УДК 004.75 https://doi.org/10.33619/2414-2948/68/22

КОНЦЕПЦИЯ ДОВЕРЕННОЙ ПЕРЕДАЧИ ДАННЫХ

©Воронин А. А., *SPIN-код: 2892-7023, ORCID: 0000-0003-4375-7559, канд. техн. наук,*
Владимирский государственный университет им. А.Г. и Н.Г. Столетовых,
г. Владимир, Россия, a_voron@mail.ru

TRUSTED DATA EXCHANGE CONCEPT

©Voronin A., *SPIN-code: 2892-7023, ORCID: 0000-0003-4375-7559,*
Ph.D., Vladimir State University, Vladimir, Russia, a_voron@mail.ru

Аннотация. В работе рассматриваются возможности реализации механизмов обмена разнородной информации между информационными и автоматизированными системами предприятия, формулируется концепции системы доверенной передачи данных.

Abstract. The paper considers main problems of the possibilities of implementing mechanisms for exchanging heterogeneous information between information systems and automated systems of the enterprise. The system of trusted data exchange concept defined.

Ключевые слова: доверие, обмен данными, распределенные системы.

Keywords: trust, data exchange, distributed systems.

Большинство организаций в определенный момент своего развития сталкивается с необходимостью внедрения решений по комплексной автоматизации. К этому моменту в организации может использоваться множество информационных и автоматизированных систем, разработанных и введенных в эксплуатацию в разное время, разными разработчиками.

Как правило, решения сторонних организаций имеют закрытые модули, территориально поставщики решений могут располагаться в разных частях страны, и как следствие адаптация систем под новые правила работы представляется затруднительной. Могут меняться не только принципы работы, но и обслуживающие системы организации. Частично информация может собираться из открытых источников.

Актуальным становится вопрос обеспечения целостности и достоверности данных, передаваемых между информационными системами, особенно при использовании открытых каналов связи. Приходится оценивать источники данных с точки зрения доверия и репутации, анализировать опыт взаимодействия и события безопасности во взаимодействующих системах.

Рассмотрим типовую ИТ инфраструктуру на примере с/х предприятия (инфраструктура, имеющая обычно множество разнородных компонентов). Среди основных подсистем используются следующие системы: система бухгалтерского и налогового учета в организациях сельского хозяйства (БСП); система расчета заработной платы, расчета налогов и страховых взносов, подготовки отчетности (ЗиК); система ведения кадрового учета (СКУ);

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

система спутникового мониторинга автотранспорта (СМТ); система учета, анализа, хранения и обработки информации по крупному рогатому скоту (СКРС); система контроля весовых и измерительных устройств для сельского хозяйства и управления кормами (СКИУ); система оперативного и управленческого учета, анализа и планирования торговых операций (УТ); система подготовки отчетности, утвержденной Министерством сельского хозяйства РФ (Отчетность АПК) и др.

Схема взаимодействия систем и информационные потоки с внешними информационными системами представлены на Рисунке 1.

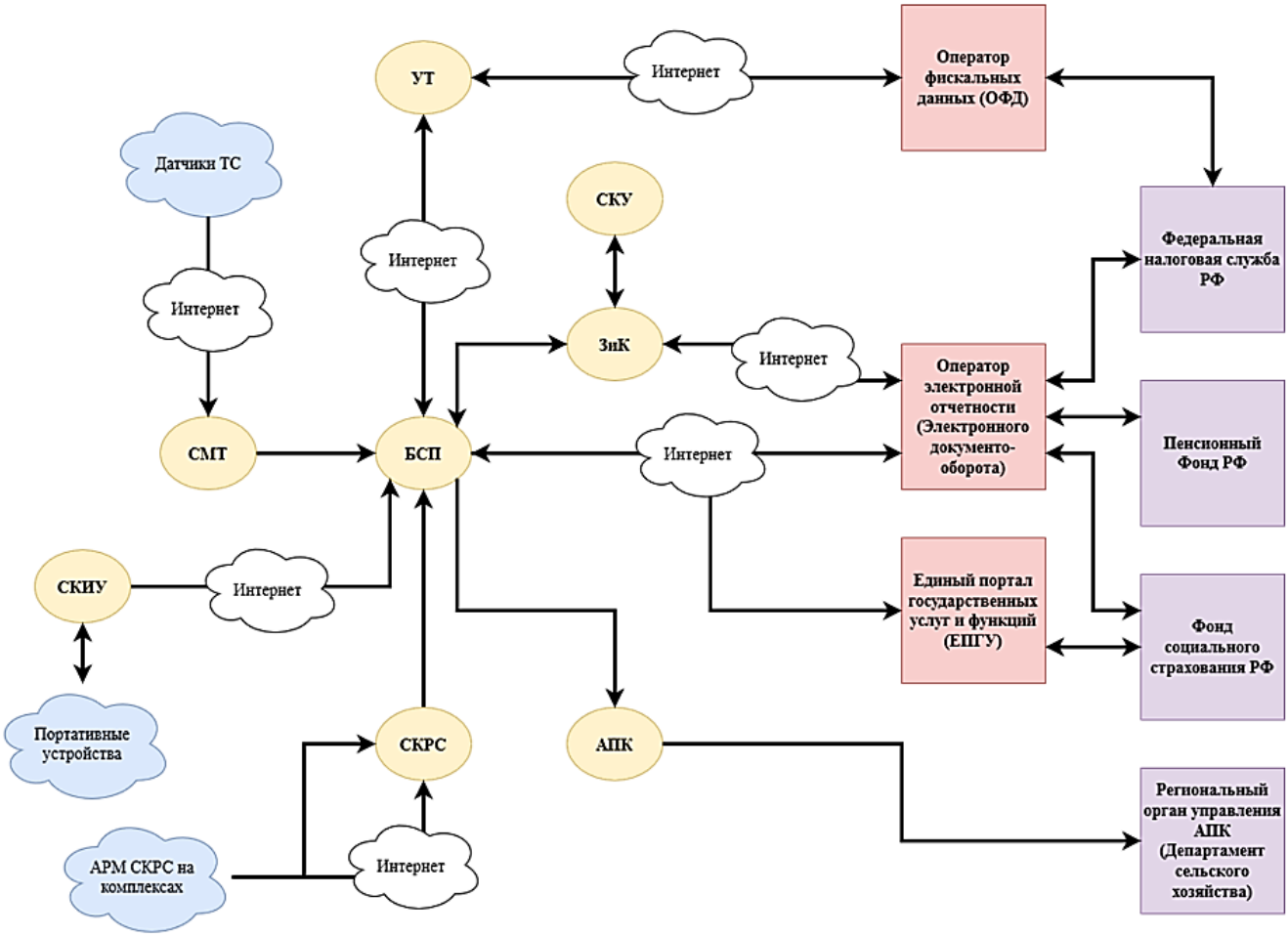

Рисунок 1. Схема взаимодействия систем и информационные потоки

В целом, общая архитектура информационной системы организации характеризуется следующими факторами:

–наличием большого количества информационных систем (подсистем);

–высокой степенью автономности подсистем (системы поставляются разными разработчиками, в том числе и зарубежными, и, как правило, работают автономно);

–использованием разнообразного программного обеспечения;

–отсутствием единых форматов обмена данными между подсистемами и периодическое обновление используемых частных форматов обмена данными (обмен данными с операторами данных, в целом, формализован).

–необходимостью переноса данных между подсистемами в ручном режиме (перенабор данных);

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

–высоким влиянием человеческого фактора при вводе данных в подсистемы (в т. ч. при обмене данными между подсистемами);

–использованием различных типов каналов связи различных операторов связи, нестабильностью этих каналов (определяется удаленностью от магистральных каналов операторов связи);

–невозможность установления прямых соединений между подсистемами;

–обмен данными осуществляется частично (большая часть данных хранится в подсистемах).

В результате анкетирования специалистов профильных организаций получены следующие данные:

–Среднее количество используемых ИС в организациях равно 10. В основном это отраслевые решения, автоматизирующие процессы на определенных участках.

–Информация по порядку и формату обмена имеется только по 24% ИС. Обмен между этими системами преимущественно осуществляется в ручном режиме (через файл, 24%), в автоматическом режиме — 1% (периодический обмен справочной информацией). При этом 26% организаций заявили о наличии у них удаленных рабочих мест.

–Объем данных, загружаемый из внешних систем в собственные информационные системы в автоматическом режиме — менее 10%. При этом объем данных, выгружаемых во внешние системы в автоматическом режиме — более 25%. Большой процент исходящих данных определяется в основном необходимость подключения и выгрузки данных в государственные информационные системы (ФНС, ПФР и т. д.).

–Ни одна из опрошенных организаций не осуществляет автоматический обмен данными с контрагентами (0%).

–Обмен данными преимущественно осуществляется посредством электронной почты (облака) — более 90% обменов.

В целом полученные данные подтверждаются данными из концепции внедрения современного унифицированного формата обмена отчетными данными для участников финансового рынка и нефинансового сектора экономики [1].

Трактовки понятия интеграция систем обычно сводится к следующей: интеграция систем — это выстраивание единого решения или системы из отдельных компонентов (подсистем) и увязывание этих компонентов между собой с целью получения новых свойств решения (системы). Дополнительные свойства получаются за счет совместного использования функций подсистем.

Интеграционные проекты рассматриваются с разных точек зрения, имеющих различные показатели эффективности (Таблица): технической (на уровнях платформ, данных или приложений); управленческой (с учетом бизнес-процессов); коммерческой; политической. В данном случае не учитываются параметры организации телекоммуникационных каналов, систем хранения, особенности используемых форматов обмена данными.

Понятие доверенного обмена в различных источниках трактуется по-разному: и как организация безопасного (защищенного) канала связи, и как защита данных от изменения и/или перехвата в процессе передачи. Также доверенный обмен может рассматриваться как обмен, при котором два участника могут обмениваться данными при условии, что ни один из них не может получить какое-либо преимущество в этом процессе.

Таблица

ПОКАЗАТЕЛИ ПОДХОДОВ К ИНТЕГРАЦИИ СИСТЕМ

№	*Подход*	*Показатель*				
		Количество взаимодейст-вующих систем	*Горизонтальное масштабирова-ние (добавление / разделение систем и функций)*	*Логистика*	*Безопасность данных*	*Безопасность каналов данных*
1	Отсутствие интеграции между системами	Небольшое	Сложное	Сложная	Слабая	Слабая
2	Вертикальная интеграция систем	Среднее	Простое — внутри функциональных блоков, Сложное — между ними	Простая	Высокая	Высокая
3	Интеграция «многие ко многим»	Большое	Сложное	Средняя	Высокая	Средняя
4	Интеграция «звезда»	Небольшое	Среднее	Средняя	Высокая	Средняя
5	Горизонтальная интеграция	Большое	Простое	Простая	Высокая	Средняя
6	Единая система	Произвольное	Сложное	Простая	Высокая	Высокая

Доверие — основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт [2]. Процесс доверенного обмена между двумя участниками можно охарактеризовать схемой, представленной на Рисунке 2.

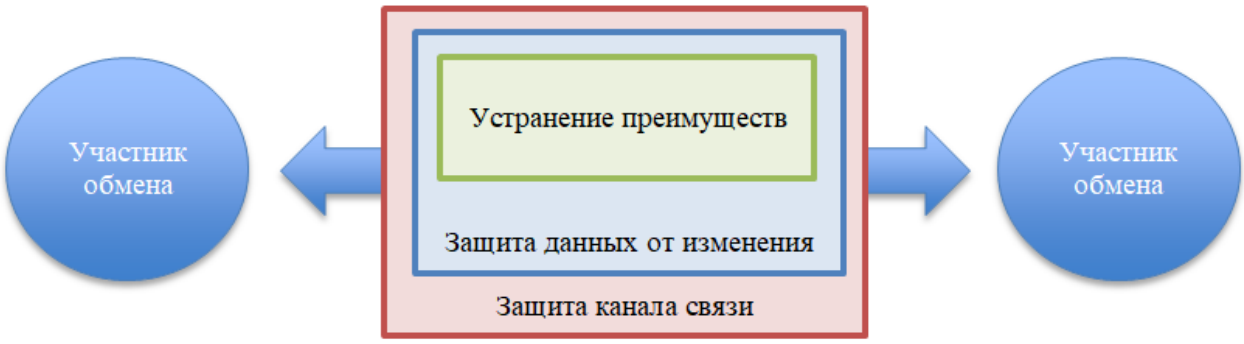

Рисунок 2. Процесс доверенного обмена между двумя участниками

Среди возможных подходов к организации доверенного взаимодействия можно выделить следующие:

–Использование специальных аппаратных и программных средств, обеспечивающих доверенный канал связи.

–Использование механизмов доверия и репутации при выборе каналов связи и промежуточных серверов хранения.

–Использования методов стеганографии для скрытой передачи данных или встраивание специальных меток в сообщения.

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

–Использование технологий контроля целостности (например, имитовставка, HMAC, блокчейн).

–Использование криптографических протоколов (например, CRISP).

Следует отметить, что обеспечение определенного уровня доверия не единичная операция, доверие необходимо поддерживать в процессе функционирования системы. Поддержка доверия — понятие, применение которого предполагается после того, как объект оценки уже оценен и, возможно, сертифицирован. Поддержка требований доверия направлена на получение уверенности в том, что объект оценки будет по-прежнему отвечать требованиям безопасности после изменений в объекте оценки или его среде. К таким изменениям относятся: обнаружение новых угроз или уязвимостей, изменения в требованиях пользователя, исправление ошибок, обнаруженных в объекте оценки, а также другие обновления функциональных возможностей.

Для обеспечения экономически оправданной поддержки доверия целесообразно определить совокупность требований, которые могут применяться к объекту, чтобы убедиться в поддержке установленного доверия, не требуя при этом (в большинстве случаев) переоценки новых версий объекта оценки. В некоторых случаях изменения могут быть настолько значительными, что для дальнейшей поддержки доверия переоценка обязательна. Таким образом, задача сводится не только к выбору наиболее оптимального механизма обмена данными между подсистемами с определенным уровнем доверия, но их выбор с учетом необходимости эффективной поддержки доверия в будущем.

Для локальных систем обеспечение доверенности входящих в их состав узлов является, как правило, достаточным для того, чтобы считать всю систему доверенной. С появлением открытых систем вопрос обеспечения доверенности каналов связи стал более актуальным (в большинстве своем каналы связи принадлежат другим собственникам с другими целями и совсем не обязательно являются доверенными [3]).

При оптимистическом доверенном обмене два участника могут обмениваться своими данными, доверено таким образом, что ни один из них не может получить какое-либо преимущество в этом процессе (передавая избыточную информацию) [4]. Простым способом реализовать доверенный обмен является предоставление третьей доверенной стороны в онлайн режиме, которая выступает в роли посредника: каждый участник отправляет значение третьей доверенной стороне, которая после проверки корректности обоих значений, пересылает их другому участнику. Минусом данного подхода является то, что третья доверенная сторона всегда участвует в обмене, даже если оба участника являются доверенными и не возникает ни одной ошибки. На практике, третья доверенная сторона может стать слабым звеном системы и подвергаться атаке отказа в обслуживании. Простым примером избыточности предоставляемых данных может быть система компоновки данных 1С:Предприятиях. СКД 1С — это способ написания отчетов в 1С, который позволяет пользователю полностью настраивать отчет самостоятельно. При этом разработчики обычно выдают пользователю больше данных, чем нужно для построения типового отчета и у пользователя появляется доступ к множеству второстепенных данных через атрибуты первичных данных.

Следует отметить, что в данном случае под избыточностью не следует понимать термин из теории информации, означающий превышение количества информации, используемой для передачи или хранения сообщения, над его информационной энтропией. Решение проблемы избыточности в теории информации (избыточности представления элементов сообщения) осуществляется применением методов сжатия без потерь. В данном случае избыточность —

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

это превышение количества передаваемых параметров, как с точки зрения количества видов параметров (атрибутов), так и с точки зрения количества значений параметров в пределах одного вида (т. е. избыточность количества элементов сообщения).

Избыточность можно устранить через полную формализацию передаваемых данных, четкое описание форматов представления этих данных, описание ограничений и требований. В данном случае целесообразно использование специализированных форматов обмена данными (например, XBRL). Контроль использования форматов и их уточнение может осуществлять третья сторона (арбитр).

Существует множество способов реализации доверенного канала передачи, часть из них предполагает использование специализированного аппаратного и/или программного обеспечения, часть — реализацию достаточно сложных систем управления (и алгоритмов функционирования этих систем).

С учетом сферы деятельности рассматриваемых предприятий, ни одно из решений не может быть использовано в «чистом виде» по экономическим, техническим или организационным причинам. Однако путем упрощения и комбинации методов, указанных в отмеченных ранее подходах, имеется возможность реализовать систему доверенной передачи данных с требуемым уровнем надежности и достоверности.

Концепция доверенной передачи определяет принципы информационно-телекоммуникационного взаимодействия территориально распределенных систем организации, а также их взаимодействие с другими отраслевыми информационными системами, информационными системами регулирующих органов.

Ключевым принципом организации информационного взаимодействия систем интегрированной информационной системы (*далее — ИИС*) является обеспечение возможности обмена между ними данными оперативного учета взаимодействующих систем в электронном виде и в объеме, необходимом и достаточном для обеспечения непрерывности процессов управления организацией. Состав информации, передаваемой между системами не должен предоставлять участникам взаимодействия дополнительных преимуществ при анализе данных.

Под информационным взаимодействием подсистем ИИС понимается организация информационного взаимодействия между системами, обеспечивающими основные операции в организации. Информация, в процессе информационного взаимодействия подсистем ИИС подлежит защите в соответствии с установленным режимом коммерческой тайны в организации. Организации самостоятельно принимают решение об объемах принимаемых мер и используемых средствах защиты (технических, правовых, организационных или социально-психологических).

Под информационным взаимодействием с отраслевыми системами понимается организация информационного взаимодействия с федеральными информационными системами, системами регулирующих органов.

Информационное взаимодействие с отраслевыми системами осуществляется при соблюдении правил подключения к этим системам (с использованием защищенных сетей сети передачи данных, шифрования, использованием электронных подписей и определенных форматов обмена). Информация, в процессе информационного взаимодействия с отраслевыми системами подлежит защите в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, законодательством Российской Федерации в области охраны здоровья граждан и

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

законодательством Российской Федерации в области персональных данных, требованиями операторов данных.

Информационное взаимодействие осуществляется с использованием программных средств различных операционных систем, некоторые элементы могут быть реализованы с использованием различных виртуальных средств. В ИИС могут включаться также мобильные устройства. Компьютеры и мобильные устройства, на которых установлено программное обеспечение для организации информационного взаимодействия в дальнейшем именуются Клиенты. Клиенты осуществляют подготовку, передачу, прием и анализ данных в процессе взаимодействия.

Обработка данных осуществляется в соответствии с установленными схемами данных информационного взаимодействия. При этом данные могут быть дополнительно обезличены:

–путем введения дополнительных идентификаторов — взаимодействующие системы могут использовать в схемах данных собственные уникальные идентификаторы для критически важных данных;

–методом декомпозиции — данные могут быть разделены и переданы через различных Координаторов;

–методом перемешивания — использование схем данных позволяет представлять данные в потоке в произвольном порядке.

Клиенты могут взаимодействовать между собой непосредственно или через Координатора (или группу координаторов), осуществляющего функции корпоративной шины данных. Координаторы осуществляют проверку данных по схемам данных (контроль избыточности, оценка репутации и доверия) и ретранслируют корректные данные адресатам. При необходимости могут осуществлять хранение данных (хранение схемы данных и данных на одном координаторе нецелесообразно с точки зрения безопасности).

Также в функции Координаторов входит поддержание связности ИИС (маршрутизацию потоков данных между подсистемами ИИС). Наличие нескольких Координаторов обеспечивает более гибкую маршрутизацию данных, повышает надежность и безопасность системы (например, путем использования обезличивания декомпозицией и использованием нескольких маршрутов передачи одновременно).

Клиенты и Координаторы называются узлами сети ИИС. Возможность обмена данными по сети ИИС между узлами (связи узлов) задает администратор для каждого узла.

Архитектура Клиента представлена на Рисунке 3, координатора на Рисунке 4.

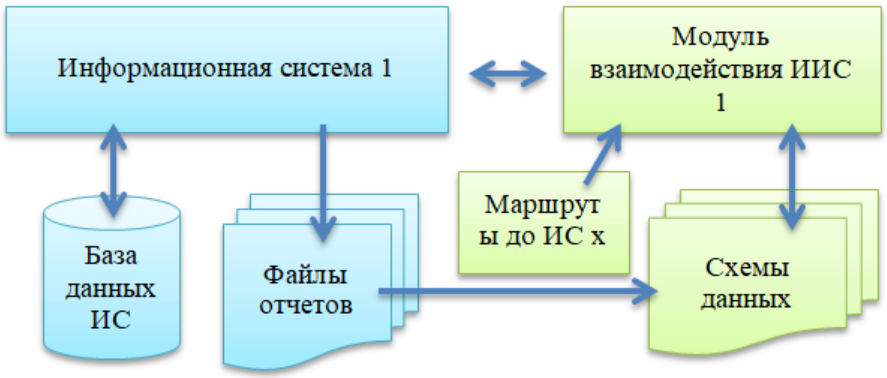

Рисунок 3. Архитектура Клиента ИИС

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

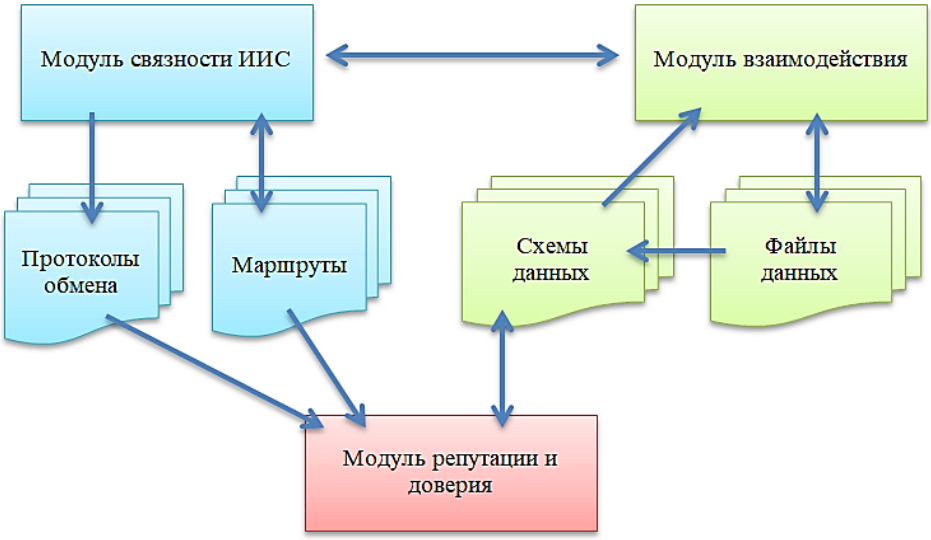

Рисунок 4. Архитектура Клиента ИИС

Как правило, невозможно гарантировать одновременное присутствие всех клиентов в сети ИИС в определенный момент времени. Причины могут быть разные, это и отсутствие подключения к интернету, и проблемы с электрической сетью, и временное прекращение подписки на сервисы подсистемы. Между Клиентами может отсутствовать возможность организации прямого канала связи (NAT, особенности организации системы защиты, политика безопасности организации). Координаторы выполняют роль шлюзов, через которые осуществляется обмен данными и какая-то часть Координаторов должна быть доступа всегда (минимум один). Головной Координатор должен задаваться в настройках клиентов при их развертывании. Дополнительные Координаторы могут подключаться к сети ИИС для повышения надежности, безопасности и организации более оптимальной маршрутизации.

Узлы сети ИИС могут располагаться в сетях любого типа, поддерживающих IP-протокол. Способ подключения узла к сети может быть любой: Ethernet, xDSL, Dial-up или ISDN, сеть сотовой связи, устройства Wi-Fi и другие.

Как правило, два узла в сети ИИС могут взаимодействовать друг с другом находясь в пределах одного сегмента сети. Для доступа к удаленным узлам сети нужно задать маршрут через Координатора. Создание маршрута между двумя узлами означает установку у двух узлов необходимой ключевой информации для организации соединения с выбранным Координатором и указанием Координаторов Клиента-получателя. Каждому клиенту назначается уникальное имя, и он подключается к одному из Координаторов. Обмен служебными данными между Координаторами не подразумевается, все необходимые параметры задаются администратором в настройках Координаторов при их развертывании. Данные передаются Клиентом-отправителем на Координатора Клиента-Получателя, где сохраняются до момента их запроса получателем. При наличии нескольких маршрутов маршрутная информация содержит данные о порядке разделения потока данных между маршрутами.

В общем случае связь узлов ИИС можно описать по принципу «все Клиенты со всеми Координаторами». С целью сокращения трафика число маршрутов между узлами ИИС следует минимизировать и задавать связи исходя из потребностей в обмен данными. Также следует учитывать, что некоторые Координаторы могут быть развернуты в пределах закрытых сегментов локальных сетей организации. При этом должна обеспечиваться уникальная адресация (именование) Координаторов.

Т. 7. №7. 2021
https://doi.org/10.33619/2414-2948/68

На Рисунке 5 представлена схема организации взаимодействия между двумя узлами ИИС. В данном случае имеется два возможных маршрута обмена данными между узлами (Координатор 1 может использоваться для обновления схем данных, Координатор 2 — для обмена данными).

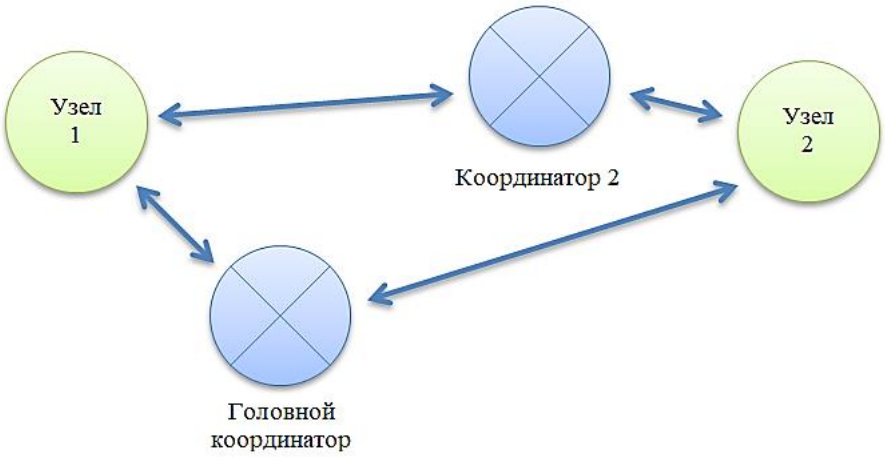

Рисунок 5. Типовая схема взаимодействия двух узлов

Предлагается реализация обмена данными между Координатором и Клиентом с использованием технологии блокчейна (для обеспечения целостности данных при промежуточном хранении). В передаваемые файлы данных встраивается контрольная информация (контрольная сумма) о предыдущем переданном файле.

Результаты исследования свидетельствуют о низком уровне организации доверенного обмена в организациях, особенно в сегменте малых и средних предприятий. Таким образом представляется актуальным разработка алгоритмов, расширяющих возможности используемых систем и позволяющих осуществлять обмен данным между разнородными системами. В данном случае разработанная концепция доверенной передачи данных может использоваться как основа.

Список литературы:

1. Концепция внедрения современного унифицированного формата обмена отчетными данными для участников финансового рынка и нефинансового сектора экономики. https://clck.ru/W5zfR

2. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 19 июня 2002 г. №187. https://clck.ru/W5zqo

3. Доверенная информационная среда и противодействие подмене данных и атакам на каналы управления. https://clck.ru/W5zwh

4. Huang X., Mu Y., Susilo W., Wu W., Xiang Y. Further observations on optimistic fair exchange protocols in the multi-user setting // International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer, 2010. P. 124-141. https://doi.org/10.1007/978-3-642-13013-7_8

References:

1. The concept of introducing a modern unified format for the exchange of reporting data for participants in the financial market and the non-financial sector of the economy. https://clck.ru/W5zfR

2. Guidance document. Information technology security. Criteria for assessing the security of information technology. Approved by the decision of the Chairman of the State Technical Commission under the President of the Russian Federation of June 19, 2002 No. 187. https://clck.ru/W5zqo

3. Trusted information environment and counteraction to data spoofing and attacks on control channels. https://clck.ru/W5zwh

4. Huang, X., Mu, Y., Susilo, W., Wu, W., & Xiang, Y. (2010, May). Further observations on optimistic fair exchange protocols in the multi-user setting. *International Workshop on Public Key Cryptography. Berlin, Heidelberg, Springer, 124-14*. https://doi.org/10.1007/978-3-642-13013-7_8

Работа поступила
в редакцию 20.06.2021 г.

Принята к публикации
24.06.2021 г.

Ссылка для цитирования:

Воронин А. А. Концепция доверенной передачи данных // Бюллетень науки и практики. 2021. Т. 7. №7. С. 164-173. https://doi.org/10.33619/2414-2948/68/22

Cite as (APA):

Voronin, A. (2021). Trusted Data Exchange Concept. *Bulletin of Science and Practice, 7*(7), 164-173. (in Russian). https://doi.org/10.33619/2414-2948/68/22