких-либо, кажущихся случайными, внутренних или внешних причин. В отличие от девиантности как поведения, которое не соответствует принятым в обществе нормам, правилам и законам. Проецирование этих понятий на предметную область будет описано далее.

Так, наличие вредных привычек, чувство голода, сильная тревожность могут «заставить» сотрудника прервать или изменить выполнение указанных ему регламентов действий/маршрута и, например, зайти в место для курения, посетить столовую или сделать перерыв на отдых. Во-вторых, задача противодействия девиации будет носить, по большей части, бессмысленный характер, поскольку ее решением будет борьба с природой человека вплоть до замены сотрудников на роботов или программно-аппаратные средства, что применимо для очень ограниченного количества задач. В-третьих, предполагается, что решение проблем неумышленного инсайдинга может лежать не в аспекте психики человека, а в повышении «устойчивости» выполняемых им инструкций. В этом случае один из путей решения будет заключаться в модификации самих инструкций (заданных, например, в виде некоторой последовательности переходов между состояниями ИС) с целью недопущения

или снижения вероятности их нарушения сотрудниками вследствие девиации поведения. Как результат, у сотрудника будет в принципе снижена возможность совершать действия (и в особенности незлонамеренные, неумышленные), которые ведут к угрозам безопасности информационным ресурсам (ИР). При этом данный подход может быть перенесен из плоскости физической в плоскость полностью информационную путем противодействия инсайдерству исключительно при «нахождении» пользователей в ИС, например, используя интерфейс программного обеспечения для работы с ее ИР [4].

Реализация данного авторского подхода требует проведения соответствующего научного исследования по «канонической» схеме, разбитой на условно-логические методологические этапы. Во-первых, необходимо построение обобщенной модели пользователя в ИС (модель), способной как отразить регламент его поведения (задаваемый инструкциями) при работе с ИР и возможную девиацию этого, так и учесть пути реализации угроз ИР (например, через профили неумышленного инсайдера). Сразу можно предположить, что наиболее целесообразным видом модели должна быть аналитическая запись, позволяющая впоследствии проводить формальные оценки и эксперименты на ней. Во-вторых, требуется метод построения такой модели, поскольку она должна учитывать специфику конкретной организации, ее ИС и ИР, характеристики пользователей и прочее, что само по себе является отдельно стоящей задачей. Так, в результате применения метода будет произведен структурно-параметрический синтез модели – будет создана не только ее структура (например, граф), но и определены параметры (например, свойства узлов и веса связей). В-третьих, необходима методика оценки интегральной безопасности выполнения инструкций по модели с учетом различной девиации сотрудников в заданной организации. В-четвертых, логичным продолжением должна стать разработка алгоритма оптимизации инструкций (с учетом задач организации, решаемых сотрудниками), целевой функцией которой как раз и является данная интегральная безопасность. И, в-пятых, необходимо проектирование программно-моделирующего средства, которое бы позволило оператору построить данную модель, задать ее параметры, указать сотрудников и их особенности, имеющиеся инструкции (или решаемые задачи), оценить интегральную безопасность, произвести ряд оптимизационных мероприятий (как вручную, так и с помощью реализованных алгоритмов, в том числе и с применением искусственного интеллекта [5]), а также визуализировать все эти операции и их результаты в текстовом или графическом виде для проверки и дополнительной подстройки экспертом, занимающимся данным аспектом информационной безопасности в организации (эксперт).

Одним из наиболее сложных элементов в подходе является представление поведения сотрудника в ИС в виде модели, в особенности, исходя из предъявляемых к ней требований. В интересах этого, далее в статье будет произведен обзор и систематизация существующих отечественных решений, в которых в том или ином способе и виде данная задача (задача) уже решалась.

Обзор работ

Для выявления наиболее подходящих и актуальных решений касательно моделирования поведения пользователя в ИС был произведен анализ поисковой выдачи базы Российского индекса научного цитирования по ключевому запросу «модель поведения пользователя» за последние 10 лет в статьях и книгах, имеющих также текст в открытом доступе; первая Web-страница результатов поиска содержала 100 различных публикаций, обзор топ-10 наиболее релевантных из которых приведен далее.

Работа [6] посвящена моделированию поведения инсайдеров в корпоративной ИС, для чего применяется граф де Брюина второго порядка. Узлы такого графа хранят текстовые данные, отображаемые, в том числе, в пользовательском интерфейсе системы. Для построения модели используется запись действий пользователя с ИР, включающая в себя помимо его идентификатора, времени взаимодействия и самих данных (например, ссылки на документ или его часть, просмотренную пользователем), указание также на используемый

интерфейсный элемент и URL. В результате накопления такой информации строится модель поведения пользователя, соответствующая портрету легального сотрудника. Соответственно, аномалии в работе пользователя с документами, выявляемые по новым собранным логам, позволят как говорить о потенциальной инсайдерской деятельности, так и выделять затронутые при этом документы и их тематики (что будет востребовано при расследовании киберпреступлений). Автор в своем докладе описывает эксперимент с предложенной моделью с помощью созданного прототипа, реализованного в виде расширения для браузера Google Chrome. Для выявления аномалий использовалась искусственная нейронная сеть (ИНС) с архитектурой автокодировщика, имеющей три скрытых слоя и функцию активации типа «сигмоид».

В исследовании [7] рассматривается поиск информации в сети Интернет с позиции повышения эффективности данного процесса. В частности, описывается модель поведения пользователя, состоящая из 11 следующих действий, заданных в текстовом виде: определить длительность сеанса; поставить цель; выбрать поисковую систему; выбрать категорию искомой информации (опционально); перебрать поисковые запросы; получить по ним поисковую выдачу; переформулировать или изменить запрос (опционально); оценить качество поисковой выдачи и, следовательно, самого запроса, а при необходимости скорректировать его; проанализировать материал по ссылкам из поисковой выдачи; оценить достижение цели поиска информации и повторить предыдущие шаги соответствующим образом; использовать полученную информацию (или сохранить ее).

Автор в работе [8] сравнивает применимость двух инструментов «глубинного анализа данных» (а именно Disco и ProM) [9] для построения модели поведения пользователя на интернет-ресурсе, содержащем систему управления образовательными курсами. Итоговые модели, создаваемые первым инструментом, представляют собой графы переходов между узлами-событиями на основании действий пользователей, указывая, в том числе, частоту посещений таких узлов; также отмечены переходы из начального и в конечное состояние. Поскольку подобные представления за длительный период времени, как правило, занимают существенный размер и сложно воспринимаемы человеком, то предлагается их упрощать путем отображения наиболее частых событий и переходов (согласно некоторому критерию). При этом дополнительным атрибутом ребра графа может служить время соответствующего ему процесса. Модели поведения, создаваемые вторым инструментом, достаточно корреспондируют с получаемыми первым, однако дополнены кластеризацией близких событий.

Авторы в работе [10] строят систему, предназначенную для выявления аномального поведения пользователя в ИС (являющейся при этом распределенной вычислительной), что может сигнализировать о наличии в организации инсайдера. Данную задачу предлагается решать путем построения модели вычислительного процесса, содержащей портрет нормального поведения пользователя в ИС, полученного по статистически собранным данным. В качестве примера, шаблон пользователя строится по сделанным им за некоторый период времени телефонным звонкам; отклонение же поведения от шаблона будет означать искомую аномальность. Также в работе описывается общий подход к минимизации ошибок I и II рода.

Автор работы [11] предлагает модель пространства признаков, необходимую для использования в машинном обучении (МО), а в качестве основного применения указывается анализ поведения пользователей в центрах обработки данных (ЦОД), детектирование аномалий в работе с которыми потенциально позволит выявить производимые атаки (например, SQL-инъекции и несанкционированный доступ к данным). Поведение пользователей определяется по их запросам к базам данных ЦОД (БД). Модель пространства строится достаточно классическим способом, состоящим из выбора признаков и их оптимизации. Для построения модели берутся логи работы системы управления БД, включающие дату и время операции, идентификатор пользователя и сам SQL-запрос. Сами же признаки получаются из текста запросов и делятся на три категории, связанные

с ключевыми словами, сигнатурами и именами таблиц (с использованием «мешка слов»). Оптимизацию предлагается осуществлять применением различных метрик информативности, таких как прирост информации, его отношение к разделенной информации и модель дисперсионного анализа; также возможно вычисление нормированного среднего всех трех метрик. Автор указывает, что имеется реализация подхода на языке Python и в системе Orange (версии 3.32); при этом в первом прототипе применялся полный набор признаков, а во втором – его оптимизированный вариант. Для выявления аномалий были выбраны такие модели машинного обучения с учителем, как логистическая регрессия, машина опорных векторов, дерево решений, метод k-ближайших соседей, наивный Байес, многослойная ИНС и случайный лес.

Исследование [12] ставит своей целью прогнозирование количества пользователей интернет-сервиса, что в некотором приближении также можно считать моделью их поведения (а точнее – посещения). На основании собранной статистики взаимодействия с некоторым интернет-магазином авторы решают задачу линейной регрессии по установлению зависимости между количеством пользователей сайта и временем его работы. В частности, коэффициенты линейного уравнения вычисляются с использованием метода наименьших квадратов и модели машинного обучения, при этом применение первого способа вычисления дало более точные результаты, чем второго.

Работа [13] посвящена выявлению аномального поведения пользователей информационно-вычислительной системы (ИВС) путем анализа переходов между ее состояниями с учетом предыдущей истории; для этого, в частности, применяется конечный автомат и модель Гогена-Мезигера. Также предлагается создавать сигнатуры цепочек действий пользователя, разделяя их на две группы – разрешенные (то есть безопасные) и запрещенные (то есть потенциально опасные), при этом в первой группе имеется дополнительное деление на нейтральные действия пользователя (при нормальном выполнении им задач) и те, при которых он не может справиться с заданиями (в этом случае система может давать соответствующие подсказки о необходимых действиях). В качестве новизны предлагаемого решения по определению аномального поведения пользователей авторы указывают построение сигнатур именно переходов между состояниями в отличие от аналогов, учитывающих признаки объектов мониторинга.

В статье [14] исследуется возможность выявления аномалий в пользовательской активности при взаимодействии с ЦОД путем анализа логов работы с их БД, для чего предлагается применять ИНС типа многослойного персептрона с различными функциями активации. Приводятся методы обнаружения аномалий, основанные на применении моделей данных, метрик, статистических тестов, индукции и машинного обучения в части кластеризации, а также их комбинированных версий. В качестве признаков разработанной ИНС использовались дата, время и источник обращения к БД, а также сам SQL-запрос.

Исследователи в работе [15] описывают абстрактную модель поведения интеллектуального агента, который может быть сопоставлен участнику социальной сети (в частности, взаимодействующий с другими участниками посредством сообщений); агент рассматривается как совокупность следующих сущностей: его цель и характеристики, состояние, память, механизм поведения, связь с окружением и шаблон поведения, при этом наличие памяти, накапливающей знания без их непосредственной проверки (представляющей собой структуру нейрологических уровней Р. Дилтса [16]), является отличительной особенностью модели от аналогичных.

Статья [17] посвящена построению профилей пользователей, работающих в интернет-пространстве, с учетом их предпочтений касательно имеющихся ИР. Метод построения состоит из четырех следующих шагов: отбор признаков, под которыми понимается тематика посещаемых Интернет-сайтов; формирование данных для машинного обучения, связанных с интересами; создание «грубого» классификатора; оптимизация его параметров с помощью «кукушкиного поиска» [18]. Здесь следует уточнить, что под поведением пользователей авторы понимают именно их обобщенные тематические предпочтения, что может

использоваться интернет-сервисами для персонализации предоставляемой информации (например, более релевантной поисковой выдачи).

Отдельного внимания заслуживает работа [19], которая хотя и не имеет прямого отношения к области ИС, тем не менее может считаться достаточно релевантной текущей задаче, поскольку рассматривает с различных аспектов «девиантное поведение» члена социума, определяемое авторами как «устойчивое поведение личности, отклоняющееся от наиболее важных социальных норм, не соответствующее распространенным в обществе ценностям, правилам, стереотипам поведения, ожиданиям, установкам, причиняющее реальный ущерб обществу или самой личности, непосредственно угрожающее благополучию межличностных отношений, а также сопровождающееся социальной дезадаптацией личности». Так, с точки зрения текущего исследования под социальными нормами могут пониматься инструкции для сотрудников, ценностям и ожиданиям – априори предполагаемые в рамках инструкций действия для выполнения, ущербом – результат реализации угрозы ИР, дезадаптацией личности – обратное негативное действие на сотрудника после совершения и осознания им акта неумышленного вредоносного действия. Впрочем авторы в работе основной упор делают на воспитание личности, что является противоположным подходом для текущего исследования. В качестве причин девиантного поведения указывается генетическая предрасположенность, психологические установки и дезорганизация социальной среды. Таким образом, по крайней мере, противодействие первой из трех причин представляется крайне проблематичной (поскольку она заложена в природе человека), противодействие второй организационными методами потребует определенного насилия над личностью (что попросту приведет к увольнению сотрудника), а третьей – гипотетически существенной перестройки социальной инфраструктуры всей организации (что также в большинстве случаев практически неосуществимо). Все это говорит в пользу противодействия неумышленному по причине человеческой девиации инсайдерству через формирование, так называемых «устойчивых» инструкций (или регламентов деятельности) [20].

Необходимо отметить, что «беглый» анализ последующих страниц поисковой выдачи (то есть работ после 100-й) показал существенное уменьшение релевантности публикаций к исходному запросу, и поэтому все эти работы были исключены из рассмотрения.

Анализ результатов

Согласно проделанному обзору все работы были систематизированы в таблице, имеющей следующие столбцы-критерии и их интерпретацию:

К_1. Название работы и ссылка на нее.

К_2. Год публикации работы.

К_3. Область, в которой предлагается применять изложенное решение.

К_4. Основная суть (или идея) предложенной модели поведения.

К_5. Состояние решения, определяющее степень его готовности.

К_6. Представление модели в аналитическом виде: «+» – присутствует; «+/–» – допускается (предполагается); «–» – отсутствует.

К_7. Использование модели в интеллектуальных методах на базе МО: «+» – предлагается; «+/–» – допускается; «–» – не предлагается (при наличии такой возможности указывалась решаемая задача: МО_Ан – выявление аномалий; МО_Кл – классификация; МО_Кр – кластеризация; МО_Рг – регрессия).

К_8. Отражение фактора неумышленности инсайдерской деятельности: «+» – учитывает; «+/–» – может учитывать; «–» – не учитывает.

Таблица

Систематизация обзора топ-10 релевантных работ

К_1	К_2	К_3	К_4	К_5	К_6	К_7	К_8
Модель поведения пользователя корпоративной информационной системы [6]	2023	Корпоратив-ные ИС	Граф получения информации из документов при доступе к ним через интерфейс	Прототип	+	+ (МО_Ан)	+/–
Поиск информации в интернете: анализ влияющих факторов и моделей поведения пользователей [7]	2017	Поисковая система Интернет	Линейная последователь-ность действий пользователя при поиске информации	Теория	–	–	–
Построение модели поведения пользователя на веб-ресурсе средствами Process Mining [8]	2015	Интернет-ресурсы с событийным логированием	Граф переходов ИС между событиями (с весами)	Продукт	+/–	+/– (МО_Кр)	–
Разработка метода мониторинга аномального поведения пользователя в распределенной ИВС: построение математической модели [10]	2021	ИВС	Граф штатного поведения ИС	Теория	+/–	+/– (МО_Ан)	+
Модель признакового пространства для выявления аномального поведения пользователей ЦОД методами МО [11]	2022	ЦОД	Пространство признаков SQL-запросов к БД	Прототип	+/–	+ (МО_Ан)	+/–
Сравнительный анализ результатов МО и регрессионной модели траекторий поведения пользователей онлайн-сервисов [12]	2023	Интернет-пространство	Статистика посещения сервиса	Теория	+	+ (МО_Рг)	–
Разработка имитационной модели для исследования поведения пользователя в распределенных ИВС [13]	2021	ИВС	Граф штатного поведения пользователя в ИС	Теория	+/–	–	+/–

К_1	К_2	К_3	К_4	К_5	К_6	К_7	К_8
Применение искусственных нейронных сетей для выявления аномального поведения пользователей ЦОД [14]	2022	ЦОД	Пространство признаков SQL-запросов к БД	Прото-тип	+/–	+ (МО_Ан)	+/–
Подход к формированию памяти интеллектуального агента при моделировании поведения пользователей социальной сети [15]	2019	Социальные сети	Интеллектуаль-ный агент с памятью и поведением	Теория	+	–	+
Биоинспирирован-ный подход к решению задачи классификации профилей поведения пользователей в интеллектуальных интернет-сервисах [17]	2019	Интернет-пространство	Тематические предпочтения пользователей	Прото-тип	+	+ (МО_Кл)	+

Согласно проведенной систематизации обзоров (табл.) можно сделать следующие частные выводы касательно каждого из критериев (то есть столбцов таблицы).

Во-первых, проанализируем хронологию количества публикаций релевантных работ (К_2) – то есть за последние 10 лет; она в виде гистограммы представлена на рисунке.

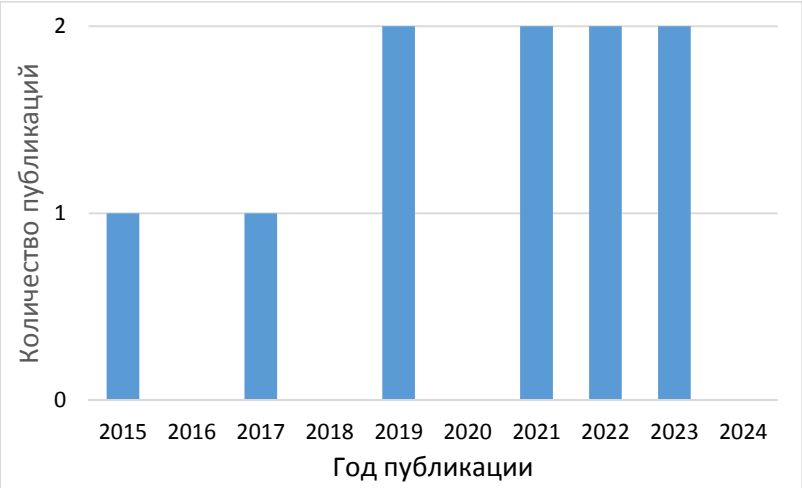

Рис. **Количество публикаций по годам**

Несмотря на достаточно небольшую выборку для построения трендов или иных зависимостей (то есть всего 10 публикаций), тем не менее можно предположить, что задача моделирования поведения пользователей за последние 10 лет оставалась одинаково актуальной с небольшим увеличением научного интереса в последнее время. Отсутствие

публикаций в 2024 г. нельзя считать аномальным, поскольку в 2016, 2018 и 2020 гг. они также отсутствовали, а в остальные года их количество было достаточно небольшим (не более одной-двух). Таким образом, с позиции специфики задачи текущего исследования можно предположить, что ее полноценные решения вряд ли были найдены.

Обобщение областей приложения решений в работах (К_3) позволило выделить следующие основные их группы:

– интернет-пространство: четыре публикации;

– ИВС и ЦОД: по две публикации;

– корпоративные ИС и социальные сети: по одной публикации.

Таким образом, все работы рассматривают две основные (укрупненные) группы областей – интернет и ИС, и лишь одна – социальные сети. То есть по крайне мере половина работ относится к предметной области текущего исследования – поведение пользователя в ИС, и, следовательно, предлагаемые в них решения (естественно, путем качественного их развития) могут быть применены в интересах решения задачи.

С точки зрения основных идей, лежащих в основе решений (К_4), их можно сгруппировать следующим образом:

– графы переходов (между состояниями пользователя или ИС): четыре публикации;

– работа с SQL-запросами к БД: две публикации;

– другие, более узкоспециализированные решения (интеллектуальные агенты, сигнатуры действий, статистические данные, тематики документов): четыре публикации.

Исходя из приведенной группировки, а также учитывая предыдущий вывод (в части анализа таблицы по К_3), новое гипотетическое решение задачи может строиться на идее графового представления процессов предметной области с ее дополнительным развитием путем существенного учета специфики предметной области – например, неумышленности действий сотрудников и наличия шаблонов поведения пользователей в ИС, приводящих к угрозам ИР. Естественно нельзя отбрасывать и возможность построения решения на качественно новых принципах, подходах, моделях и т.п. При этом отдельное внимание нужно уделить вопросам итоговой визуализации графа модели, поскольку предполагается некоторая работа с ним эксперта (например, за счет метафор визуализации [21]).

С точки зрения готовности решения к применению на практике (К_5), большинство из них носит лишь теоретический характер (пять публикаций) с чуть меньшим количеством работающих прототипов (четыре публикации), и только в одной работе [8] используется готовый продукт, при этом предназначенный для обобщенного решения задач анализа графов.

Модели в работах в той или иной степени (К_6) представлены в аналитическом виде (пять полностью и четыре частично), и только одна из них оперирует словесным описанием. Таким образом, данный научный опыт целесообразно применить и при решении задачи.

Применение МО при работе с моделями (К_7) предполагается в семи рассмотренных публикациях (хотя в двух из них это допускается не напрямую), в трех вопрос об этом не стоит в принципе. При этом с позиции решаемых задач МО в четырех указывается выявление аномалий, а в остальных – классификация, кластеризация и регрессия. Следовательно, подобного рода модели достаточно хорошо подходят для обработки интеллектуальными методами, хотя это и не является обязательным условием.

И, наконец, с точки зрения выделения неумышленных инсайдеров (К_8), три работы позволяют учитывать данную специфику, четыре подходят для это частично и три не подходят совсем. Важно отметить, что указанные работы лишь гипотетически содержат указанную возможность, однако в качестве принципиального решения задачи все они не подойдут. Таким образом, подтверждается вывод по К_4 о целесообразности поиска нового решения на базе существующих (хотя и немногочисленных).

Предпосылки к модели

Подводя итоги в частных выводах, можно сделать достаточно общий, предлагающий ближайший (то есть в данной точке исследования) основной путь решения задачи на первом этапе исследования. Модель, предназначенная для учета девиаций пользователя в ИС и оценки реализуемых при этом угроз, гипотетически может строиться на графо-ориентированном подходе (по аналогии, например, с работами [22, 23]), учитывающем отдельные аспекты информационного обмена с ИС (не ограничиваясь SQL-запросами), а также применять сигнатурные, статистические и агентно-ориентированные методы, в том числе используя все множество инструментария области МО; аналитическая форма модели является необходимой де-факто [24].

Также можно предположить и иные принципы, на которых возможно построение решения задачи, например – моделирование не поведения пользователя ИС при выполнении должностных инструкций, а создание модели самих инструкций в рамках текущей структуры организации, ее ИС и ИР, при учете пользовательской девиации. При этом целесообразно рассмотреть и более сложные «архитектуры» решений в виде мета-моделей [25], состоящих как раз из частных взаимосвязанных моделей основных сущностей предметной области – ИС, ИР, сотрудник, поведение с девиацией, инструкция, нарушитель (при том как злонамеренный, так и неумышленный), угроза и т.п. Тем не менее полагаясь на научную интуицию и определенный авторский опыт, на данном шаге исследования сделанный общий вывод касательно построения модели рассматривается как наиболее предпочтительный.

Заключение

Работа относится к первому этапу основного исследования по противодействию неумышленному инсайдингу, а именно – построению модели поведения пользователя в ИС согласно заданным инструкциям с учетом возможной реализации угроз ввиду его девиации. В интересах этого произведен отбор и анализ топ-10 научных публикаций на более общую тему, сведенных в единую таблицу. Исходя из критериального сравнения предлагаемых в работах решений, сделаны первоначальные выводы касательно будущего вида создаваемой модели.

Научным результатом текущего исследования является сравнительная таблица топ-10 публикаций, релевантных к решаемой задаче, а также сделанные по ней частные и общие выводы.

Новизна работ заключается в некотором обобщении всего имеющегося 10-летнего опыта российских ученых в части моделирования поведения пользователей в ИС, который позволил дать общую картину о состоянии предметной области. Теоретическая значимость состоит в сделанных по обзорам выводах (новом знании); практическая же частично состоит в конструктивности требований к гипотетической модели. Предполагается, что реализующие ее программно-алгоритмические средства позволят предсказывать поведения пользователей в ИС по заданным должностным инструкциям, оценивать соответствующий этому уровень безопасности ИР, а также проводить аналогичные модельные эксперименты.

Стоит отметить, что недостатком сделанного обзора релевантных работ является то, что все они взяты из отечественной базы цитирования, тем самым практически исключая опыт зарубежных ученых (такой, например, как в работе [26]); однако, обзор зарубежного сегмента планируется сделать в будущем. Также продолжением исследования должно стать итоговое (формальное) описание модели, наиболее подходящее для решения текущей задачи.

Список источников

1. Буйневич М.В., Моисеенко Г.Ю. Комбинирование разнородных деструктивных воздействий на информационную систему и противодействие атакам (на примере инсайдерской деятельности и DDoS-атаки) // Информационные технологии и телекоммуникации. 2023. Т. 11. № 3. С. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36.

2. 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.

3. Буйневич М.В., Власов Д.С., Моисеенко Г.Ю. Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024. № 3 (61). С. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.

4. Курта П.А., Буйневич М.В. Онтологическая модель взаимодействия пользователя с информационной системой в рамках получения услуги информационного сервиса // Вестник кибернетики. 2021. № 2 (42). С. 17–23. DOI: 10.34822/1999-7604-2021-2-17-23.

5. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. P. 1335. DOI: 10.3390/s22041335.

6. Банокин П.И. Модель поведения пользователя корпоративной информационной системы // Доклады Томского государственного университета систем управления и радиоэлектроники. 2023. Т. 26. № 4. С. 78–83. DOI: 10.21293/1818-0442-2023-26-4-78-83.

7. Брумштейн Ю.М., Васьковский Е.Ю., Куаншкалиев Т.Х. Поиск информации в интернете: анализ влияющих факторов и моделей поведения пользователей // Известия Волгоградского государственного технического университета. 2017. № 1 (196). С. 50–55.

8. Кузнецов А.А. Построение модели поведения пользователя на веб-ресурсе средствами Process Mining // Современные научные исследования и инновации. 2015. № 5-2 (49). С. 36–47.

9. Cai C. Exploration on Data Mining Algorithms for University Information Systems Based on Big Data Environment // The proceedings of International Conference on Computer Simulation and Modeling, Information Security (Buenos Aires, Argentina, 15–17 November 2023). 2023. P. 626–632. DOI: 10.1109/CSMIS60634.2023.00117.

10. Ряполова Е.И., Преснов А.А., Цветкова К.Е. Разработка метода мониторинга аномального поведения пользователя в распределенной информационно-вычислительной системе: построение математической модели // Инфокоммуникационные технологии. 2021. Т. 19. № 1. С. 80–91. DOI: 10.18469/ikt.2021.19.1.11.

11. Аль-Барри М.Х. Модель признакового пространства для выявления аномального поведения пользователей центров обработки данных методами машинного обучения // Известия Тульского государственного университета. Технические науки. 2022. № 10. С. 79–83. DOI: 10.24412/2071-6168-2022-10-79-84.

12. Шипилова Е.А., Некрылов Е.Е. Сравнительный анализ результатов машинного обучения и регрессионной модели траекторий поведения пользователей Онлайн-сервисов // Вестник Воронежского института высоких технологий. 2023. № 4 (47). С. 9–10.

13. Ряполова Е.И., Студянникова М.А. Разработка имитационной модели для исследования поведения пользователя в распределенных информационно-вычислительных системах // Инфокоммуникационные технологии. 2021. Т. 19. № 2. С. 207–216.

14. Саенко И.Б., Котенко И.В., Аль-Барри М.Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. 2022. № 2 (48). С. 87–97. DOI: 10.21681/2311-3456-2022-2-87-97.

15. Бессонов Н.В., Кожаринов А.С. Подход к формированию памяти интеллектуального агента при моделировании поведения пользователей социальной сети // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 4. С. 37–41.

16. Шпер В.Л. Пирамида Дилтса // Методы менеджмента качества. 2015. № 8. С. 58–59.

17. Бова В.В., Кравченко Ю.А. Биоинспирированный подход к решению задачи классификации профилей поведения пользователей в интеллектуальных Интернет-

сервисах // Известия ЮФУ. Технические науки. 2019. № 4 (206). С. 89–102. DOI: 10.23683/2311-3103-2019-4-89-102.

18. Сарин К.С. Гибридный алгоритм смешанной многокритериальной оптимизации «кукушкин поиск» с генетическим оператором скрещивания // Искусственный интеллект и принятие решений. 2024. № 2. С. 87–105. DOI: 10.14357/20718594240207.

19. Сидоренко Н.С., Нижник Н.С. Детерминанты девиантного поведения несовершеннолетних: значение правовой культуры при выборе личностью модели правового поведения // Общество и право. 2022. № 4 (82). С. 119–126.

20. Буйневич М.В. Моисеенко Г.Ю. Повышение «устойчивости» регламентов деятельности как способ противодействия неумышленному инсайдингу // Вопросы кибербезопасности. 2024. № 6 (64). С. 108–116. DOI: 10.21681/2311-3456-2024-6-108-116.

21. Исаев Р.А., Подвесовский А.Г. Визуализация графовых моделей: подход к построению метафор представления // Научная визуализация. 2021. Т. 13. № 4. С. 9–24. DOI: 10.26583/sv.13.4.02.

22. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3 (55). С. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

23. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4 (56). С. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

24. Тютюнник В.М., Громов Ю.Ю., Александров Е.Ю. Аналитические модели парирования негативных внешних воздействий на сетевую информационную систему // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2020. № 9. С. 15–20. DOI: 10.36535/0548-0027-2020-09-3.

25. 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.

26. Sun X., Yang G., Zhang J. A Real-time Detection Scheme of User Behavior Anomaly for Management Information System // The proceedings of IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (Chongqing, China, 12–14 June 2020). 2020. P. 1054–1058. DOI: 10.1109/ITNEC48623.2020.9084982.

References

1. Bujnevich M.V., Moiseenko G.Yu. Kombinirovanie raznorodnykh destruktivnykh vozdejstvij na informacionnuyu sistemu i protivodejstvie atakam (na primere insajderskoj deyatel'nosti i DDoS-ataki) // Informacionnye tekhnologii i telekommunikacii. 2023. T. 11. № 3. S. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36.

2. Vlasov D.S. K voprosu o motivacii insajdera organizacii i sposobakh ego klassifikacii // Ehlektronnyj setevoj politematicheskij zhurnal «Nauchnye trudy KuBGTU». 2022. № 1. S. 128–147.

3. Bujnevich M.V., Vlasov D.S., Moiseenko G.Yu. Kombinirovanie sposobov vyyavleniya insajderov bol'shikh informacionnykh sistem // Voprosy kiberbezopasnosti. 2024. № 3 (61). S. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.

4. Kurta P.A., Bujnevich M.V. Ontologicheskaya model' vzaimodejstviya pol'zovatelya s informacionnoj sistemoj v ramkakh polucheniya uslugi informacionnogo servisa // Vestnik kibernetiki. 2021. № 2 (42). S. 17–23. DOI: 10.34822/1999-7604-2021-2-17-23.

5. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. P. 1335. DOI: 10.3390/s22041335.

6. Banokin P.I. Model' povedeniya pol'zovatelya korporativnoj informacionnoj sistemy // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioehlektroniki. 2023. T. 26. № 4. S. 78–83. DOI: 10.21293/1818-0442-2023-26-4-78-83.

7. Brumshtejn Yu.M., Vas'kovskij E.Yu., Kuanshkaliev T.KH. Poisk informacii v internete: analiz vliyayushchikh faktorov i modelej povedeniya pol'zovatelej // Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. 2017. № 1 (196). S. 50–55.

8. Kuznecov A.A. Postroenie modeli povedeniya pol'zovatelya na veb-resurse sredstvami Process Mining // Sovremennye nauchnye issledovaniya i innovacii. 2015. № 5-2 (49). S. 36–47.

9. Cai C. Exploration on Data Mining Algorithms for University Information Systems Based on Big Data Environment // The proceedings of International Conference on Computer Simulation and Modeling, Information Security (Buenos Aires, Argentina, 15–17 November 2023). 2023. P. 626–632. DOI: 10.1109/CSMIS60634.2023.00117.

10. Ryapolova E.I., Presnov A.A., Cvetkova K.E. Razrabotka metoda monitoringa anomal'nogo povedeniya pol'zovatelya v raspredelennoj informacionno-vychislitel'noj sisteme: postroenie matematicheskoj modeli // Infokommunikacionnye tekhnologii. 2021. T. 19. № 1. S. 80–91. DOI: 10.18469/ikt.2021.19.1.11.

11. Al'-Barri M.Kh. Model' priznakovogo prostranstva dlya vyyavleniya anomal'nogo povedeniya pol'zovatelej centrov obrabotki dannykh metodami mashinnogo obucheniya // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2022. № 10. S. 79–83. DOI: 10.24412/2071-6168-2022-10-79-84.

12. Shipilova E.A., Nekrylov E.E. Sravnitel'nyj analiz rezul'tatov mashinnogo obucheniya i regressionnoj modeli traektorij povedeniya pol'zovatelej Onlajn-servisov // Vestnik Voronezhskogo instituta vysokikh tekhnologij. 2023. № 4 (47). S. 9–10.

13. Ryapolova E.I., Studyannikova M.A. Razrabotka imitacionnoj modeli dlya issledovaniya povedeniya pol'zovatelya v raspredelennykh informacionno-vychislitel'nykh sistemakh // Infokommunikacionnye tekhnologii. 2021. T. 19. № 2. S. 207–216.

14. Saenko I.B., Kotenko I.V., Al'-Barri M.Kh. Primenenie iskusstvennykh nejronnykh setej dlya vyyavleniya anomal'nogo povedeniya pol'zovatelej centrov obrabotki dannykh // Voprosy kiberbezopasnosti. 2022. № 2 (48). S. 87–97. DOI: 10.21681/2311-3456-2022-2-87-97.

15. Bessonov N.V., Kozharinov A.S. Podkhod k formirovaniyu pamyati intellektual'nogo agenta pri modelirovanii povedeniya pol'zovatelej social'noj seti // Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki. 2019. № 4. S. 37–41.

16. Shper V.L. Piramida Diltsa // Metody menedzhmenta kachestva. 2015. № 8. S. 58–59.

17. Bova V.V., Kravchenko Yu.A. Bioinspirirovannyj podkhod k resheniyu zadachi klassifikacii profilej povedeniya pol'zovatelej v intellektual'nykh Internet-servisakh // Izvestiya YuFu. Tekhnicheskie nauki. 2019. № 4 (206). S. 89–102. DOI: 10.23683/2311-3103-2019-4-89-102.

18. Sarin K.S. Gibridnyj algoritm smeshannoj mnogokriterial'noj optimizacii «kukushkin poisK» s geneticheskim operatorom skreshchivaniya // Iskusstvennyj intellekt i prinyatie reshenij. 2024. № 2. S. 87–105. DOI: 10.14357/20718594240207.

19. Sidorenko N.S., Nizhnik N.S. Determinanty deviantnogo povedeniya nesovershennoletnikh: znachenie pravovoj kul'tury pri vybore lichnost'yu modeli pravovogo povedeniya // Obshchestvo i pravo. 2022. № 4 (82). S. 119–126.

20. Bujnevich M.V. Moiseenko G.Yu. Povyshenie «ustojchivostI» reglamentov deyatel'nosti kak sposob protivodejstviya neumyshlennomu insajdingu // Voprosy kiberbezopasnosti. 2024. № 6 (64). S. 108–116. DOI: 10.21681/2311-3456-2024-6-108-116.

21. Isaev R.A., Podvesovskij A.G. Vizualizaciya grafovykh modelej: podkhod k postroeniyu metafor predstavleniya // Nauchnaya vizualizaciya. 2021. T. 13. № 4. S. 9–24. DOI: 10.26583/sv.13.4.02.

22. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 1. Predposylki i skhema // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

23. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 2. Algoritm, model' i ehksperiment // Voprosy kiberbezopasnosti. 2023. № 4 (56). S. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

24. Tyutyunnik V.M., Gromov Yu.Yu., Aleksandrov E.Yu. Analiticheskie modeli parirovaniya negativnykh vneshnikh vozdejstvij na setevuyu informacionnuyu sistemu // Nauchno-tekhnicheskaya informaciya. Seriya. 2: Informacionnye processy i sistemy. 2020. № 9. S. 15–20. DOI: 10.36535/0548-0027-2020-09-3.

25. Vlasov D.S. Mul'tikriterial'naya model' sistematizacii sposobov obnaruzheniya insajdera // Voprosy kiberbezopasnosti. 2024. № 2 (60). S. 66–73. DOI: 10.21681/2311-3456-2024-2-66-73.

26. Sun X., Yang G., Zhang J. A Real-time Detection Scheme of User Behavior Anomaly for Management Information System // The proceedings of IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (Chongqing, China, 12–14 June 2020). 2020. P. 1054–1058. DOI: 10.1109/ITNEC48623.2020.9084982.

Информация о статье:
Статья поступила в редакцию: 13.12.2024; одобрена после рецензирования: 26.12.2024;
принята к публикации: 28.12.2024

The information about article:
The article was submitted to the editorial office: 13.12.2024; approved after review: 26.12.2024;
accepted for publication: 28.12.2024

Информация об авторах:
Буйневич Михаил Викторович, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN-код: 9339-3750
Моисеенко Григорий Юрьевич, руководитель направления Министерства обороны Российской Федерации (119160, Москва, ул. Знаменка, д. 19), e-mail: mogreq@mail.ru

Information about authors:
Buinevich Mikhail V., professor department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN: 9339-3750
Moiseenko Grigory Yu., head of direction, Ministry of defense of the Russian Federation, (119160, Moscow, st. Znamenka, 19), e-mail: mogreq@mail.ru