Безопасность мультиагентной платформы

**Человек:** Работа посвящается актуальной проблеме обеспечения безопасности гетерогенных информационных платформ, с применением мультиагентной системы обнаружения угроз. Объектом исследования является мультиагентная платформа. Особое внимание автор уделяет таким аспектам темы как: безопасность мультиагентных платформ, управление агентами обнаружения угроз, взаимосвязь между разными агентами обнаружения угроз, уязвимости в мультиагентных платформах. Рассматриваются тенденции для разработки новых распределённых моделей безопасности. в работе представлена мультиагентная архитектура для службы безопасности, а также общий сценарий развертывания безопасности в мультиагентных системах обнаружения угроз. В работе представлена мультиагентная архитектура для службы безопасности, а также общий сценарий развертывания безопасности в мультиагентных системах обнаружения угроз. В теоретическом плане полученные результаты предполагают расширение области использования мультиагентного подхода и осуществление его интеграции с интеллектуальным анализом развития и функционирования информационных систем. Результатом проведенного исследования является формирование концепции создания безопасной мультиагентной платформы для применения в мультиагентной системе обнаружения угроз.

**Key words:** защита информации, обнаружение угроз, интеллектуальные системы защиты, мульти агентная платформа, гетерогенные информационные платформы, агент обнаружения угроз, системы анализа, алгоритм обнаружения, агент платформа, мульти агентная система

=================================

**FastText\_KMeans\_Clean:** Методики проектирования СЗИ для гетерогенных ИС, разработанные к настоящему времени, содержат лишь комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое (запрограммированное) их осуществление невозможно в силу высокой сложности самой информационной системы и ее распределённостью по множеству вычислительных узлов. Одной из них является платформа IBM Aglet (http://aglets.sourceforge.net/), которая не обеспечивает безопасности для защиты агентов и не требует строгой аутентификации и авторизации. Она обеспечивает базовый процесс аутентификации пользователя и пароля для идентификации агентов, который, в свою очередь, позволяет им анонимно получать доступ к платформе вместе с простым контролем доступа на основе их двух возможных ролей “доверенные аглеты” для агентов, созданных сервером и “ненадёжные аглеты” для агентов, созданных внешними серверами. В этом контексте Mosqueira-Rey и др.

**Key words part:** 0.6176470588235294

=================================

**FastText\_KMeans\_Raw/:** Методики проектирования СЗИ для гетерогенных ИС, разработанные к настоящему времени, содержат лишь комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое (запрограммированное) их осуществление невозможно в силу высокой сложности самой информационной системы и ее распределённостью по множеству вычислительных узлов. Одной из них является платформа IBM Aglet (http://aglets.sourceforge.net/), которая не обеспечивает безопасности для защиты агентов и не требует строгой аутентификации и авторизации. Она обеспечивает базовый процесс аутентификации пользователя и пароля для идентификации агентов, который, в свою очередь, позволяет им анонимно получать доступ к платформе вместе с простым контролем доступа на основе их двух возможных ролей “доверенные аглеты” для агентов, созданных сервером и “ненадёжные аглеты” для агентов, созданных внешними серверами. В этом контексте Mosqueira-Rey и др. Для серьёзных случаев безопасности Szymczyk [18] предлагает мультиагентную систему безопасности для обнаружения ботов, чтобы предотвратить проблемы, связанные с общими компьютерными атаками, полученными от хакеров или систем, заражаемых вредоносным программным обеспечением, и используемых для незаконных действий.

**Key words part:** 0.7058823529411765

=================================

**FastText\_PageRank\_Clean/:** Общий сценарий развертывания безопасности в МАС. Это защищает платформу от любых возможных атак злоумышленников. Например, такие эксперты, как Nguyen и др. TuCSoN от Ricci и др. В этом контексте Mosqueira-Rey и др. [16] используют метод, с участвующим агентом обнаружения злоупотреблений. Затем генерируется иммунный ответ на вредоносное поведение, активируемое либо компьютером, либо центром безопасности. Результатом проведенного исследования является формирование концепции создания безопасной мультиагентной платформы.

**Key words part:** 0.5

=================================

**FastText\_PageRank\_Raw/:** Общий сценарий развертывания безопасности в МАС. Это защищает платформу от любых возможных атак злоумышленников. Например, такие эксперты, как Nguyen и др. TuCSoN от Ricci и др. В этом контексте Mosqueira-Rey и др. [16] используют метод, с участвующим агентом обнаружения злоупотреблений. Затем генерируется иммунный ответ на вредоносное поведение, активируемое либо компьютером, либо центром безопасности. Результатом проведенного исследования является формирование концепции создания безопасной мультиагентной платформы.

**Key words part:** 0.5

=================================

**Mixed\_ML\_TR/:** Одним из подходов к проектированию интеллектуальных СЗИ основывается на парадигме мультиагентных систем (МАС). Известно, что использование платформы с несколькими агентами упрощает реализацию МАС. Например, на рисунке 1 показан общий сценарий, в котором разные агенты используются для разработки системы безопасности в рамках мультиагентной платформы. Второй уровень защиты представляет безопасность платформы-агента, являющийся службой безопасности, которую платформа предоставляет для агентов. Одной из них является платформа IBM Aglet (http://aglets.sourceforge.net/), которая не обеспечивает безопасности для защиты агентов и не требует строгой аутентификации и авторизации. Эта схема авторизации может использоваться для сложных систем, отвечающих за комплексные услуги в больницах, каждая из которых имеет свою собственную систему безопасности, где агенты обеспечивают отображение информации о безопасности во всей системе, предоставляющей услуги по обеспечению взаимодействия между ними. Стоит отметить, что операционная система безопасности является элементом архитектуры этого предложения, предназначенным для использования в координации информации, предоставляемой различными агентами. Несмотря на большое количество и многообразие существующих мультиагентных платформ, большинство из них не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов.

**Key words part:** 0.6176470588235294

=================================

**MultiLingual\_KMeans/:** Одним из подходов к проектированию интеллектуальных СЗИ основывается на парадигме мультиагентных систем (МАС). Известно, что использование платформы с несколькими агентами упрощает реализацию МАС. Стоит отметить, что операционная система безопасности является элементом архитектуры этого предложения, предназначенным для использования в координации информации, предоставляемой различными агентами. Несмотря на большое количество и многообразие существующих мультиагентных платформ, большинство из них не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов.

**Key words part:** 0.6176470588235294

=================================

**Multilingual\_PageRank/:** Например, такие эксперты, как Nguyen и др. Эта платформа не занимается никакими службами безопасности и полностью полагается на внутреннюю безопасность Java. TuCSoN от Ricci и др. Они даже не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов. Некоторые не предоставляют никакой аутентификации, а некоторые не обеспечивают безопасность для коммуникаций. Для первого подхода Shakshuki и др. Аналогичным образом можно назвать другое использование схемы авторизации для нескольких агентов для медицинских систем, MedIGS [15]. В этом контексте Mosqueira-Rey и др.

**Key words part:** 0.5588235294117647

=================================

**RuBERT\_KMeans\_Without\_ST/:** Такие мультипрограммные комплексы должны состоять из нескольких логических уровней и содержать множества компонентов защиты, специализирующихся по различным типам решаемых задач (обнаружение угроз, вторжений, аномалий в работе и т.п.), взаимодействовать между собой путем обмена информацией с целью принятия более правильного решения, а также уметь адаптироваться к новым видам атак. TuCSoN от Ricci и др. Это, в действительности, можно рассматривать как мультиагентную схему аутентификации PKI (Public Key Infrastructure), которая содержит несколько агентов аутентификации, собирающихся вместе для действия, когда появляется новый клиентский запрос. Для серьёзных случаев безопасности Szymczyk [18] предлагает мультиагентную систему безопасности для обнаружения ботов, чтобы предотвратить проблемы, связанные с общими компьютерными атаками, полученными от хакеров или систем, заражаемых вредоносным программным обеспечением, и используемых для незаконных действий.

**Key words part:** 0.6470588235294118

=================================

**RuBERT\_KMeans\_With\_ST/:** Это, в действительности, можно рассматривать как мультиагентную схему аутентификации PKI (Public Key Infrastructure), которая содержит несколько агентов аутентификации, собирающихся вместе для действия, когда появляется новый клиентский запрос. Чтобы способствовать справедливому распределению, лучшей масштабируемости и высокой производительности, а также простоте управления и расширений, концепция мультиагентной автоматизации применяется в автоматизации большинства процессов, таких как функции аутентификации, авторизации и учёта. Для серьёзных случаев безопасности Szymczyk [18] предлагает мультиагентную систему безопасности для обнаружения ботов, чтобы предотвратить проблемы, связанные с общими компьютерными атаками, полученными от хакеров или систем, заражаемых вредоносным программным обеспечением, и используемых для незаконных действий. В работе представлена мультиагентная архитектура для службы безопасности.

**Key words part:** 0.5

=================================

**RUBERT\_page\_rank\_Without\_ST/:** Для агент-платформы безопасности задача состоит в управлении агентами. Например, такие эксперты, как Nguyen и др. TuCSoN от Ricci и др. Для первого подхода Shakshuki и др. Другими системами безопасности, подходящими для дальнейшей разработки в рамках МАС, являются распределённые системы обнаружения вторжений (distributed intrusion detection systems, DIDS).

**Key words part:** 0.5

=================================

**RUBERT\_page\_rank\_With\_ST/:** Общий сценарий развертывания безопасности в МАС. Например, такие эксперты, как Nguyen и др. TuCSoN от Ricci и др. Для первого подхода Shakshuki и др. В этом контексте Mosqueira-Rey и др.

**Key words part:** 0.2647058823529412

=================================

**RUSBERT\_KMeans\_Without\_ST/:** В современных технологиях ПО это может быть обеспечено через промежуточное ПО, чтобы облегчить развертывание агентов, контроль связи между агентами и поддержание необходимых мер безопасности для агентов. Второй уровень защиты представляет безопасность платформы-агента, являющийся службой безопасности, которую платформа предоставляет для агентов. Одной из них является платформа IBM Aglet (http://aglets.sourceforge.net/), которая не обеспечивает безопасности для защиты агентов и не требует строгой аутентификации и авторизации. Что касается уровня аутентификации, МАС позволяет использовать облачные и грид-вычисления, которые должны обрабатывать несколько пользовательских приложений для пользователей, принадлежащих к различным организациям.

**Key words part:** 0.4705882352941176

=================================

**RUSBERT\_KMeans\_With\_ST/:** Методики проектирования СЗИ для гетерогенных ИС, разработанные к настоящему времени, содержат лишь комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое (запрограммированное) их осуществление невозможно в силу высокой сложности самой информационной системы и ее распределённостью по множеству вычислительных узлов. Чтобы способствовать справедливому распределению, лучшей масштабируемости и высокой производительности, а также простоте управления и расширений, концепция мультиагентной автоматизации применяется в автоматизации большинства процессов, таких как функции аутентификации, авторизации и учёта. Другими системами безопасности, подходящими для дальнейшей разработки в рамках МАС, являются распределённые системы обнаружения вторжений (distributed intrusion detection systems, DIDS). В работе представлена мультиагентная архитектура для службы безопасности.

**Key words part:** 0.5

=================================

**RUSBERT\_page\_rank\_Without\_ST/:** TuCSoN от Ricci и др. Они даже не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов. Некоторые не предоставляют никакой аутентификации, а некоторые не обеспечивают безопасность для коммуникаций. Для первого подхода Shakshuki и др. В этом контексте Mosqueira-Rey и др.

**Key words part:** 0.4705882352941176

=================================

**RUSBERT\_page\_rank\_With\_ST/:** Например, такие эксперты, как Nguyen и др. TuCSoN от Ricci и др. Они даже не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов. Некоторые не предоставляют никакой аутентификации, а некоторые не обеспечивают безопасность для коммуникаций. Для первого подхода Shakshuki и др.

**Key words part:** 0.4705882352941176

=================================

**Simple\_PageRank/:** Методики проектирования СЗИ для гетерогенных ИС, разработанные к настоящему времени, содержат лишь комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое (запрограммированное) их осуществление невозможно в силу высокой сложности самой информационной системы и ее распределённостью по множеству вычислительных узлов. Такие мультипрограммные комплексы должны состоять из нескольких логических уровней и содержать множества компонентов защиты, специализирующихся по различным типам решаемых задач (обнаружение угроз, вторжений, аномалий в работе и т.п.), взаимодействовать между собой путем обмена информацией с целью принятия более правильного решения, а также уметь адаптироваться к новым видам атак. Информация, разделяемая агентами, чувствительна, поэтому платформа должна иметь возможность обрабатывать аспекты безопасности связи агент-агент, для которых NIST предлагает различные уровни решений безопасности [2]. Практическим методом для достижения этой меры безопасности является использование изолированной программной среды, определяемой как безопасная среда выполнения, позволяющая подлинным агентам защищать платформу от вредоносных агентов. Она обеспечивает базовый процесс аутентификации пользователя и пароля для идентификации агентов, который, в свою очередь, позволяет им анонимно получать доступ к платформе вместе с простым контролем доступа на основе их двух возможных ролей “доверенные аглеты” для агентов, созданных сервером и “ненадёжные аглеты” для агентов, созданных внешними серверами. Для серьёзных случаев безопасности Szymczyk [18] предлагает мультиагентную систему безопасности для обнаружения ботов, чтобы предотвратить проблемы, связанные с общими компьютерными атаками, полученными от хакеров или систем, заражаемых вредоносным программным обеспечением, и используемых для незаконных действий.

**Key words part:** 0.7941176470588235

=================================

**TextRank/:** Например, на рисунке 1 показан общий сценарий, в котором разные агенты используются для разработки системы безопасности в рамках мультиагентной платформы. Второй уровень защиты представляет безопасность платформы-агента, являющийся службой безопасности, которую платформа предоставляет для агентов. Одной из них является платформа IBM Aglet (http://aglets.sourceforge.net/), которая не обеспечивает безопасности для защиты агентов и не требует строгой аутентификации и авторизации. Эта схема авторизации может использоваться для сложных систем, отвечающих за комплексные услуги в больницах, каждая из которых имеет свою собственную систему безопасности, где агенты обеспечивают отображение информации о безопасности во всей системе, предоставляющей услуги по обеспечению взаимодействия между ними. Это один из отличных агентов в мультиагентной системе обнаружения вторжений, которая также реализована на платформе JADE. Стоит отметить, что операционная система безопасности является элементом архитектуры этого предложения, предназначенным для использования в координации информации, предоставляемой различными агентами.

**Key words part:** 0.6764705882352942

=================================

**TF-IDF\_KMeans/:** Такие мультипрограммные комплексы в различных работах часто называют интеллектуальными СЗИ. Например, на рисунке 1 показан общий сценарий, в котором разные агенты используются для разработки системы безопасности в рамках мультиагентной платформы. Предположим, что система безопасности развернута для работы с распределённой системой обнаружения вторжений. Второй уровень защиты представляет безопасность платформы-агента, являющийся службой безопасности, которую платформа предоставляет для агентов. Учитывая, что безопасные платформы МАС обеспечивают повышенную эффективность и надёжную производительность, они могут эффективно использоваться для защиты сложных распределённых систем. Наиболее значимыми являются две тенденции для разработки новых распределённых моделей безопасности. Для первого подхода Shakshuki и др. Несмотря на большое количество и многообразие существующих мультиагентных платформ, большинство из них не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов.

**Key words part:** 0.6764705882352942

=================================

**Текст:** Интенсивное развитие Интернет, повсеместный переход на электронные формы хранения и передачи информации, активное внедрение в повседневную жизнь электронных форм платежей и многие другие факторы сегодняшней реальности повлияли на то, что безопасность сетей и сетевых сервисов стала действительно насущной проблемой практически всех организаций.. Благодаря постоянному положительному тренду развёртывания широкополосного доступа к сети Internet, в том числе и мобильного, а также интенсивному развитию информационных технологий, с помощью которых создаются разнообразные пользовательские сервисы, нагрузка на информационную систему (ИС) может составлять тысячи и даже миллионы одновременных сеансов. Поддержка даже нескольких сотен одновременных сеансов пользователей для ИС с развитыми динамическими сервисами в «монолитном» исполнении является крайне трудновыполнимой задачей, а в случае существенно большего количества сеансов – просто невыполнимой. В связи с чем основной вектор развития современных ИС, как правило, лежит в плоскости гетерогенных информационных систем, обладающих свойствами динамического расширения, как в контексте предоставляемых сервисов, так и в контексте доступности для увеличивающегося количества пользователей ИС. Типичным примером этого является быстрое развитие различных облачных технологий и предоставляемых ими сервисов (PaaS, IaaS, SaaS).. Одной из наиболее важных проблем функционирования гетерогенных ИС является обеспечение информационной безопасности. Однако в отличие от «монолитных» ИС, для которых за долгие годы их развития появились определенные методики и подходы к проектированию систем защиты информации (СЗИ), для гетерогенных ИС ситуация иная. Методики проектирования СЗИ для гетерогенных ИС, разработанные к настоящему времени, содержат лишь комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое (запрограммированное) их осуществление невозможно в силу высокой сложности самой информационной системы и ее распределённостью по множеству вычислительных узлов.. В такой ситуации невозможно заранее спрогнозировать все возможные атаки на гетерогенную ИС и предусмотреть соответствующие сценарии защиты. Поэтому методы обеспечения информационной безопасности гетерогенных систем могут быть основаны только на использовании мультипрограммных комплексов, способных к планированию поведения в сложных средах. Такие мультипрограммные комплексы должны состоять из нескольких логических уровней и содержать множества компонентов защиты, специализирующихся по различным типам решаемых задач (обнаружение угроз, вторжений, аномалий в работе и т.п.), взаимодействовать между собой путем обмена информацией с целью принятия более правильного решения, а также уметь адаптироваться к новым видам атак. Такие мультипрограммные комплексы в различных работах часто называют интеллектуальными СЗИ.. Одним из подходов к проектированию интеллектуальных СЗИ основывается на парадигме мультиагентных систем (МАС). Такие системы отличаются от традиционных объектно-ориентированных программных систем тем, что в них, наряду с пассивными сущностями (классы и объекты), существуют и активные сущности – агенты, сообщество которых позволяет решать сложные задачи в условиях неопределенности внешней среды. Обнаружение вторжений и аномалий, а также их предупреждение являются примером таких задач в условиях отсутствия исчерпывающего перечня потенциальных угроз. [1].. Известно, что использование платформы с несколькими агентами упрощает реализацию МАС. В современных технологиях ПО это может быть обеспечено через промежуточное ПО, чтобы облегчить развертывание агентов, контроль связи между агентами и поддержание необходимых мер безопасности для агентов. Благодаря расположению в системе агенты могут легко выполнять большинство функций безопасности, а также фоновые процессы в МАС. Например, на рисунке 1 показан общий сценарий, в котором разные агенты используются для разработки системы безопасности в рамках мультиагентной платформы.. . Рис. 1. Общий сценарий развертывания безопасности в МАС. Предположим, что система безопасности развернута для работы с распределённой системой обнаружения вторжений. Процессы, выполняющие мультиагентную платформу (МАП), развертываются на разных компьютерах. Каждый агент отвечает за анализ поведения сети по отношению к своей собственной машине, в то же время обмениваясь информацией на платформе друг с другом, чтобы они могли сотрудничать в обнаружении возможной деятельности по вторжению. Информация, разделяемая агентами, чувствительна, поэтому платформа должна иметь возможность обрабатывать аспекты безопасности связи агент-агент, для которых NIST предлагает различные уровни решений безопасности [2]. Для агент-платформы безопасности задача состоит в управлении агентами. Это защищает платформу от любых возможных атак злоумышленников. Практическим методом для достижения этой меры безопасности является использование изолированной программной среды, определяемой как безопасная среда выполнения, позволяющая подлинным агентам защищать платформу от вредоносных агентов.. Второй уровень защиты представляет безопасность платформы-агента, являющийся службой безопасности, которую платформа предоставляет для агентов. По сути, аналогией этому может быть какое-то вычисление конфиденциальности, такое как шифрование, которое защищает информацию, связанную с агентом, от любых возможных манипуляций, таких как рабочий процесс, конфиденциальность и целостность данных. Третий уровень защиты представляет безопасность агента от агента, в которой агент пытается защитить себя от действий, порождаемых неправильным поведением других агентов, таких как отказ в обслуживании, шпионаж или заведомо сложные действия от имени других агентов. Наконец, разработана защита платформы от другой платформы для обеспечения взаимодействия между различными платформами.. В тоже время, несмотря на свою естественность, МАС не была эффективно использована в прошлом для полной защиты приложений. Например, такие эксперты, как Nguyen и др. [3], Poslad и др. [4], Mana и др. [5] и Garrigues и др.[6], чётко указывают на отсутствие надлежащей безопасности в большинстве приложений МАС. Одной из них является платформа IBM Aglet (http://aglets.sourceforge.net/), которая не обеспечивает безопасности для защиты агентов и не требует строгой аутентификации и авторизации. Она обеспечивает базовый процесс аутентификации пользователя и пароля для идентификации агентов, который, в свою очередь, позволяет им анонимно получать доступ к платформе вместе с простым контролем доступа на основе их двух возможных ролей “доверенные аглеты” для агентов, созданных сервером и “ненадёжные аглеты” для агентов, созданных внешними серверами.. Другим примером является JACK [7], коммерческая МАП для построения Распределённой мультиагентной системы анализа (Distributed Multi-Agent Reasoning System, dMARS) [8]. Эта платформа не занимается никакими службами безопасности и полностью полагается на внутреннюю безопасность Java. Она использует политики безопасности Java для контроля доступа к файлам. TuCSoN от Ricci и др. [9] представляет собой бесплатный МАП с открытым исходным кодом и “S-Moise +” из [10], промежуточное ПО, которое можно использовать для создания структурированных МАС и AgentService, Vecchiola и др. [11], свободная среда с открытым исходным кодом для разработки МАС, всем этим структурам не хватает серьёзных мер безопасности. Они даже не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов. Некоторые не предоставляют никакой аутентификации, а некоторые не обеспечивают безопасность для коммуникаций.. Учитывая, что безопасные платформы МАС обеспечивают повышенную эффективность и надёжную производительность, они могут эффективно использоваться для защиты сложных распределённых систем. Наиболее значимыми являются две тенденции для разработки новых распределённых моделей безопасности. Один из них заключается в разработке существующих платформ МАС для повышения своих возможностей в области безопасности, а второй тенденции – в обеспечении наложения для существующих платформ, а затем в разработке новых безопасных платформ для платформ.. Для первого подхода Shakshuki и др. [12] предоставляют подробное и полное описание МАС, включая службы безопасности, создание прототипов и внедрение платформы. На рисунке 2. показана эта архитектура, состоящая из четырёх уровней: (1) уровень интерфейса для взаимодействия человека и системы, (2) уровень аутентификации для аутентификации пользователей платформы, (3) уровень полномочий для контроля доступа к сервисам и информационным ресурсам и (4) уровень обслуживания, обеспечивающий предоставление архитектурных услуг. Следовательно, каждый уровень содержит несколько агентов, чтобы предлагать сервисы, связанные с этим уровнем, и выполнять эти сервисы масштабируемым и распределённым образом.. . Рис. 2. Мультиагентная архитектура для службы безопасности. . Что касается уровня аутентификации, МАС позволяет использовать облачные и грид-вычисления, которые должны обрабатывать несколько пользовательских приложений для пользователей, принадлежащих к различным организациям. Fugkeaw и др. [13] предлагают подход аутентификации для улучшения существующих сценариев приложений МАС при проектировании безопасной МАС. Это, в действительности, можно рассматривать как мультиагентную схему аутентификации PKI (Public Key Infrastructure), которая содержит несколько агентов аутентификации, собирающихся вместе для действия, когда появляется новый клиентский запрос. Поскольку все агенты отвечают за весь набор проверки запроса сертификата, предоставления ролей доступа к клиентам и контролирования плавного одновременного использования приложений, тогда безопасное сотрудничество между агентами МАС имеет важное значение для поддержания обслуживания. Этот подход также может поддерживать службу единого входа для всех других приложений для всех пользователей в среде.. Для уровня авторизации модели Fugkeaw и др. [14] предоставляют распределённый метод управления доступом на основе ролей (distributed role-based access control, dRBAC) для мульти-прикладных сценариев с несколькими пользователями и мульти-пользовательскими объединениями. Агенты используют инфраструктуру открытых ключей и инфраструктуру управления привилегиями для предоставления служб аутентификации и авторизации. Чтобы способствовать справедливому распределению, лучшей масштабируемости и высокой производительности, а также простоте управления и расширений, концепция мультиагентной автоматизации применяется в автоматизации большинства процессов, таких как функции аутентификации, авторизации и учёта. Наконец, они могут способствовать использованию списков сертификатов доверия для создания различных доменов PKI, которые могут более эффективно взаимодействовать. Аналогичным образом можно назвать другое использование схемы авторизации для нескольких агентов для медицинских систем, MedIGS [15]. Эта схема авторизации может использоваться для сложных систем, отвечающих за комплексные услуги в больницах, каждая из которых имеет свою собственную систему безопасности, где агенты обеспечивают отображение информации о безопасности во всей системе, предоставляющей услуги по обеспечению взаимодействия между ними.. Другими системами безопасности, подходящими для дальнейшей разработки в рамках МАС, являются распределённые системы обнаружения вторжений (distributed intrusion detection systems, DIDS). Архитектура этих систем аналогична архитектуре, ранее упомянутой в связи с рисунком 1. В этом контексте Mosqueira-Rey и др. [16] используют метод, с участвующим агентом обнаружения злоупотреблений. Это один из отличных агентов в мультиагентной системе обнаружения вторжений, которая также реализована на платформе JADE. Агент анализирует пакеты в сетевых соединениях с помощью анализатора пакетов и затем создает модель данных на основе собранной информации. Эта модель данных вводится в агент на основе правил, основанных на правилах, которые использует алгоритм соответствия шаблонов Rete (Rete pattern) для применения правил сигнатурной системы обнаружения вторжений Snort.. Ещё один мультиагентный подход для обеспечения обнаружения вторжений исходит от Ou и Ou для искусственной иммунной системы, ориентированной теорией, основанной на теории опасности, MAAIS [17]. Наилучшей аналогией для этого метода является то, что каждый агент координирует свои действия с другими, чтобы вычислить значение опасности для системы. Затем генерируется иммунный ответ на вредоносное поведение, активируемое либо компьютером, либо центром безопасности. Стоит отметить, что операционная система безопасности является элементом архитектуры этого предложения, предназначенным для использования в координации информации, предоставляемой различными агентами.. Для серьёзных случаев безопасности Szymczyk [18] предлагает мультиагентную систему безопасности для обнаружения ботов, чтобы предотвратить проблемы, связанные с общими компьютерными атаками, полученными от хакеров или систем, заражаемых вредоносным программным обеспечением, и используемых для незаконных действий. Этот метод использует гибридный стиль системы обнаружения узловых вторжений с анализатором журнала событий операционной системы. Алгоритмы обнаружения этого предложения основаны на сигнатурах, полученных при анализе различных групп вредоносного ПО, известных для создания ботов.. Таким образом, данная работа предполагает анализ современных подходов к разработке новых распределённых моделей безопасности. Несмотря на большое количество и многообразие существующих мультиагентных платформ, большинство из них не способствуют надлежащей защите агентов внутри платформы и не обеспечивают надёжную защиту платформы от вредоносных агентов.. В работе представлена мультиагентная архитектура для службы безопасности. Результатом проведенного исследования является формирование концепции создания безопасной мультиагентной платформы.. В теоретическом плане полученные результаты предполагают расширение области использования мультиагентного подхода и осуществление его интеграции с интеллектуальным анализом развития и функционирования ИС.