DOI 10.37882/2223-2966.2024.02.22

ИНТЕЛЛЕКТУАЛЬНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ НА НЕФТЯНЫХ И ГАЗОВЫХ МЕСТОРОЖДЕНИЯХ

AN INTELLIGENT INFORMATION SECURITY MODEL FOR OIL AND GAS FIELDS

S. Lozovoy

Summary. The study raises a rather topical issue due to the improvement of the traditional process of dispatching control and data collection at oil and gas fields through the formation of an intelligent information security model. This study is devoted to the concept of an intelligent information security model in oil and gas fields based on a multi-agent approach. The article contains the advantages of a multi-agent approach to ensuring information security in oil and gas fields; the conceptual structure of the intellectual model of information protection in oil and gas fields; evaluation of the effectiveness of the proposed conceptual structure of the intellectual information security model based on an experiment, according to which it was noted that while maintaining high decision-making accuracy, the decision tree generated by experimental group A is much smaller than that of control group B, and the duration of the algorithm implementation is shorter, therefore, the effectiveness of decision-making by the attribute of the experimental group is higher in other words, the intelligent information security model proposed in this study for oil and gas fields, it is very effective.

Keywords: information protection, information security, intelligent model, oil and gas fields, multi-agent approach, conceptual structure.

Лозовой Сергей Викторович
Инженер по системам безопасности,
Sorror IT & Telecommunications Co, West Qurna-2 Project
sergeylozovoy80@gmail.com

Аннотация. В исследовании поднимается достаточно актуальный вопрос, обусловленный совершенствованием традиционного процесса диспетчерского управления и сбора данных на нефтяных и газовых месторождениях посредством формирования интеллектуальной модели защиты информации. Данное исследование посвящено концепции интеллектуальной модели защиты информации на нефтяных и газовых месторождениях, базирующейся на мультиагентском подходе. Статья содержит преимущества мультиагентского подхода к обеспечению информационной безопасности на нефтяных и газовых месторождениях; концептуальную структуру интеллектуальной модели защиты информации на нефтяных и газовых месторождениях; оценку эффективности предложенной концептуальной структуры интеллектуальной модели защиты информации на основе эксперимента, в соответствии с чем было отмечено, что при сохранении высокой точности принятия решения дерево решений, сгенерированное экспериментальной группой А, намного меньше, чем у контрольной группы В, а продолжительность реализации алгоритма короче, следовательно, эффективность принятия решения по атрибуту экспериментальной группы выше, другими словами, интеллектуальная модель защиты информации, предложенная в данном исследовании для нефтяных и газовых месторождений, является весьма эффективной.

Ключевые слова: защита информации, информационная безопасность, интеллектуальная модель, нефтяные и газовые месторождения, мультиагентский подход, концептуальная структура.

Введение

Система диспетчерского управления и сбора данных в современной сети управления промышленной автоматизацией широко используется в крупномасштабной сети нефтегазопроводов на нефтяных и газовых месторождениях [1]. Такая система диспетчеризации и сбора данных в сфере автоматизации управления и производственного процесса основана на информационно-компьютерных технологиях. Как система промышленной сети управления, диспетчеризация и сбор данных построены на универсальном компьютерном программном и аппаратном обеспечении, что приводит к уязвимости киберсистемы и увеличению её открытости в нефтегазовой отрасли. После установки системы в целях информационной безопасности нефтяных и газовых месторождений и в процессе её практической эксплуатации она не будет часто обновляться, что создаёт дополнительные проблемы, обнаруженные в последующем системе, которые трудно решить, при этом они создают существенные риски для информационной безопасности на нефтяных и газовых месторождениях [2; 3]. В то же время все больше нефтегазовых систем диспетчеризации управления и сбора данных позволяют обмениваться информационными данными с другими сетевыми моделями, поэтому существующие системы диспетчеризации управления и сбора данных практически полностью уязвимыми для внешних воздействий, следовательно возникает определённая угроза информационной безопасности на нефтяных и газовых месторождениях. Поскольку система диспетчерского управления и сбора данных выступает весьма крупным объектом нефтегазовой инфраструктуры, то, если нефтегазовая система, имеющаяся на предприятиях, подвергнется кибератаке и не будет достаточно быстро устранена, это приведет к значительному повреждению информационной системы и определённым денежным потерям. Кроме того, в связи с тем, что система диспетчерского управления и сбора данных является крупномасштабной базовой сетевой системой управле-

ния промышленной автоматизацией на нефтяных и газовых месторождениях, то информационной безопасности предприятий нефтегазовой отрасли уделяется много внимания зарубежными исследователями.

К. Хуан, К. Чжоу, Ю.К. Тянь в соавт. применили байесовскую модель для оценки рисков кибербезопасности на основе данных в сети диспетчеризации и сбора информационных данных, однако не обсуждали направления построения архитектуры информационной безопасности посредством интеллектуальной модели защиты информации [4].

Т. Марсио, С. Тара, З. Маеде в соавт. представили подход машинного обучения для испытаний диспетчеризации и сбора информационных данных для кибербезопасности, проанализировав пять традиционных алгоритмов машинного обучения, но распределенная защита информации, которая возможна при помощи использования интеллектуальной модели, не рассматривалась данными исследователями [5].

Дж. Мохаммади, Г. Хуг, С. Кар предложили агентно-ориентированную распределенную систему информационной безопасности с ограниченным оптимальным потоком производственной мощности на нефтяных и газовых месторождениях. Но агентский подход с машинным обучением не анализировался в качестве составляющей интеллектуальной модели защиты информации [6].

В крупномасштабной сетевой системе модель защиты информации, как правило, основана на многоуровневой распределенной структурой, что позволяет решать проблемы информационной безопасности в сетевой системе посредством сбора распределённых информационных данных, обработки и централизованного управления промышленной автоматизацией на нефтяных и газовых месторождениях [7].

Агентская крупномасштабная распределенная система защиты информации представляет собой новую концепцию и современную технологию, предложенную за рубежом. Эта новая модель широко изучалась исследователями, например, Г. Хелмер [8] впервые предложил агентскую систему обнаружения внешних вторжений в модель информационной безопасности.

Поскольку применение агентской технологии в распределенной системе обнаружения кибервторжений является основным в условиях защиты информации нефтегазовых компаний, в этом исследовании рассматривается интеллектуальная модель защиты информации, базирующаяся на мультиагентском подходе.

Актуальность работы

Исследование современного состояния нефтяных и газовых месторождений, а также формирования интеллектуальной модели защиты информации, основанной на мультиагентском подходе, является крайне актуальным и востребованным направлением в современных условиях развития информационных технологий и увеличения угроз кибербезопасности.

Нефтегазовые предприятия на сегодняшний день используют множество компьютерных систем и сетей для мониторинга и управления производственными процессами на нефтяных и газовых месторождениях. Однако с ростом зависимости от информационных технологий, также повышается и уровень угроз информационной безопасности. Кибератаки на промышленные объекты могут привести к значительным последствиям, таким как разрушение основного оборудования, производственным потерям, экологические катастрофы.

Мультиагентский подход предлагает нефтегазовым предприятиям интеллектуальное решение для эффективной защиты информации на нефтяных и газовых месторождениях. В рамках данного подхода, различные агенты, работающие автономно и совместно, обеспечивают мониторинг, детекцию и противодействие киберугрозам. Каждый агент выполняет специфическую функцию, например, мониторинг сетевой модели, анализ информационных данных или принятие управленческих решений об адаптации системы диспетчерского управления и сбора информационных данных к изменяющимся условиям.

Практическое применение интеллектуальной модели защиты информации на основе мультиагентского подхода на современном этапе отраслевого развития нефтегазовых предприятий позволяет выявлять и предотвращать кибератаки в реальном времени, обеспечивая информационную безопасность при осуществлении производственных процессов на газовых и нефтяных месторождениях, что способствует тому, что компании могут сохранить и увеличить экономический потенциал, улучшить эффективность промышленной автоматизации и обеспечить защиту природной среды.

Исследование интеллектуальной модели имеет практическую значимость для энергетической отрасли в целом, поскольку позволит в перспективе разрабатывать новые методы и алгоритмы для защиты информации и противодействия кибератакам. Благодаря этому инженеры нефтегазового дела, специалисты по информационной безопасности смогут сформировать и потом апробировать наиболее надежные и безопасные системы на нефтяных и газовых месторождениях.

Цель данного исследования — разработать концепцию интеллектуальной модели защиты информации на нефтяных и газовых месторождениях.

Задачи исследования:

1. Выявить преимущества мультиагентского подхода к обеспечению информационной безопасности на нефтяных и газовых месторождениях.
2. Представить концептуальную структуру интеллектуальной модели защиты информации на нефтяных и газовых месторождениях.
3. Оценить эффективность предложенной концептуальной структуры интеллектуальной модели защиты информации.

Материалы и методы

Для выявления преимуществ мультиагентского подхода к обеспечению информационной безопасности на нефтяных и газовых месторождениях автором статьи был проведён обзор и анализ научно-прикладной литературы.

Помимо метода анализа научно-прикладной литературы, автором статьи использовался метод индукции, дедукции, систематизации, графического представления информации, абстрактно-логический метод, мультиагентский метод построения интеллектуальной модели защиты информации, метод математической обработки информационных данных KDD CUP 99.

Результаты и их обсуждения

Агентский метод обеспечивает более эффективную и гибкую модель распределенных вычислений, представляет собой инновационный способ решения проблемы защиты информации в крупномасштабных распределенных сетевых системах. В рамках защиты информации промышленной безопасности принята мультиагентская структура, позволяющая в полной мере использовать независимость и автономию непосредственно агента для своевременного локального реагирования, что может уменьшить корреляцию между различными компонентами интеллектуальной модели защиты информации. При этом взаимодействие агентов в данном подходе используется для практической реализации сложного алгоритма защиты информации [9; 10]. Мультиагентская архитектура имеет следующие характеристики, отражающие преимущества:

1. Отказ одного или некоторых агентов в системе защиты информации не повлияет на оставшихся агентов, что уменьшает риск общего сбоя системы диспетчерского управления и сбора информационных данных, а также позволяет избежать единичного сбоя классической централизованной системы. Если у агента возникли проблемы или он поврежден внутри модели, ущерб от сбоя будет ограничен минимальным диапазоном и незначительной ошибкой диффузии. Агент может работать в автономном режиме, используя встроенную базу знаний и логику обработки информационных данных, поэтому агент может временно продолжать работу из системы. Когда соединение с другим системным агентом восстанавливается, расчетные данные могут быть перенаправлены к нему [11; 12; 13].
2. Различные агенты могут воспринимать внешнюю среду по-разному, и их источники информационных данных находятся в различных формах, таких как данные аудита хоста, конфигурация хост-системы, захват сетевых пакетов интеллектуальной модели защиты информации. Для всего диапазона восприятие информационных данных агентом не ограничено, что подходит для развертывания в крупномасштабной интеллектуальной модели защиты информации.
3. Обнаружение агентов в системе может использоваться для разных источников данных, при этом используемый алгоритм обнаружения киберугроз не является постоянным. Сопоставление шаблонов, анализ состояния, статистический анализ, мониторинг поведения как методы могут применяться к разным агентам. Анализируя характеристики вторжения или аномалии, встречающиеся в киберсистеме, о которых сообщают разные агенты, в контексте интеллектуальной модели можно получить более точные результаты.

Основываясь на эксплуатационных характеристиках системы диспетчеризации и сбора информационных данных в нефтяных и газовых месторождениях в сочетании с преимуществами мультиагентской архитектуры, такая технология может применяется для защиты информации в контексте предлагаемой интеллектуальной модели. В этом исследовании представлена интеллектуальная модель защиты информации на основе мультиагентского подхода к информационной безопасности на нефтяных и газовых месторождениях. Интеллектуальная модель использует преимущества мультиагентской архитектуры в распределенной системе и позволяет классифицировать общую структуру на три уровня: уровень мониторинга, уровень принятия решений и уровень управления (рис. 1). На этих трех уровнях разные типы агентов играют индивидуальную роль для практической реализации конкретных функций. В соответствии с вышеуказанными уровнями они могут эффективно разделить сложные функции системы и соответственно снизить степень объединения различных частей интеллектуальной. В то же время может быть реализовано разделение стратегии и методов защиты информации на нефтегазовых предприятиях, что увеличивает гибкость конфигурации и надежность интеллектуальной модели.

Уровень мониторинга включает в себя агента, осуществляющего мониторинг, и агента, исполняющего ре-

Уровень управления	**Агент, предоставляющий пользовательский интерфейс**
	Агент координации функций в системе
Уровень принятия решений	**Агент регистрации входящих данных**
	Агент, принимающий решения
Уровень мониторинга	**Агент, исполняющий решения**
	Агент, осуществляющий мониторинг

Рис. 1. Концепция мультиагентского подхода к построению интеллектуальной модели защиты информации с распределением агентов в структуре модели

Источник: разработано автором.

шения. На этом уровне собираются и обрабатываются основные исходные данные в интеллектуальной модели защиты информации, а также выполняются действия, когда система этого требует, поэтому агенты могут контролировать процесс диспетчерского управления и сбора данных, а также поддерживать контроль его информационной безопасности.

Уровень принятия решений является основным уровнем интеллектуальной модели защиты информации, на котором выполняют функции агент регистрации входящих информационных данных и агент принятия решений. В основном он анализирует результаты принятых решений с оценкой обнаружения киберугроз, полученных на уровне мониторинга. При необходимости уровень принятия решений координирует агента принятия множественных решений для выработки совместных решений и затем передает результаты решения агенту, исполняющему решения, на уровне мониторинга.

Уровень управления включает агента, предоставляющего пользовательский интерфейс, и агента координации функций в системе. Он реализует работы по конфигурации модели, настройке и планированию функций всех агентов в интеллектуальной модели защиты информации.

В рамках представленной концепции количество агентов в интеллектуальной модели защиты информации может повышаться либо сокращаться в зависимости от характеристик обновления встроенной базы знаний внутри интеллектуальной модели. В случае необходимости уровень управления может координировать действия нескольких агентов принятия решений для выработки совместного решения.

В таблице 1 представлена характеристика функций, выполняемых каждым агентом в рамках концепции мультиагентского подхода к построению интеллектуальной модели защиты информации.

Когда агент мониторинга обнаруживает некоторые исключения в интеллектуальной модели защиты информации, он передает соответствующую информацию об обнаружении угрозы агенту, принимающему решения, который, в свою очередь, формирует аргументированное суждение по сложившейся ситуации. Если для принятия решения агенту необходима совместная работа с другими агентами, то агент координации функций в системе координирует принятие решения другим агентом для участия в основном решении, и результаты двух агентов уже являются синергетическими. Окончательное решение будет передано соответствующему агенту, исполняющему решения, и уже он будет заниматься мониторингом аномального поведения в системе диспетчерского управления и сбора данных на нефтяных и газовых месторождениях.

Агент мониторинга использует встроенную базу знаний и логику обработки информационных данных мониторинга для анализа. Если результаты ненормальные, информация будет передана агенту, принимающему решения.

После получения информации от агента мониторинга агент, принимающий решения, анализирует информацию через базу знаний, принимает решение и использует метод обработки исключений в интеллектуальной модели защиты информации. Если один агент не может принять решение, агенту координации функций в системе необходимо скоординировать действия нескольких

Таблица 1.

Характеристика функций, выполняемых каждым агентом в рамках концепции мультиагентского подхода к построению интеллектуальной модели защиты информации

Наименование агента	Функции, выполняемые агентом
Агент, предоставляющий пользовательский интерфейс	— предоставление удобного пользовательского интерфейса; — обновление информационных данных (автоматизированное и ручное); — предоставление информации для агентов, если нужно ручное обновление информационных данных
Агент координации функций в системе	— передача информационных данных и заданий между агентами интеллектуальной модели защиты информации; — обеспечение совместной работы агентов в интеллектуальной модели защиты информации
Агент регистрации входящих данных	— регистрация новых агентов в интеллектуальной модели защиты информации; — аннулирование регистрации агента в интеллектуальной модели защиты информации; — регистрация входящих данных в систему
Агент, принимающий решения	— аккумулирование знаний об информационной безопасности и процессе защиты информации; — завершение обработки информации; — осуществление систематического анализа данных; — самостоятельное выполнение задач по обнаружению проблем информационной безопасности в различных аспектах интеллектуальной модели защиты информации; — применение методов обнаружения аномального либо подозрительного поведения пользователей
Агент, исполняющий решения	— обработка обнаруженных угроз информационной безопасности; — использование принятых решений для передачи параметров принятого решения; — принятие эффективных мер по прекращению нарушений операций информационной безопасности и борьбе с угрозами информационной безопасности
Агент, осуществляющий мониторинг	— мониторинг и обработка информационных данных целевого хоста или сетевого нефтегазового оборудования, поступающие из сетевых пакетов информационных данных; — сбор входящих данных; — предварительная обработка исходных данных, включая фильтрацию, форматирование, извлечение и анализ информационных данных; — передача информационных данных агенту, принимающему решения

Источник: разработано автором.

агентов, принимающих решения, для формирования совместного решения с аномальной особенностью данных и затем передать информацию о решении соответствующему агенту, исполняющему решения. Если он отсутствует в среде интеллектуальной модели защиты информации, то необходимо перенести выполнение решения с данного агента на агента, назначенного субъектом, принимающим решения.

По информации агента, принимающего решения, агент, исполняющий решения, предпримет различные действия по работе с исключениями интеллектуальной модели защиты информации, обнаруженными в системе, например, изоляция файлов в библиотеке, блокировка операций.

Согласно отчету агента мониторинга интеллектуальная модель защиты информации фиксирует специфику диспетчерского управления и сбора данных на нефтяных и газовых месторождениях, если данная система подверглась атаке, и классифицирует ее по категориям. Система анализирует уровень информационной безопасности территории, занимаемой нефтяным и газовым месторождением, и предупреждает систему диспетчеризации и сбора данных о необходимости принятия соответствующих мер. Одновременно с этим агент в совместном принятии решения может обновить свою базу знаний, для того чтобы завершить обработку информационных данных по исключительной ситуации, возникшей в интеллектуальной модели защиты информации.

В нефтегазовой системе диспетчерского управления и сбора данных взаимосвязь между рабочим сервером и станционным компьютером или рабочей станцией администратора и станционным компьютером основана на общем сетевом протоколе. Таким образом, широко используемый набор данных обнаружения сетевых вторжений KDD CUP 99 может быть использован в этом исследовании для обучения модели защиты информации с помощью метода дерева решений. Для сравнения результатов обучения были выбраны две группы атрибутов объектов: обучение по тому же методу обработки данных атрибутивным характеристикам TCP-соединения. В эксперименте для анализа и сравнения были выбраны две группы показателей. Первая группа А выделила некоторые характерные показатели обучения TCP-соединению и контенту (продолжительность соединения, тип протокола, поток информационных данных, количество точек доступа, количество состояний угроз, попытки выполнения команды), а вторая группа В — интеллектуальный анализ данных сетевого трафика хоста (продолжительность соединения, поток информационных данных, количество соединений с того же целевого хоста на 100 текущих соединений, количество соединений, обладающих аналогичной целевой информационной службой, на 100 текущих соединений, доля

соединений, обладающих одинаковым целевым хостом и целевой информационной службой, на 100 текущих соединений, доля соединений, обладающих одинаковым целевым хостом, но различными целевыми информационными службами, на 100 текущих соединений).

Экспериментальные результаты оценки эффективности предложенной концептуальной структуры интеллектуальной модели защиты информации представлены в таблице 2.

Таблица 2.

Экспериментальные результаты оценки эффективности предложенной концептуальной структуры интеллектуальной модели защиты информации

Группа	Количество соединений в выборке	Продолжительность реализации алгоритма, секунд	Размер дерева решений	Точность классификации, %
A	90408	0,52	46	97,418
B	90408	0,96	118	99,813

Источник: разработано автором.

Согласно результатам эксперимента, несмотря на то, что точность классификации решения группы B выше, дерево решений больше, а продолжительность реализации алгоритма в существенной мере выше, чем у группы A, при сохранении высокой точности принятия решения дерево решений, сгенерированное группой A, намного меньше, чем у группы B, а продолжительность реализации алгоритма короче, можно говорить о том, что эффективность принятия решения по атрибуту группы A выше.

Выводы

В исследовании были выявлены преимущества мультиагентского подхода к обеспечению информационной безопасности на нефтяных и газовых месторождениях.

Представлена концептуальная структура интеллектуальной модели защиты информации на нефтяных и газовых месторождениях.

Оценена эффективность предложенной концептуальной структуры интеллектуальной модели защиты информации.

ЛИТЕРАТУРА

1. Helmer G., Wong J.S.K., Honavar V., Miller L., Wang Y. Lightweight Agent for intrusion detection // The Journal of Systems and Software. — 2003. — Vol. 67. — P. 109–122.
2. Lee W., Stolfo S., Mok K. A Data Mining Framework for Building Intrusion Detection Models // IEEE Symposium on Security and Privacy. — 1999. — P. 120–132.
3. Balasubramaniyan J.S., Garcia-Fernandez J.O., Isacoff D., et al. An architecture for intrusion detection using autonomous agent // Computer Security Applications Conference. — 1998. — P. 1–19.
4. Huang K., Zhou C., Tian Y.C., et al. Application of Bayesian network to data-drivencyber-security risk assessment in SCADA networks // IEEE 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). — 2017. — P. 1–6.
5. Marcio T., Tara S., Maede Z., et al. SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach // Future Internet. — 2018. — Vol. 10 (8). — P. 76–90.
6. Mohammadi J., Hug G., Kar S. Agent-Based Distributed Security Constrained Optimal Power Flow // IEEE Transactions on Smart Grid. — 2018. — Vol. 9 (2). — P. 1118–1130.
7. Asaka M., Taguchi A., Goto S. The implementation of IDA: an intrusion detection agent system // Proceedings of the 11th FIRST Conference. — 1999. — P. 97–102.
8. Helmer G., Wong J.S.K., Honavar V., Miller L., Wang Y. Intelligent Agent for Intrusion Detection // IEEE Information Technology Conference. — 1998. — P. 121–124.
9. Undercoffer J., Joshi A., Pinkston J. Modeling computer attacks: an ontology for intrusion detection // Computer Science. — 2003. — No. 2820. — P. 113–135.
10. Cao X., Wei C., Li J., Li Y. The Geological Disasters Defense Expert System of the Massive Pipeline Network SCADA System Based on FNN // LNCS. — 2012. — No. 7234. — P. 19–26.
11. Spafford E.H., Zamboni D. Intrusion Detection Using Auto-nomous Agent // Computer Networks. — 2000. — Vol. 34. — No. 5472570.
12. Li Y. A new cyber security risk evaluation method for oil and gas SCADA based on factor state space // Chaos, Solitons and Fractals. — 2016. — Vol. 89. — P. 203–209.
13. Maio F.D., Colli D., Zio E., et al. A Multi-State Physics Modeling approach for the reliability assessment of Nuclear Power Plants piping systems // Annals of Nuclear Energy. — 2015. — Vol. 80. — P. 151–165.

Журнал «Современная наука: актуальные проблемы теории и практики»