На правах рукописи

СМИРНОВ Дмитрий Владимирович

МЕТОДЫ ПОИСКА ПРИЗНАКОВ ИНСАЙДЕРА В BIG DATA

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2021

Работа выполнена в Федеральном исследовательском центре «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН)

Научный руководитель: **Грушо Александр Александрович**
доктор физико-математических наук, профессор

Официальные оппоненты: **Зегджа Петр Дмитриевич**
доктор технических наук, профессор,
директор Специализированного научно-учебно-исследовательского центра защиты информации,
профессор Института кибербезопасности и защиты информации

Смирнов Сергей Николаевич
доктор технических наук, профессор, профессор кафедры ИУ-10 (защита информации) МГТУ им. Н. Э. Баумана

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники»

Защита диссертации состоится «___» _____ 2021 г. в 16 ч. 00 м. на заседании диссертационного совета Д 002.073.02 при Федеральном исследовательском центре «Информатика и управление» Российской академии наук по адресу: 119333, г. Москва, ул. Вавилова, д.44, кор.2.

С диссертацией можно ознакомиться в библиотеке Федерального исследовательского центра «Информатика и управление» Российской академии наук по адресу: г. Москва, ул. Вавилова, д.44, кор. 2 и на сайте www.frccsc.ru.

Автореферат разослан «___» _____ 2021 г.

Ученый секретарь
диссертационного совета Р. В. Разумчик

Общая характеристика работы

Актуальность темы. Кража персональных данных совместно другими конфиденциальными данными такими как остаток на счете, портфель ценных бумаг, ИНН с движением средств по счету и т. д. позволяет злоумышленникам производить целевые атаки на физические лица, собирать информацию о конкурирующих фирмах и т. д.

При этом крупные организации встроили в свою инфраструктуру достаточно много технических средств защиты. Технические средства защищают от атак, исходящих из-за периметра организации (внешние атаки): DDOS-атаки, побор паролей, обход сетевых экранов, заражение вирусами, эксплуатация уязвимостей операционной системы. Именно по причине наличия адекватных технических средств защиты, крупные организации относительно хорошо защищены от внешних атак. Также внешние атаки весьма дорогостоящие и гораздо менее экономически выгодны по сравнению с использованием внутреннего злоумышленника (инсайдера), который может, например, своими руками или руками коллег выгрузить конфиденциальные данные на флэш-носитель, переслать через электронную почту, изъять зашифрованный жесткий диск из рабочей станции или сервера и т.д. Используя свои должностные полномочия и сетевые привилегии, инсайдер может провести ряд легальных процедур по выводу информации из защищенных контуров и хранилищ данных. Наибольшую ценность для инсайдера представляют объекты концентрации данных – хранилища (Big Data). Для борьбы с инсайдерскими активностями используется ряд технических средств такие как DLP, SIEM и т. д., но данные средства производят мониторинг нелегальных каналов, а инсайдеры используют легальные каналы движения информации. Инсайдерские атаки становится не только более экономически выгодным способом кражи информации, а часто единственно возможным.

В данной работе представлены результаты исследований возможностей выявления признаков внутренних инсайдерских угроз, где стандартные технические средства защиты не дают результата.

Таким образом, инсайдерские угрозы — это вредоносные для организации активности, которые исходят от сотрудников внутри организации (периметра защиты), в частности – от действующих работников, бывших работников, подрядчиков, деловых партнеров и даже завербованных работников или работников, специально внедренных в организацию, которые обладают доступом к конфиденциальной информации по своим должностным обязанностям и которые имеют представление о системе управления информационной безопасностью организации.

Журналы аудита действий сотрудников в комплексе Big Data тоже является Big Data, но меньшего объема (~10%). Поэтому для поиска признаков инсайдерской активности, то есть вкраплений таких признаков в данные о взаимодействиях большого количества пользователей с хранилищем Big Data необходимо научиться оперировать большими объемами текущей информации, анализируя ее и формируя рекомендации для принятия соответствующих управленческих решений в условиях жестких ограничений по времени. Именно этим обусловлено использование в подобном анализе систем искусственного интеллекта, с помощью которых обеспечивается выявление искомых признаков в больших данных в режиме требуемых ограничений по времени.

Итак, в данной диссертационной работе решается важнейшая научно-техническая задача обеспечения информационной безопасности, сформулированная как научно-техническая проблема поиска признаков вредоносных действий инсайдеров в Big Data в условиях больших и постоянно обновляемых данных при ограничениях на время поиска.

Поиск основан на том, что инсайдеры порождают аномалии, по которым удается выявлять признаки их активности. При этом необходимо, чтобы сформированные в процессе такого анализа рекомендации были объясняемы и понятны экспертам по противодействию инсайдерским активностям – работникам оперативных служб безопасности, ведь именно на них в конечном итоге ложится ответственность за принятые решения и их последствия. Например, могут ли выявленные признаки проявиться случайно, за счет больших уклонений при обработке огромного объема обрабатываемы данных. Это - проблема борьбы с «ложными тревогами». Или же проблема: можно ли не пропустить вредоносные признаки инсайдера в условиях больших гетерогенных данных? Наконец, как создать техническую систему обработки больших данных, которая реально решает задачи поиска признаков деятельности инсайдеров?

Необходимо отметить российских ученых П.Д. Зегжда, И.В. Котенко, А.А. Грушо, Е.Е. Тимонина, М.И. Забежайло и иностранных специалистов D. Cappelli, A. Moor, T. Senator, M. Bishoh, M. Salem, O. Backley, B. Ruttenbtrg, получивших серьезные результаты в этой области.

Для решения поставленной научно-технической проблемы **необходимо** разработать методы и программные «инструменты» работы с Big Data гетерогенной информации о действиях большого числа пользователей, которые позволяют:

- выделять без потерь в этих данных описания *взаимодействий*, несущих потенциальные или же явные риски вредоносных последствий – **выделять *вредоносные взаимодействия***,
- организовать подобный процесс фильтрации Big Data **эффективным образом**, в частности, i) разработать соответствующие процедуры сокращения объемов детально анализируемых данных, сохраняющие тем не менее в этих данных соответствующие признаки вредоносности, ii) обеспечить реализуемость всего процесса фильтрации в рамках соответствующих ресурсных ограничений (бюджетов, выделяемых на эти цели основным бизнесом банка; сроков выполнения каждого цикла анализа данных и приятия решений; численности персонала соответствующей квалификации в службе безопасности и др.).

Из описания стоящей научно-технической проблемы следует, что:

Объект исследования - гетерогенная информация о действиях большого числа пользователей при взаимодействиях с большими хранилищами данных, возможно, содержащая сведения о *вредоносных действиях* персонала с ИТ-ресурсами объекта зашиты. Описания таких *вредоносных взаимодействий* могут содержаться в постоянно пополняемых новыми сведениями Big Data о «поведении» объекта защиты.

Предмет исследования - модели, методы и технические возможности реализации поиска признаков инсайдеров в условиях Big Data, гетерогенности и пополняемости данных и ограничениях времени обработки данных.

Цель работы и задачи исследования. Цель – разработка методов выявления признаков инсайдерской активности в условиях Big Data, гетерогенности и пополняемости данных и ограничениях времени обработки данных, создание программно-технического решения - компьютерной системы для поддержки деятельности оперативных работников служб безопасности по выявлению признаков враждебной инсайдерской деятельности.

Создание *программно-технического решения* понимается как разработка комплекса ИТ-средств (при необходимости включающего в себя также обеспечивающие системные и аппаратные составляющие), в основу которого положены разработанные автором данной диссертационной работы и защищенные соответствующими авторскими свидетельствами программные продукты. При этом все необходимые аппаратно-программные дополнения (системное ПО, ранее приобретенные на рынке «типовые» инструментальные ИТ-решения и т.п.) задействованы в таких комплексах в соответствии с корпоративными политиками в области защиты данных и обеспечения кибербезопасности.

В соответствии с целью определены следующие **задачи исследования:**

1. Проанализировать представленные в профильной литературе данные по моделям, методам и алгоритмам выявления признаков вредоносных инсайдерских активностей.
2. Исследовать возможности и условия выявляемости признаков деятельности инсайдеров в условиях Big Data информации мониторинга, гетерогенности и пополняемости данных и ограничениях времени обработки данных.
3. Разработать методы интеллектуального анализа данных, позволяющие управлять балансом между детальностью представления знаний и объемами при поиске признаков вредоносных инсайдерских активностей.
4. Разработать комплекс программных средств, реализующих предложенные методы выявления признаков вредоносных инсайдерских действий и экспериментально продемонстрировать работоспособность и результативность разработанных методов.

Методология исследования. Для достижения поставленной цели и решения сформулированных в диссертационной работе задач использовались методы статистического анализа данных и машинного обучения, интеллектуального анализа данных, теории вычислительных систем и теории алгоритмов. Экспериментальные исследования осуществлялись с помощью моделирования процессов идентификации вредоносных инсайдерских активностей на тестовых стендах, в том числе имитирующих характеристики производительности вычислительной инфраструктуры крупной индустриальной организации.

Основные научные результаты, выносимые на защиту

1. Разработаны методы работы с противоречиями при выявлении аномалий в поведении сотрудников. В том числе, методы, обладающие свойствами изменять параметризацию среды и позволяющие управлять балансом между детальностью представления знаний

и объемами вычислений при поиске признаков вредоносных инсайдерских активностей.

2. Разработаны методы, позволяющие работать с гетерогенными данными, выявлять компрометирующие данные в различных информационных пространствах и объединять выявленные данные в единый результат.
3. Разработаны методы, позволяющие с помощью кластеризации Big Data и применения статистических методов выявлять сговор инсайдеров.
4. Разработаны методы оценки вероятности случайного возникновения аномалии, позволяющие ранжировать выявленные аномалии по вероятности и, позволяющие определить, является ли случайная аномалия рисковым событием.
5. Разработана методика анализа в ограниченное время большого потока данных, релевантных цели поиска признаков вредоносной деятельности инсайдера.
6. Разработан комплекс программных средств, обеспечивающих реализацию предложенной методики и проведены эксперименты, подтверждающие решение поставленной научно-технической задачи.

Научная новизна диссертационной работы определяется в первую очередь разработкой ***оригинальной методики*** аналитической оценки поведенческой активности пользователей и персонала, с помощью которой в режиме ограниченного времени можно обрабатывать большие объемы релевантных цели поиска операционных данных на предмет выявления признаков вредоносных инсайдерских активностей.

Методика опирается на разработанные автором диссертационной работы ***теоретические модели*** (использующие методы статистического анализа данных, интеллектуального анализа данных и машинного обучения), а также реализующие их ***алгоритмические конструкции***, позволяющие выявлять аномалии в отслеживаемых данных, вести в целях идентификации признаков инсайдеров их оперативный анализ, по результатам которого и формируются рекомендации для работников оперативных служб безопасности по целенаправленному противодействию выявленным инсайдерским активностям.

Теоретическая значимость исследования заключается в том, что данная работа не только систематизирует известные методы выявления инсайдеров, но и интегрирует их с новыми, разработанными автором в рамках данного диссертационного исследования, методами проблемно-ориентированного анализа данных (статистического анализа данных об аномалиях в поведении объектов мониторинга, интеллектуального анализа данных и машинного обучения при идентификации угроз и формировании рекомендаций по противодействию их влиянию), что позволило предложить принципиально новые эффективные способы выявления признаков инсайдерских активностей в информационной среде Big Data.

Практическая значимость исследования состоит в том, что экспериментально подтверждена работоспособность и результативность разработанных методов. Эти методы преобразованы в промышленное решение в виде программного комплекса в крупной коммерческой организации. Получены свидетельства на регистрацию программ для ЭВМ

и базы данных № 2021614494 «Аналитическая панель доступа данных», № 2021613506 «Поисковая система доступа к данным».

Реализация и внедрение результатов диссертационной работы. В результате исследований удалось построить систему, решающую практическую задачу поиска признаков инсайдера: разработанные в диссертации программные инструменты внедрены в промышленный контур крупного отечественного коммерческого банка, что подтверждено соответствующим актом о внедрении.

Достоверность и апробация результатов исследования подтверждается проведёнными экспериментами и моделированием, согласованностью с данными, имеющимися в отечественной и зарубежной литературе. Основные результаты работы докладывались и обсуждались на различных научных семинарах и конференциях, в том числе:

1. На семинаре в подразделении, реализовавшем (проприетарную) промышленную систему поиска признаков инсайдера в крупном коммерческом банке (10 заседаний семинара)
2. На совместном семинаре 53 и 16. отделов ФИЦ ИУ РАН.

Публикации. Всего автор опубликовал 7 научных статей. По теме диссертации опубликовано 6 научных статей в изданиях, рекомендованных ВАК [2-7], 4 статьи – в изданиях, индексированных в базах SCOPUS [3-6]. Одна статья в рецензированном журнале [1]. Получены свидетельства на регистрацию программ для ЭВМ и базы данных № 2021614494 «Аналитическая панель доступа данных», № 2021613506 «Поисковая система доступа к данным».

Личный вклад. Выносимые на защиту результаты получены соискателем лично. Результаты работ [1-5] получены автором лично, соавторы привлечены как консультанты. Работа [7] выполнена без соавторов.

Структура и объём диссертации. Диссертация состоит из введения, 4 разбитых на параграфы Глав, списка литераторы из 98 наименований. Объем текста диссертации составляет 144 листа. Рисунков – 26. Таблиц – 3.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи работы, аргументирована научная новизна и практическая ценность задач, решаемых в диссертации. Кратко описаны основные результаты работы.

В первой главе приводится обзор представленных в научной литературе подходов и методик, которые в настоящее время используют для выявления признаков инсайдеров. Обзор охватывает примерно пять десятков источников. Из рассматриваемых разновидностей инсайдерских угроз выделены 3, которым уделено приоритетное внимание:

1. *«Second streamers».* По оценкам организации Gartner, 62% инсайдеров – это т.н. «second streamers», люди, которые ищут дополнительный доход. Такой тип угрозы практически не

зависит от должности, которую инсайдер занимает в компании, т.е. злоумышленником может оказаться как стажер, так и человек из руководящего состава. Только 14% людей, которые неоднократно похищали данные, работали управляющими, и примерно у 2/3 этих сотрудников был доступ к секретным данным. А у 1/3 не был, и они этот доступ как-то организовывали. Проблема усложняется тем, что профессиональные киберпреступники, а также заинтересованные в добывании данных или мошеннические преступные группы часто предпринимают попытки завербовать сотрудников, в том числе дистанционно, через интернет. Оказывается, что в значительной доле случаев - легче подкупить инсайдера, чем организовывать дорогие и масштабные технические многовекторные атаки.

2. *Сговоры*. По оценкам организации Community Emergency Response Team (CERT), процент сговоров с участием инсайдеров (в т. ч. нескольких инсайдеров) от общего количества инсайдерских угроз оценивается на уровне 48.32%. Доля сговоров, в которых участвуют инсайдеры и сторонние злоумышленники, составляет 16.75%. Выделяют несколько форматов таких угроз: a) около 37% инцидентов – это мошенничество; b) 24% – кражи интеллектуальной собственности, c) 6% инцидентов – это комбинированные мошенничества и кражи. По сведениям того же источника, категория инцидентов с участием инсайдеров, включая сговоры, – одна из тех, которые наносят компаниям наибольший финансовый ущерб. И расследования таких случаев длятся в среднем в четыре раза дольше, по сравнению со случаями, когда инсайдер действует в одиночку.

3. *Недовольные сотрудники*. Последняя категория инсайдеров – сотрудники, которые занимаются вредительством или саботажем, похищая информационную собственность. По данным Gartner, 29% тех сотрудников, которые становятся инсайдерами - воруют данные после того, как их увольняют, и только в 9% это ничем не мотивированное хулиганство или вредительство. Большая часть инсайдеров-одиночек — это сотрудники, которые считают, что их не оценили по достоинству. Некоторые недовольные сотрудники могут начать «копать» информацию, не руководствуясь какой-то определенной целью. Другие же, могут искать очень специфические данные, когда получают извещение об увольнении за две недели. В течение этого времени они находят возможности, чтобы продать торговые секреты конкурентам.

Основные элементы предлагаемых в литературе методик выявления инсайдерских активностей характеризуются следующими аспектами:

a) М*атематическими методами* и *процедурными схемами,* в том числе психологическими и социальными теориями, техникой honeypot, методами выявления аномалий, которые включают:

- анализ локальных уровней выброса (LoF),
- метод опорных векторов,
- байесовский индуктивный вывод,
- кластеризацию методом *k*-средних, iForest и др.,
- графовыми методами – анализом структуры графа, анализом сообществ в графе и др.,
- методами теории игр и др.

b) Д*анными*, в том числе:

- особенностями их семантики и синтаксиса (почтовой переписки, данными по полномочиям сотрудников и др.),

- операциональными особенностями (характеристиками цифровых сред и инфраструктуры, журналов обращений к базам данных – SQL-запросов и др.),
- различными видами контекстной информации (временем, датой, странами, городами, офисами, помещениями и т.п.).

Выполненный обзор позволяет сделать следующие **выводы**: в рассмотренных методиках предлагается использовать лишь однородные данные (например, только данные по сетевой активности сотрудника, его доступам к базам данных и т.д.), что влечет наследование ошибок и коллизий, зацикливание или размножение ошибок и др. Как следствие, профильные службы ищут данные из *иных* по природе источников для *подтверждения* или выявления *значимых расхождений*. Следовательно, для выявления признаков инсайдера, требуется только *совокупность* данных, описывающих *различные* области деятельности и жизни человека в разных сферах, его поведения в работе, как пользователя ИС и т.д. Особую значимость при оценке возможной причастности к утечкам информации имеет учет характеристик личности сотрудников, попадающих в круг подозреваемых. Эффективность анализа, использующего однородные данные в таких случаях сомнительна, т.к. инсайдер обычно достаточно умен, профессионален, и именно поэтому ему доверен доступ к обработке ценной информации, следовательно, он знает способы, позволяющие обойти системы контроля. Таким образом, анализ инсайдерской активности нужно проводить по всему спектру сведений – как из эксплуатируемых технических систем и систем контроля, так и с учетом информации из реальной жизни персонала – данных HR-служб, оперативной информации служб собственной безопасности или детективных агентств, баз данных различного назначения (разного рода справочных систем, в том числе баз правоохранительных и других гос. органов, социальных сетей, данных кадровых агентств и т.д.). Чем разнообразнее исходные данные, – тем точнее работа моделей, и тем более тонкие, малозаметные отклонения можно проанализировать (чем “дальше” по своей природе данные друг от друга, тем ценнее их взаимосвязанный анализ). Следует подчеркнуть, что в обозреваемых методиках не ставится задача анализа взаимодействий пользователей с хранилищами Big Data и ограничениями на время анализа, хотя наиболее ценная для целей поиска признаков вредоносной инсайдерской активности информация аккумулируется именно во взаимодействиях пользователей с хранилищами Big Data.

Во второй главе рассмотрены методы работы с противоречиями при выявлении аномалии в поведении сотрудников, а также методы, позволяющие оперировать гетерогенными данными и выявлять компрометирующие сведения в различных информационных пространствах, объединяя выявленные данные в единый результат.

Представлены возможности описания конечных классов объектов в форме множества характеристик – параметров (параметризации рассматриваемых классов). Рассмотрены [4] задачи выявления причины того, что некоторые объекты заданного класса C обладают определенным свойством P. В ситуациях, когда для решения этой задачи при появлении новых объектов исходного множества характеристик может не хватить, предложены процедуры изменения начальной параметризации, позволяющие уточнять эмпирические причины появления целевого свойства P при расширении

исходных данных новой информацией. Предлагаемые методы иллюстрируются на практических примерах их применения. В частности, демонстрируется, как при появлении противоречий при объяснении зафиксированной аномалии можно подключить и проанализировать дополнительные данные, а затем “глубже” проанализировать существующие данные, что позволяет устранить зафиксированное ранее противоречие.

При этом особенности Big Data – это, в том числе, и расширяющиеся данные, разнородные по своей «природе» (гетерогенные, представляемые различными информационными пространствами со своим специфическим типом данных). Инструменты обработки данных объектно-ориентированы и позволяют обрабатывать именно тот тип данных, под который они создавались. Представлен разработанный в диссертации метод, позволяющий работать с гетерогенными данными и выявлять компрометирующие данные в различных информационных пространствах, объединяя полученные заключения в единый результат [3]. Полученный единый результат обработки нескольких информационных пространств далее предоставляется оперативному сотруднику через пользовательский интерфейс. Таким образом, в задаче поиска инсайдеров разработан подход к объединению компрометирующих данных, наблюдаемых в различных информационных пространствах. При этом накопление информации в каждом пространстве рассматривается как вероятностный процесс. Рассматриваемый подход основан на запретах и полузапретах вероятностных мер в различных информационных пространствах. С последовательностями событий, наблюдаемыми в таких информационных пространствах, связываются булевы переменные. Появление полузапретов соответствует значению «1» соответствующих булевых переменных. Последовательности булевых переменных в различных информационных пространствах легко связываются с помощью логических выражений. Эти выражения описывают опасные сводные тенденции, наблюдаемые в анализируемых информационных пространствах.

В третьей главе рассмотрены методы, позволяющие сегментировать анализируемые Big Data на такие однородные фрагменты (сегменты), где возможно применять методы математический статистики и методы оценки вероятности возникновения аномалии.

Проблема выявления организованной группы нарушителей информационной безопасности является одной из самых сложных задач обеспечения безопасности организации. Исходное множество данных для анализа состоит из большого множества малых выборок, описывающих функционал информационных технологий организации. Ввиду его размеров это множество можно считать большими данными. Для сокращения объема исходных данных использован метод кластеризации. Это позволило [5] эффективно использовать методы математической статистики, т.е. выявить малые выборки, несущие информацию о враждебных инсайдерах. Сложность задачи заключалась в том, чтобы как можно меньше потерять искомых малых выборок.

Пусть транзакция обрабатывается случайной парой менеджеров (u,u'), $u \in U_1$, $u' \in U_2$. Положим $|U_1| = n_1$, $|U_2| = n_2$, $|U_1 \times U_2| = n_1 \cdot n_2 = n$. Тогда вероятность появления пары (u,u') равна $\frac{1}{n}$.

Если (u_1, u_2) – инсайдеры, использующие сговор, и клиент v представляет для них интерес, то вероятность того, что эта пара будет обслуживать этого клиента равна

$$\mathrm{P}\left((u_1, u_2) \mid v\right) = p,$$

и в случае любой другой пары $(u, u') \neq (u_1, u_2)$ эта вероятность равна

$$\mathrm{P}\left((u, u') \mid v\right) = (1-p)\frac{1}{n-1}.$$

С помощью методов кластеризации можно выделить множество V_1 тех клиентов, которые представляют интерес для инсайдеров, использующих сговор. Ясно, что мощность множества V_1 много меньше, чем мощность множества V.

Пусть C_1 - среднее число транзакций у клиентов из множества V_1. Тогда средний объем данных для клиентов из множества V_1 равен $|V_1| \cdot C_1 = m$. Далее считаем m известным параметром схемы. Тогда соотношение параметров m, n, p определяет возможность выявления инсайдеров, использующих сговор. Поскольку числа m и n являются большими, то рассмотрение задачи выявляемости инсайдеров (u_1, u_2) в множестве V_1 будет вестись в терминах асимптотических распределений вероятностей в схеме серий, т.е. в предположении, что $m \to \infty, n \to \infty, p \to 0$. Пусть $m \to \infty, n \to \infty$ удовлетворяет условию $\frac{\alpha}{\ln n} \to 0$, где $\alpha = \frac{m}{n}$, и $p \le \frac{\ln m}{m}$. Тогда превышение числа появлений пары (u_1, u_2), начиная с 4, однозначно идентифицирует эту пару инсайдеров с вероятностью, стремящейся к 1.

Исследованы возможности использования различных подходов к описанию диагностики действий инсайдеров при анализе больших эмпирических данных. В задачах этого типа необходимо установить (спрогнозировать, диагностировать, и др.) наличие или отсутствие целевых свойств у каких-либо пользователей из заданного множества. Оценка правильности используемых при этом правдоподобных рассуждений выполняется на основе оценок вероятностей случайного появления найденных закономерностей в простейших вероятностных моделях. Показано [6] при каких соотношениях параметров возможно эффективное выявление корреляционных связей между событиями, с помощью которых можно идентифицировать признаки вредоносной активности инсайдеров.

Указаны два способа управления соотношениями между параметрами, позволяющие получать содержательную информацию о потенциально опасных активностях. Первый способ основан на разделении периода наблюдений на промежутки, в течение которых искомая корреляция может проявиться. Второй способ связан со способами сокращения множества пользователей, которые потенциально могут стать инсайдерами. Т.е. речь идет о формировании кластеров, в которых вероятностные оценки становятся работоспособными. Искомые соотношения между параметрами для поиска корреляций можно определять с помощью предельных теорем в схеме серий.

В четвертой главе представлена разработанная автором методика [7] анализа в ограниченное время большого потока данных, релевантных цели поиска признаков действий инсайдеров.

На основе сравнения наиболее широко используемых в обсуждаемой предметной области коммерческих корпоративных поисковых систем выделен перечень основных функций таких программно-технических инструментов. Обозначены критически значимые их характеристики: скорость индексации первичных данных, и их переиндексации – обновления индексов с приходом новой информации, поддерживаемые API, взаимосвязи текущих размеров базы и скорости поиска, поддерживаемые типы входных документов и др.

Определены параметры целевой ИТ-среды анализа данных и поддержки принятия решений для реального объекта защиты в решаемой задаче идентификации признаков вредоносной инсайдерской активности в крупном российском коммерческом банке. Это комплекс постоянного накапливания и обработки Big Data, охватывающий, примерно, 2000 серверов и более 120 промышленных информационных ресурсов (источников данных). Данный комплекс Big Data, в силу специфики решаемых на его базе бизнес-задач, является динамической структурой, конфигурация которой варьируется в части увеличения или же, наоборот, уменьшения, примерно на 10 серверов ежесуточно. В этом комплексе одновременно работают несколько тысяч специализированных сотрудников-аналитиков данных, в задачи которых входит обеспечение полного цикла анализа данных и принятия соответствующих решений (подготовка данных, разработка моделей и т.д.). Требуемых для их работы так называемых *полезных* данных - порядка десятка петабайт при общем объеме накапливаемой и обрабатываемой информации в несколько раз больше. *Полезные* данные представлены как более чем сотня баз данных и несколько сотен аналитических продуктов (витрин данных).

Разработанные методика и программный инструментарий выявления признаков инсайдера реализованы в специализированном комплексе меньшего, однако также вполне внушительного размера (примерно 6% от общего парка серверов Big Data). Данный инструментальный комплекс порождает несколько десятков терабайт так называемых «сырых» данных в сутки, которые необходимо обрабатывать (фильтровать, приводить к нормализованному виду, индексировать, …), чтобы постоянно обеспечивать требуемые ограничения по времени для обновления\актуализации параметров системы мониторинга и защиты основного комплекса Big Data.

Созданный инструментарий защиты имеет два различных типа интерфейсов, ориентированных на задачи формализованного представления знаний для так называемых *первичного* и *вторичный* поиска. *Первичный* поиск характеризуется классом задач, где аналитик выявляет в исходных «сырых» данных те данные, которые являются релевантными отдельно накапливаемым знаниям в соответствии с текущим профилем угроз. *Первичный* поиск аккумулирует уже накопленный опыт экспертов служб безопасности о признаках наблюдавшихся ранее инсайдерских активностей и определяет необходимые характеристики поиска в «сырых» данных (поля, идентификаторы и т.п.). Далее, с использованием специальных средств машинного обучения и опираясь на прецеденты ранее идентифицированных инсайдерских атак, из текущих «сырых» данных

выделяется вся та информация, которая затем будет использоваться для поддержки текущей работы служб безопасности, то есть мониторинга основного комплекса Big Data на предмет идентификации в его текущей операционной работе тех или иных аномальных активностей а также организации противодействия противоправным действиям инсайдерского характера.

Вторичный поиск обеспечивает оперативное отображение и ответы на релевантные целям анализа безопасности запросы (это - своего рода «локальный Яндекс»). Используя вторичный поиск, оперативный сотрудник может ввести необходимые идентификационные данные (ФИО, табельный номер или источник данных и др.) и посмотреть детальный профиль соответствующего сотрудника или подразделения, в том числе, штатный профиль доступов данного сотрудника к ресурсам хранилища Big Data. При разработке обсуждаемой методики и комплекса реализующих ее программно-технических средств были выделены 4 группы типичных для работы с Big Data барьеров, для преодоления которых пришлось создавать проблемно-ориентированные решения:

1. Ограничения по времени для анализа текущего объема постоянно пополняемых больших данных (эффекты *Big* и *Open)*. Требующие анализа большие данные о работе большого множества пользователей с хранилищем используемой информации необходимо обрабатывать в условиях жестких ограничений по времени, обеспечивая «упаковку» всех необходимых стадий обработки в жесткие сроки анализа данных и принятия решений. При этом следовало учитывать постоянные динамические изменения в объекте мониторинга и регулярное поступление новых данных.
2. Интеграция данных, извлекаемых из различных источников. Интеграция данных, отбираемых из различных источников «сырых» первичных данных представляет собою нетривиальную задачу: необходимо в условиях жестких ограничений по времени отбирать релевантную целям мониторинга информацию из огромного перечня объектов (ресурсов), характеризуемых своими собственными типами представления данных. Для преодоления таких барьеров был предложен и реализован в виде программных инструментов ряд эвристик, отражающих зарекомендовавшую себя на практике «логику» оперирования с разнородными данными – «склеивания» согласуемых данных.
3. Нормализация данных. Пользователи сервисов вторичного поиска при работе со средствами диалогового интерфейса допускают различного рода неточности и\или ошибки в именовании искомого объекта. Именно это обстоятельство потребовало разработки соответствующих средств автоматической идентификации и коррекции ошибок (клавиатурных ошибок, опечаток, «ослышек» и т.п.).
4. Ресурсные ограничения. Операциональные характеристики разрабатываемого комплекса средств защиты должны быть результативны и практически эффективны. При этом термин *результативность* понимается как демонстрируемая на практике способность разработанных программно-технических решений обеспечивать выявление действий инсайдеров за ограниченное время в крупном отечественном коммерческом банке. В свою очередь, термин *практическая эффективность* понимается как способность разработанных программно-технических решений «вписываться» в предъявляемые требованиями основного бизнеса объекта защиты

ресурсные ограничения – на размеры бюджетов, выделяемых на эти цели основным бизнесом банка; на сроки выполнения каждого цикла анализа данных и принятия решений; на численности персонала соответствующей квалификации в Службе безопасности и др. Все эти ограничения могут быть в установленном порядке оформлены в виде необходимых корпоративных Соглашений об уровне сервиса (Service Level Agreement), соответствующие их нарушению риски захеджированы заранее согласованными объемами резервов на такие риски.

Стоимость инструментального комплекса защиты от инсайдерских активностей не должна превышать 10% процентов от стоимости собственно объекта защиты.

Для преодоления названных барьеров был предложен ряд специальных решений по организации обработки данных. Так, в частности, в рамках защиты от вредоносных инсайдерских активностей:

1. При обработке исходных «сырых» данных на первом этапе их фильтрации «стартовые» несколько десятков терабайт характеристик анализируемых событий удалось «ужать» без потерь данные до 600 Гб (1,5 млрд. записей об анализируемых активностях).
2. Далее на 2-м этапе фильтрации данных эти 600 Гб «ужали» без потерь до 2 гигабайт (3 млн записей).
3. Удалось добиться, чтобы индексы вторичного поиска обновлялись в режиме имеющихся ограничений процессно-реального времени, а время отклика на запрос не превышало 10 сек. на выделенном для этого программно-техническом комплексе.

Разработанная методика идентификации признаков инсайдерской активности основана на формировании актуальной модели угроз. Модель угроз формализуется в виде Профиля Угроз (ПУ), представляющего собою постоянно поддерживаемый в актуальном состоянии перечень так называемых Типовых Сценариев (ТС). Каждый из Типовых Сценариев порождается обобщением опыта оперативных сотрудников, вовлеченных в расследования конкретных случаев мошенничества (инсайдерских активностей). Опыт оперативных сотрудников сперва фиксируется в виде текстового описания, а далее преобразуется в машиночитаемый формализованный вид. При этом задействовано промежуточное представление знаний о каждом из ТС в виде фрейма. Для описания данных в слотах подобных фреймов предусмотрены иерархии типов данных (от булевских значений признаков – Да\Нет, до графов параметров и отношений между такими параметрами с метками на вершинах и ребрах, а также текстовых комментариев, в т.ч. - в виде Binary Large Objects).

Подобные иерархии типов данных могут быть задействованы в случае необходимости получения более тонкой «дифференциации» состояний НОРМА\АНОМАЛИЯ с использованием более детального представления знаний об анализируемых инцидентах, извлекаемых из соответствующих информационных пространств (см. выше Главы 1-3). Простейший вариант представления знаний в ТС из ПУ – использование булевских значений Да\Нет, позволяющих описать каждый такой фрейм в виде множества, характеризующих именно его признаков (см. схемы параметризации из Главы 2). В свою очередь множество всех используемых при описании текущего ПУ

признаков определяет битовую строку, соответствующими единицами которой кодируется каждый из соответствующих ТС в ПУ. Обработка машиночитаемого описания фреймов, представленных в виде именно битовых строк, дает возможность получить существенный выигрыш в производительности при анализе текущих данных, т.к. позволяет организовать сравнение описания текущей ситуации с описаниями ТС средствами одной вычислительной макрооперации.

В формализованном виде текущий ПУ может быть описан как матрица, строки которой (при использовании булевского варианта представления знаний от ТС в соответствующих фреймах) представлены задействованными при описании угроз параметрами/признаками, а каждый из столбцов этой матрицы отображает соответствующий ТС.

Сравнивая элементы (ячейки) этой матрицы с характеристиками (профилем значений признаков) доступа к защищаемым ресурсам комплекса Dig Data, актуальными в данный момент для конкретного сотрудника, можно оценить (в т.ч. – с использованием статистических средств анализа рисков при идентификации аномалий – см. выше Главы 2-3) весомость угроз несанкционированных активностей этого сотрудника – релевантность его текущего поведения каким-либо известным угрозам из текущего ПУ. Однако, проведение таких сравнений «лобовым» методом «грубой силы» оказывается чрезвычайно ресурсоемким. Для сокращения объемов перебора при формировании «диагностических» заключений по каждому из отслеживаемых сотрудников используется диаграмма сходств ТС: определив бинарную алгебраическую операцию сходства описаний ТС можно построить диаграмму взаимной вложимости множеств признаков, задействованных в описаниях ТС. А далее (один раз сформировав такую диаграмму) проверять релевантность текущего анализируемого профиля доступов конкретного сотрудника имеющемуся ПУ, начиная со сравнения его элементов с элементами нижнего «этажа» (минимальных по вложению подмножеств признаков, одновременно актуальных для нескольких ТС) и далее двигаясь лишь по релевантным цепочкам частичного порядка этой диаграммы к ее верхнему «этажу» (подмножеств максимальных по числу актуальных общих признаков), а от него – к релевантным данной ситуации описаниям ТС. Формализованное описание переборных задач, возникающих при формировании Диаграммы Сходств (ДС) описаний ТС текущего ПУ представлено в Приложении 1 к диссертации.

В случае булевского представления данных об имеющихся ТС каждый такой ТС характеризуется как битовая строка. Таким образом можно вычислять сходства описаний ТС, используя стандартные для многих современных системных программных сред макро-операции с битовыми строками. Это позволяет работать с имеющимися Big Data достаточно быстро и эффективно, формируя результат сходства описаний ТС средствами соответствующей машинной макро-операции.

Предложенный подход позволяет существенным образом сократить - по сравнению с тактикой «грубой силы» - объемы необходимых вычислений: здесь один раз сформированная ДС позволяет последовательно вести проверки пересечений ее фрагментов с теми «релевантными» анализируемому профилю доступов конкретного сотрудника элементами диаграммы сходств ТС, которые размещены на ее цепочках

частичного порядка. В ситуации, когда речь идет о миллиардах событий и о сотнях ТС, этот способ дает возможность получить значительный выигрыш в скорости принятия финальных решений.

Дополнительный аргумент в пользу предлагаемого подхода – возможность организовать *проактивный* мониторинг негативного развития «аномальных» ситуаций, подсказывая конкретному сотруднику безопасности наиболее опасные варианты изменения отслеживаемой им конкретной ситуации (вдоль релевантных ей цепочек частичного порядка на диаграмме сходств ТС).

При разработке программных средств, реализующих предложенную методику идентификации инсайдерских активностей, пришлось уделить особое внимание нескольким типам алгоритмических проблем [2]. Поддержка изменений в «архитектуре» актуального ПУ потребовала разработки соответствующих программных инструментов экономного реинжиниринга структуры диаграммы сходств описаний ТС. Известно, что при порождении диаграммы сходств ТС в общем случае приходится иметь дело с объектом, размеры которого растут экспоненциально быстро при линейном росте размеров множества ТС. То есть, актуальной оказалась задача по снижению объема перебора локальных сходств описаний ТС при формировании текущей ДС. Для этого был разработан специальный программный инструмент со встроенными алгоритмом экономной организации генерации локальных сходств описаний ТС. Следуя подходу Rapid Application Development сперва в инструментальной среде Matlab был проведена отладка и проверка корректности этого алгоритма анализа данных и принятия решений, а далее на Python была реализована его промышленная версия, использующая возможности экономной обработки битовых строк. Вместе со специально разработанным проблемно-ориентированным графическим редактором, обеспечивающим аналитикам возможности формировать новые ТС и поддерживать ПУ в актуальном состоянии, эта промышленная Python-версия генератора диаграммы сходств описаний ТС образует ядро программного инструментария представления и обработки знаний о вредоносных инсайдерских активностях. Для поддержки информационных сервисов разработаны соответствующие пользовательские интерфейсы.

Вторичный поиск обеспечивается отдельной поисковой системой, пользовательский интерфейс которой поддерживает работу с текстовым полем для ввода запросов и кнопкой “искать”. Цель вторичного поиска - оперативно предоставлять информацию, включающую результаты работы алгоритмов машинного обучения, в простом и понятном виде для сотрудников, не имеющих продвинутых ИТ-навыков. Важнейший эффект, обеспечиваемый средствами вторичного поиска, — это ускорение работы оперативных сотрудников, занятых мониторингом и противодействием вредоносным инсайдерским активностям

В заключении приведены основные итоги и научно-практические результаты диссертационной работы, в частности – перечень основных результатов, которые выносятся на защиту, а также краткий обзор возможных направлений дальнейшего развития представленных в данной диссертационной работе исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Решена научно-техническая проблема поиска признаков вредоносной инсайдерской активности в Big Data информации о взаимодействии большого множества пользователей с большим хранилищем данных при допущении о пополнении новыми сведениями в условиях жестких ограничений времени анализа данных и поддержки принятия решений.

1. В результате разработаны, обоснованы и реализованы следующие методы и алгоритмы:
- **a)** интеллектуального анализа данных, обеспечивающие эффективный первичный поиск в "сырых"(неразмеченных) исходной Big Data информации о взаимодействии большого множества пользователей с большим хранилищем данных сведений, релевантных идентификации признаков вредоносных инсайдерских активностей;
- **b)** представления знаний об анализируемых угрозах в виде динамически пополняемого новыми данными профиля угроз, сформированного типовыми сценариями потенциально опасных действий инсайдеров, а также диаграммы сходств типовых сценариев угроз;
- **c)** идентификации и статистического анализа аномалий в поведении объектов мониторинга;
- **d)** методы оценки качества\надежности формируемых статистическими средствами заключений о классификации аномалий в поведении объектов мониторинга, дающие дополнительные основания для принятия решений о приоритетности отработки соответствующих "подсвеченных" ситуаций;
- **e)** метод выявления сговора инсайдеров, сочетающий методы кластеризации и статистических оценок.

2. Разработан программный комплекс, включающий в себя:
- a) набор сервисных программных инструментов, поддерживающих нормализацию данных как в первичном, так и во вторичном поиске;
- b) набор оригинальных программных инструментов формирования и реконструкции диаграммы сходств типовых сценариев используемого профиля угроз;
- c) проблемно-ориентированные средства имитационного моделирования для оценки ряда эффектов и поддержки принятия управленческих решений;
- d) предложения по интеграции вновь разработанных программных инструментов интеллектуального анализа данных (ИАД) с уже имеющимися в организации промышленными программными инструментами обработки данных.

3. Получено подтверждение работоспособности и результативности разработанных в диссертации методов в процессе создания промышленной реализации программных инструментов ИАД в деятельности крупной коммерческой организации.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. О комплексной аутентификации // Системы и средства информатики, 2017, том 27, № 3, с. 3-10.
2. Смирнов Д. В., Грушо А.А., Забежайло М.И., Тимонина Е. Е. Система сбора и анализа информации из различных источников в условиях Big Data // International Journal of Open Information Technologies, 2021. V. 9. № 4. Pp. 64-74. http://injoit.org/index.php/j1/article/view/1099 (ВАК- 05.13.19)
3. Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. Модель множества информационных пространств в задаче поиска инсайдера // Информатика и ее применения, 2017, том 11, № 4, с. 65-69. (Scopus, ВАК -05.13.19.)
4. Грушо А.А., Грушо Н.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. Параметризация в прикладных задачах поиска эмпирических причин // Информатика и ее применения, ИПИ РАН (М.), 2018, том 12, № 3, с. 62-66 (Scopus, ВАК -05.13.19.)
5. Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е., С.Я. Шоргин. Методы математической статистики в задаче поиска инсайдера // Информатика и ее применения, 2020. Т. 14. Вып. 3. С. 71-75 (Scopus, ВАК - 05.13.19.)
6. Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. О вероятностных оценках достоверности эмпирических выводов // Информатика и ее применения, 2020. Т. 14. Вып. 4. С. 3-8. (Scopus, ВАК - 05.13.19.)
7. Смирнов Д. В., Об одной методике проблемно-ориентированного анализа Big Data в режиме процессно-реального времени // International Journal of Open Information Technologies, 2021. V. 9. № 4. Pp. 64-74. http://injoit.org/index.php/j1/article/view/1099 (ВАК- 05.13.19)
8. Свидетельство о государственной регистрации программы для ЭВМ № 2021614494 «Аналитическая панель доступов к данным», дата государственной регистрации 25.03.2021.
9. Свидетельство о государственной регистрации программы для ЭВМ № 2021613506 «Поисковая система доступа к данным», дата государственной регистрации 19.04.2021.