Анализ моделей идентификации и аутентификации

В. С. Бельский, И. Ю. Герасимов, А. Г. Сабанов, К. Д. Царегородцев

***Аннотация*—В настоящее время оказание различных услуг пользователям производится с использованием цифровых сервисов. Цифровизация существующих процессов требует развития систем обработки информации о пользователях услуг. Система должна обеспечивать идентификацию пользователя и его аутентификацию на основе идентификационных данных, зарегистрированных в данной системе. Для этого применяются системы IAM (Identity and Access Management) - идентификации и управления доступом. По мере развития цифровизации было предложено несколько моделей реализации систем управления учетными записями (данными пользователей), начиная от изолированной модели, в рамках которой во время регистрации сервис (в данной модели иногда просто регистратор) самостоятельно генерирует для пользователя отдельную учетную запись, и заканчивая суверенной моделью, в которой после генерации и выдачи пользователю идентификационных данных сервисом идентификации (Identity Provider, IdP) пользователь может самостоятельно зарегистрироваться в системе и независимо от сервиса выдачи идентификатора выполнять аутентификацию на основе данных, использованных при регистрации.**

В некоторых используемых моделях существует угроза кражи аутентификационных данных пользователя злоумышленником с целью получения некоторой услуги от его имени. Проблема осложняется тем, что переход на цифровые сервисы по обработке услуг не должен исключать их физические аналоги, в которых злоумышленник также не должен иметь возможности использовать данные пользователя для получения услуг от его имени. В статье рассмотрим системы идентификации и аутентификации в соответствии с существующими моделями, а также сравним эти модели в части обеспечения свойств безопасности, скорости выполнения аутентификации и удобства работы для участников процесса аутентификации.

***Ключевые слова*—идентификация, аутентификация, модели идентификации и аутентификации**

I. Введение

Цифровизация существующих процессов требует развития систем обработки информации об участниках процессов. Системы управления доступом, включающих в себя управление идентификационными данными, аутентификацией, авторизацией и учетными записями должны обеспечивать надежную и безопасную идентификацию и аутентификацию (ИА) пользователей. Несмотря на то, что процедура аутентификации является известной задачей и имеет множество решений, перенос существующих идей не позволяет в полной мере обеспечить корректность и безопасность аутентификации в случае удаленного взаимодействия. Задача осложняется тем, что удаленное взаимодействие участников предполагает использование аппаратно-программного обеспечения, которое, в свою очередь, может не иметь привязки к одному участнику и использоваться только как средство установления связи.

В результате процесс аутентификации включает в себя не только аутентификацию пользователя на уровне приложения, но и обеспечение участников аппаратно-программным комплексом на протяжении всего жизненного цикла. По мере развития технологий распределенного и удаленного доступа было предложено несколько моделей реализации систем ИА. Широко распространенной является федеративная модель. Однако одной модели недостаточно в ситуации, когда аутентификация осуществляется на основе уже существующих идентификаторов (например, на основе персональных данных), или аутентифицируемый и аутентифицирующие сущности не имеют собственного аппаратно-программного обеспечения и полагаются на технологии облачных вычислений. В случае добавления соответствующего функционала требуется набор дополнительных мер по обеспечению свойств безопасности со стороны системы управления учетными данными.

В рамках работы проводится анализ моделей ИА с точки зрения выполнения требований безопасности. Цель статьи заключается в анализе того, какие модели ИА рекомендуются к использованию в зависимости от требований безопасности, а также в определении различных ограничений на участников и их возможностей. В зависимости от поставленных целей по реализации ИА в статье сделаны выводы по возможности и порядку доработки рекомендуемых к использованию моделей при сохранении необходимого функционала и требований безопасности.

II. Основные термины и определения

Далее будем использовать следующие определения.

- Автоматизированная система (АС)[1] — система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование.
- Объект информатизации [2] — совокупность информационных ресурсов, средств и систем обработки

Статья получена 12 марта 2024.

Бельский Владимир Сергеевич, Лаборатория Криптографии АО «НПК «Криптонит», (email: v.belsky@kryptonite.ru).

Герасимов Илья Юрьевич, Лаборатория Криптографии АО «НПК «Криптонит», МГУ им. М.В. Ломоносова (email: i.gerasimov@kryptonite.ru).

Сабанов Алексей Геннадьевич, АНО НТЦ ЦК, МГТУ им Н.Э. Баумана, (email: asabanov@mail.ru).

Царегородцев Кирилл Денисович, Лаборатория Криптографии АО «НПК «Криптонит», (email: k.tsaregorodtsev@kryptonite.ru).

информации, используемых в соответствии с заданной информационной технологией, а также средств АС.

- Объект доступа [3] — одна из сторон информационного взаимодействия, предоставляющая доступ.
- Субъект доступа [3] — одна из сторон информационного взаимодействия, которая инициирует получение и получает доступ.
- Атрибут субъекта (объекта) доступа [атрибут] [3] — признак или свойство субъекта доступа или объекта доступа.
- Аутентификация [3] — действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.
- Аутентификационная информация [3] — информация, используемая при аутентификации субъекта доступа или объекта доступа.
- Доверенная третья сторона (ДТС) — участник процессов ИА, предоставляющий один или более сервисов в области защиты информации, которому доверяют другие участники процессов ИА как поставщику данных услуг. При ИА доверенной третьей стороне доверяют все участники процесса — субъект доступа и объект доступа.
- Идентификатор доступа [субъекта (объекта) доступа], [идентификатор] [3] — признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию.
- Идентификация [3] — действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- Первичная идентификация [3] — действия по формированию и регистрации информации о субъекте доступа или объекте доступа, а также действия по присвоению идентификатора доступа субъекту доступа или объекту доступа и его регистрации в перечне присвоенных идентификаторов доступа.
- Вторичная идентификация [3] — действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа при доступе, в перечне идентификаторов доступа, которые были присвоены субъектам доступа и объектам доступа при первичной идентификации.
- Идентификационные данные [3] — совокупность идентификационных атрибутов и их значений, которая связана с конкретным субъектом доступа или конкретным объектом доступа.
- Среда функционирования [3] — среда с предопределенными (установленными) граничными условиями, в которой существуют (функционируют) и взаимодействуют субъекты доступа и объекты доступа.
- Анонимный субъект доступа (аноним) [3] — субъект доступа, первичная идентификация которого выполнена в конкретной среде функционирования, но при этом его идентификационные данные не соответствуют требованиям к первичной идентификации или не подтверждались.
- Аутентификация анонимного субъекта доступа, анонимная аутентификация [3] — аутентификация, используемая для подтверждения подлинности анонимного субъекта доступа.
- Верификация [3] — процесс проверки информации путем сопоставления предоставленной информации с ранее подтвержденной информацией.
- Доверие (assurance) [3] — выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.
- Аргумент доверия (assurance argument) [4] — совокупность структурированных утверждений о доверии, поддерживаемых свидетельством и обоснованием, которые наглядно демонстрируют то, как были удовлетворены требования доверия.
- Оценка доверия (assurance assessment) [4] — верификация и фиксирование всех видов и результатов обеспечения доверия, связанных с оцениваемым объектом (приобщенных к аргументу доверия).
- Электронное удостоверение (Credential) [сертификат доступа] — совокупность идентификационной информации (идентификационных атрибутов) и аутентификационной информации (или прямого указания ее существования в случае использования сертификатов доступа) субъекта или объекта доступа, заверенная ДТС или администратором АС.
- Доверенный объект [3] — объект, который будет действовать в полном соответствии с ожиданиями и субъекта доступа, и объекта доступа или любого из них, при этом выполняя то, что он должен делать, и не выполняя то, что он не должен делать.
- Уровень доверия [3] — степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия.
- Метод обеспечения доверия [3] — общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия.

На основе классификации доверия [3] будем разделять уровни доверия на основе используемых методов обеспечения свойств безопасности в количественном отношении, например, по процентному соотношению количества доверенных объектов информатизации ДТС, а также на основе сравнения различных методов обеспечения свойств безопасности, например, включает ли в себя рассматриваемый метод обеспечение конфиденциальности, целостности и доступности идентификационных и аутентификационных данных.

- Верификатор идентификации [3] — доверенный объект, выполняющий вторичную идентификацию субъекта доступа при доступе.
- Верификатор аутентификации [3] — доверенный объект, выполняющий аутентификацию субъекта доступа при доступе.
- Устройство аутентификации [3] — техническое (аппаратное) или виртуальное устройство, содержащее информацию о его обладателе, которая может использоваться при идентификации и/или аутентификации.
- Метод аутентификации [3] — реализуемое при аутентификации предопределенное сочетание фак-

торов, организации обмена и обработки аутентификационной информации, а также соответствующих данному сочетанию протоколов аутентификации.

- Несанкционированный доступ [3] — доступ субъекта доступа к объекту доступа, нарушающий правила управления доступом.
- Объективное свидетельство [3] — данные, подтверждающие наличие или истинность чего-либо.
- Свидетельство идентичности [свидетельство] [3] — объективное свидетельство, обеспечивающее в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту доступа или объекту доступа, который их заявил.
- Подтверждающая информация [3] — информация, собранная и использованная для подтверждения идентификационных данных в соответствии с установленными требованиям к первичной идентификации.

III. О процессах идентификации и аутентификации

Процессы ИА объектов или субъектов являются обязательными компонентами обеспечения безопасности при управлении доступом. В задачах управления доступом идентификация разделяется на первичную, которая проводится при регистрации объекта или субъекта доступа, и вторичную, которая производится при каждом запросе на доступ. Целью первичной идентификации является установление (подтверждение) соответствия между субъектом доступа и заявленными им идентификационными данными. Полнота и строгость проверки представленных заявителем идентификационных данных определяется политикой безопасности оператора системы. Проверка может проводиться как в ручном, так и в автоматизированном режиме. Первичная идентификация должна завершаться регистрацией (присвоением новому пользователю уникального идентификатора в данной системе) или обоснованным отказом. Причиной отказа может являться недостаточный объем подтверждённых идентификационных данных. Объём связанных с новым пользователем необходимых идентификационных данных определяется политикой безопасности оператора ИС. Первичная идентификация должна ответить на вопрос: тот ли это субъект, за кого себя выдает, и определить возможность регистрации данного субъекта в конкретной системе. Роль аутентификации — обеспечение определенного уровня доверия между взаимодействующими сторонами, определение подлинности зарегистрированных в системе сторон в соответствии с предъявляемыми идентификаторами доступа. Уровень доверия зависит от обмена аутентификационной информацией (односторонний или взаимный), вида аутентификации (простая, усиленная или строгая) и корректности применяемых для аутентификации протоколов. Таким образом, корректность организации первичной идентификации и процесса аутентификации определяет взаимное доверие взаимодействующих сторон. С появлением первых ЭВМ процедуры ИА пользователей являлись физическими процессами. Однако с популяризацией информационных технологий и их внедрением в повседневные процессы увеличилось количество пользователей ЭВМ. В связи с ростом числа пользователей было предложено использовать саму ЭВМ в процессах ИА. Первое известное упоминание ИА с использованием ЭВМ в качестве объекта доступа, играющего роль верификатора аутентификации, датируется 1961 годом [5]. Тогда впервые упоминается концепция использования пароля в качестве аутентификационных данных для предоставления доступа.

Дальнейшее развитие информационных технологий привело к появлению глобальных вычислительных сетей. Таким образом, появилась задача ИА, в которой как объект, так и субъект доступа являются объектами информатизации. Существует множество решений по обеспечению ИА объекта информатизации [6, 7, 8]. Отметим, что отдельное решение может не являться полноценной технологией ИА. Например, IP протокол [7] является протоколом идентификации, но не аутентификации. Для выполнения аутентификации требуется наличие дополнительных средств, например, использование протокола IKE [9].

На сегодняшний день процессы ИА включают в себя ИА в качестве субъекта доступа как устройства, с которого осуществляется взаимодействие, так и пользователя устройства. В рамках статьи мы вводим разделение между ИА объекта информатизации и пользователя. Разделение основано на следующих принципах: если протокол, в рамках которого осуществляется ИА, работает на уровнях сетевой модели TCP / IP ниже прикладного уровня, то протокол соотносится с ИА объекта информатизации. Если протокол, в рамках которого осуществляется идентификация и аутентификация, работает на прикладном уровне сетевой модели TCP / IP, то протокол соотносится с ИА пользователя. Графически разбиение представлено на рисунке 1. Указанное разбиение обусловлено тем, что при наличии у пользователя объекта информатизации, аутентификации только объекта информатизации недостаточно для корректной аутентификации пользователя. Отметим, что аутентификация пользователя может включать в себя требование использования некоторого протокола из уровней ниже для обеспечения некоторых свойств, например, требование использовать протокол TLS [8] для обеспечения свойств безопасности сообщений, передаваемых между объектами информатизации во время аутентификации.

Рис. 1: Аутентификация по уровням сетевой модели TCP/IP

IV. Актуальность задачи

Процессы ИА пользователя в качестве субъекта доступа должны выполняться в соответствии с требованиями безопасности информационной системы (ИС). Среди существующих подходов, реализующих ИА, необходимо определить решение, которое:

- обеспечивает требования безопасности;

- обладает наилучшей скоростью работы;
- является простым в реализации;
- является удобным в использовании.

На практике возникает сложность в выборе соответствующего решения, которое удовлетворяет перечисленным свойствам. Проблема заключается в том, что стандартные решения не учитывают отдельные свойства безопасности, из-за чего разработчику необходимо самостоятельно определить, соответствует ли решение всем требованиям. Например, аутентификация по протоколу OpenID [10] является наиболее перспективной с точки зрения простоты решения, однако она не может быть использована, если аутентификационные данные включают персональные данные пользователя или если требуется, чтобы сервис не мог передавать информацию о пользователе.

С другой стороны, протоколы ИА постоянно модифицируются, чтобы обеспечить дополнительные свойства безопасности. Например, протокол может дополнительно обеспечивать приватность аутентификации [11, 12], при которой идентификаторы участников и аутентификационная информация, использующаяся для вторичной идентификации и аутентификации участников в рамках информационного взаимодействия, являются конфиденциальной информацией. Модификация протокола не должна нарушать уже обеспеченные свойства безопасности, а также, по возможности, быть совместимой с предыдущими версиями и сохранять технические характеристики (например, скорость работы). Если разработчик решает доработать решение, чтобы оно обеспечивало некоторые дополнительные свойства безопасности, первый вопрос, на который ему нужно ответить — возможна ли требуемая модификация решения, сохраняющая все предыдущие свойства исходной системы.

V. Обобщенная модель аутентификации

Для процессов ИА в стандарте [13] определены общие требования и ограничения для соответствующих участников. На основе учета перечисленных в разделе IV требований, построена обобщенная модель ИА, в рамках которой отображены участники процессов, взаимодействие между ними и передаваемые данные. Обобщенная модель определяет базовые принципы осуществления ИА. Она не накладывает каких-либо дополнительных ограничений на работу системы ИА, при этом любую систему можно описать в рамках данной обобщенной модели. Для рассматриваемой системы в рамках обобщенной модели будем дополнительно определять условия по количеству участников, взаимодействию, функционалу и уровню доверия между участниками. Эти условия определяются поставленными перед системой задачами, для которых необходимо обеспечить ИА. Обобщенная модель ИА приведена на рисунке 2.

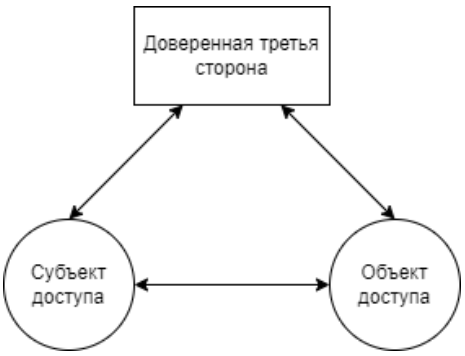

Рис. 2: Обобщенная модель аутентификации

В обобщенной модели определены следующие роли:

- субъект доступа — участник является субъектом доступа, инициирующим запросы на аутентификацию;
- объект доступа — участник является объектом доступа, обрабатывающим запросы на аутентификацию;
- доверенная третья сторона (ДТС) — участник является доверенной третьей стороной, обеспечивающей функции, связанные с подтверждением электронных удостоверений.

Перечисленный функционал участников условно выделяется как роли, поскольку допускается ситуация, когда один объект информатизации выполняет несколько ролей. Например, обобщенная модель включает в себя вариант взаимной аутентификации, при которой два и более участников одновременно являются субъектами и объектами доступа. Также допускается выполнение одной роли несколькими участниками. Например, верификация аутентификационных данных и вторичная идентификация может осуществляться различными верификаторами ИА. Отметим, что для каждой роли должен быть определен участник. При этом возможна ситуация, когда общее число участников меньше общего числа ролей, так как один участник выполняет несколько ролей.

Взаимодействие участников и передаваемые данные описаны в рамках стандарта [14], определяющего функционал системы аутентификации. На основе [14] аутентификационная информация разделена на следующие типы:

- аутентификационная информация уровня обмена (exchange authentication information) — тип информации, передаваемый между участниками;
- аутентификационная информация уровня подтверждения (claim authentication information) — тип информации, используемый субъектом доступа с целью создания аутентификационной информации уровня обмена для аутентификации субъекта доступа [14];
- аутентификационная информация верификации (verification authentication information) — тип информации, связанный с подтверждающей информацией и необходимый для осуществления верификации.

Для примера рассмотрим одностороннюю аутентификацию субъекта доступа посредством использования цифровой подписи. К Аутентификационной информацией уровня подтверждения относится закрытый ключ подписи субъекта доступа. Аутентификационной информацией верификации является сертификат открытого ключа подписи (электронное удостоверение), используемый для проверки подписи. Аутентификационной информацией уровня обмена является сообщение, для которого формируется подпись, сама подпись и сертификат открытого ключа подписи участника.

Процесс ИА в обобщенной модели разбивается на

Рис. 3: Взаимодействие между участниками в обобщенной модели

несколько этапов [14, 15]. Начальный этап является первичной идентификацией пользователя [3].

1) Субъект доступа запрашивает у ДТС регистрацию, предоставляя требуемый для данной системы набор идентификационных данных. ДТС обрабатывает запрос субъекта. ДТС может запрашивать подтверждающую идентификационную информацию из систем, не связанных с АС, в рамках которой выполняется ИА, если система обеспечивает безопасное хранение и обработку запрашиваемой информации (например, из кадровой системы или из официальных государственных реестров) для верификации предоставленной субъектом идентификационной информации. Если при этом результата обработки недостаточно для регистрации, ДТС отклоняет запрос. Если результата обработки достаточно, ДТС формирует идентификатор, аутентификационную информацию уровня обмена субъекта (или хранит информацию о способе подтверждения аутентификационной информации субъектом, например, с помощью закрытого ключа) и сохраняет записи о субъекте.
2) ДТС передает субъекту идентификационную информацию, включающую идентификатор доступа и аутентификационную информацию уровня обмена.

Результатом этапа первичной идентификации является регистрация субъекта в данной АС.

Второй этап является этапом управления регистрационными данными субъектов. Указанный этап выполняется на протяжении всего жизненного цикла АС. В рамках этапа управления данными ДТС:

- создает, обрабатывает, хранит и актуализирует регистрационные данные, полученные во время первичной идентификации субъекта;
- приостанавливает действие, аннулирует и уничтожает регистрационные данные субъекта в случае, когда вторичная ИА невыполнима в рамках информационного взаимодействия объектов информатизации;
- обновляет регистрационные данные пользователя в случае их изменения; если обновление данных инициируется субъектом, субъект должен предоставить идентификационную информацию для повторной идентификации и аутентификационную информацию уровня обмена.

Третий этап является этапом аутентификации и состоит из следующих шагов.

1) Субъект доступа создает запрос на аутентификацию, предъявляя идентификатор доступа.
2) Объект доступа высылает запрос на аутентификационную информацию уровня обмена субъекту.
3) Субъект доступа передает аутентификационную информацию уровня обмена объекту доступа.
4) Объект доступа выполняет верификацию. Если для верификации требуется участие ДТС, объект доступа выполняет запрос к ДТС по подтверждению легитимности и актуальности предоставленной субъектом аутентификационной информации обмена. Если применяемый метод аутентификации не требует участия ДТС (примером является простая аутентификация с применением пароля), то при положительном результате верификации предоставленной субъектом аутентификационной информации аутентификация считается успешно пройденной и осуществляется переход на шаг 7.
5) ДТС проверяет (верифицирует) принятую от объекта аутентификационную информацию верификации и формирует объективное свидетельство (создается с применением регистрационных данных субъекта), которое направляет объекту. В случае применения цифровой подписи ДТС верифицирует электронное удостоверение, в случае положительного результат проверки она высылает объекту объективное свидетельство, подтверждающее, что электронное удостоверение субъекта доступа действительно на момент проверки.
6) Объект выполняет верификацию аутентификационной информации обмена с учетом полученных от ДТС подтверждающей информации.
7) Если результат аутентификации положителен, объект предоставляет доступ субъекту. Если результат аутентификации отрицательный, объект отказывает субъекту в доступе. Если результат не был получен, объект отправляет запрос на дополнительную

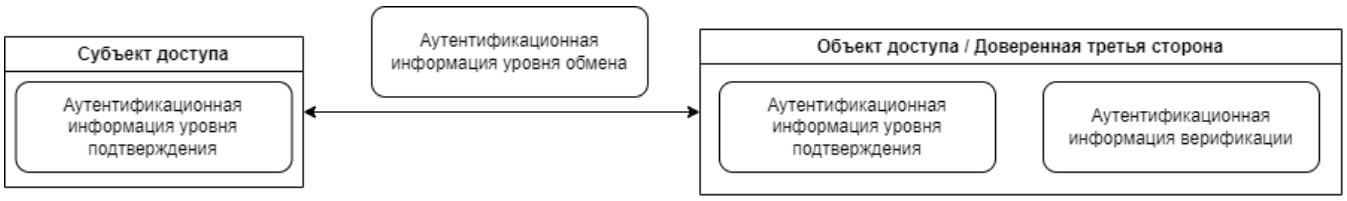

Рис. 4: Изолированная модель аутентификации

аутентификационную информацию, и выполняется переход на шаг 2.

VI. Частные модели идентификации и аутентификации

В этом разделе приводится описание частных моделей систем управления ИА, построенных из обобщенной модели с помощью добавления условий и ограничений, связанных с:

1) ролями участников, количеством участников, выполняющих некоторую роль, возможностью совмещения нескольких ролей;
2) взаимодействием между участниками;
3) передаваемыми данными между участниками;
4) функционалом участников;
5) доверием между участниками;

Приведенные далее модели отражают развитие технологий ИА, актуальные и перспективные на сегодняшний день задачи в отрасли информационных технологий, а также возможности использования в них криптографических средств защиты информации.

Дальнейшее перечисление моделей не является строгой систематизацией моделей ИА. Допускается, что одна реализация системы удовлетворяет функционалу нескольких из перечисленных моделей, а также может быть реализована система, не удовлетворяющая функциям ни одной из перечисленных моделей. Первое допущение связано с тем, что при разработке технологии ИА разработчики стремятся обеспечить универсальность решения и его пригодность в как можно большем числе задач. Второе допущение следует из того, что в рамках развития информационного взаимодействия пользователей возможно появление новых угроз и требований информационной безопасности.

A. Изолированная модель

Изолированная модель является частной моделью ИА, в которой объект доступа одновременно является и ДТС. Название модели обусловлено тем, что первичная идентификация субъекта производится каждым объектом самостоятельно, в результате чего субъект идентифицируется у каждого объекта как отдельный независимый элемент информатизации. Примером реализации изолированной модели являются протоколы парольной аутентификации (Password Authentication Protocols, PAP) [16], в которых аутентифицирующий сервис самостоятельно регистрирует пользователей, хранит и обрабатывает их логины и пароли.

Для изолированной модели имеются следующие условия:

1) Объект доступа играет роль ДТС, управление регистрационными данными осуществляется на стороне объекта доступа. Например, если некоторый сервис выполняет роль объекта доступа, аутентифицируя пользователей по паролю [16], он также выполняет роль ДТС, проверяя актуальность и действительность пароля;
2) Субъект доступа должен хранить аутентификационнную информацию обмена. Объект доступа обрабатывает полученную от субъекта аутентификационную информацию;
3) Поскольку объект доступа является ДТС, модель требует только два шага взаимодействия между субъектом и объектом на этапе аутентификации, в рамках которых субъект отправляет запрос на аутентификацию и аутентификационную информацию и получает результат аутентификации;
4) Субъект доступа доверяет объекту доступа.

Ввиду минимального необходимого количества пересылок изолированная модель является наиболее предпочтительной моделью по скорости выполнения аутентификации. Однако она накладывает серьезное ограничение на работу объекта доступа. В случае нарушения доверия к объекту аутентификационная информация может быть использована как для попытки аутентификации у других сервисов, если у этих объектов используется один метод аутентификации (например, аутентификация на основе биометрических данных), так и для получения какой-либо дополнительной информации об объекте, не указанной в аутентификационной информации, но получаемой с помощью объединения с другой аутентификационной информацией (например, при подмене объекта с использованием фишингового сайта).

B. Централизованная модель

Особенностью изолированной модели является представление субъекта доступа как множества объектов информатизации, никак не связанных между собой и с самим субъектом. На практике существуют случаи, когда субъекту необходимо объединить все имеющиеся идентификаторы в некоторый единый идентификатор (например, пользователь не может хранить у себя слишком большое количество аутентификационной информации или предоставление услуги сервисом требует некоторой информации, которая ему не может быть доверена при первичной идентификации). В качестве решения предлагается использовать некоторый провайдер учетных данных пользователя, который будет выполнять роль ДТС.

Централизованная модель является частной моделью ИА, в которой существует единственный объект информатизации, являющийся ДТС. Название модели обосновано тем, что аутентификационная информация о каж-

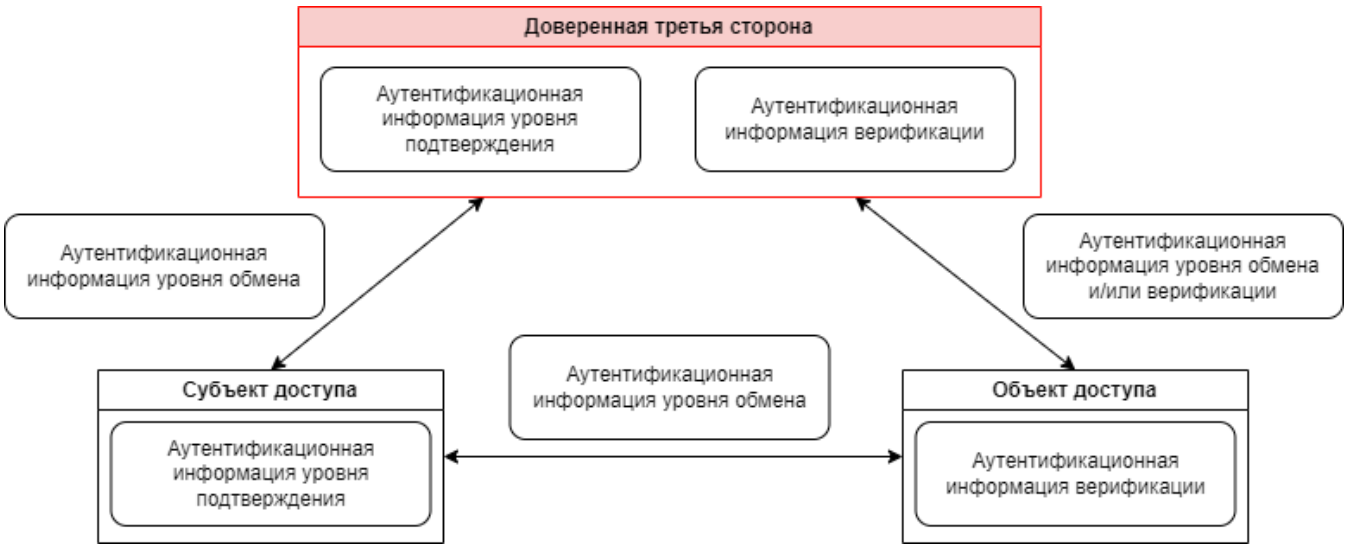

Рис. 5: Централизованная модель аутентификации

дом субъекте хранится в едином месте, а сам субъект представлен одним единым идентификатором. Примером реализации централизованной модели является протокол Kerberos [17], в котором роль ДТС выполняет центр распределения ключей.

Для централизованной модели имеются следующие условия:

1) Существует только один объект информатизации, выполняющий роль ДТС. Например, при использовании протокола аутентификации Kerberos [17] имеется единственный центр распределения ключей, выполняющий роль ДТС.
2) Субъект и объект доступа должны взаимодействовать с ДТС для аутентификации.
3) Условия передачи данных полностью соответствуют обобщенной модели.
4) Субъект и объекты доступа по определению доверяют ДТС.

Централизованная модель является наиболее перспективной моделью в части удобства работы субъекта и объекта доступа. Весь функционал по верификации идентификационных данных и формированию аутентификационных данных может быть передан ДТС. Однако недостатком является единый вектор атаки на ДТС, из-за чего для обеспечения высокого уровня доверия требуется применение серьезных средств по защите информации.

C. Федеративная модель

В рамках информационного взаимодействия возможны ситуации, когда информация о некотором объекте информатизации разделена между несколькими источниками и обрабатывается отдельными ДТС. Для аутентификации субъекта доступа может быть недостаточно участия только одной доверенной стороны. Необходимо решение, в рамках которого можно выполнить аутентификацию на основе проверки подлинности в одной из систем, участвующих в ИА.

Федеративная модель является частной моделью ИА, в которой в процессе верификации могут участвовать несколько ДТС. Название модели обусловлено тем, что идентификационные данные субъекта доступа обрабатываются различными участниками по собственным правилам системы, но могут использоваться для доступа субъекта в другую систему. Примером реализации модели является протокол OpenID Connect [10], в котором сервисы могут аутентифицировать пользователя с помощью информации о пользователе у соответствующих OpenID провайдеров.

Для федеративной модели имеются следующие ограничения:

1) Возможно наличие нескольких объектов информатизации, выполняющих роль ДТС. Например, при использовании протокола OpenID Connect [10] допускается, что аутентификационная информация о субъекте доступа, получаемая с помощью Access Token, может храниться у различных OpenID провайдеров.
2) Субъект и объект доступа должны взаимодействовать хотя бы с одной ДТС для аутентификации.
3) Условия передачи данных полностью соответствуют обобщенной модели.
4) Каждой доверенной стороне доверие обеспечивается только относительно тех данных субъекта, которые доверенная сторона обрабатывает.

Федеративная модель является наиболее предпочтительной по сравнению с перечисленными моделями с точки зрения гибкости решения. Другими словами, в модели учитывается ситуация, когда процессы ИА строятся на основе уже существующих данных пользователей. Однако по сравнению с изолированной и централизованной моделью федеративная модель требует больше затрат по унификации работы с доверенными сторонами и обработки аутентификационной информации верификации.

D. Модель, ориентированная на пользователя

Одним из основных предназначений ИА является защита объекта доступа от несанкционированного доступа. С другой стороны, субъект доступа также может быть уязвим к атакам нарушения конфиденциальности аутентификационной информации. В частности, наличие у ДТС аутентификационных данных всех типов позволяет

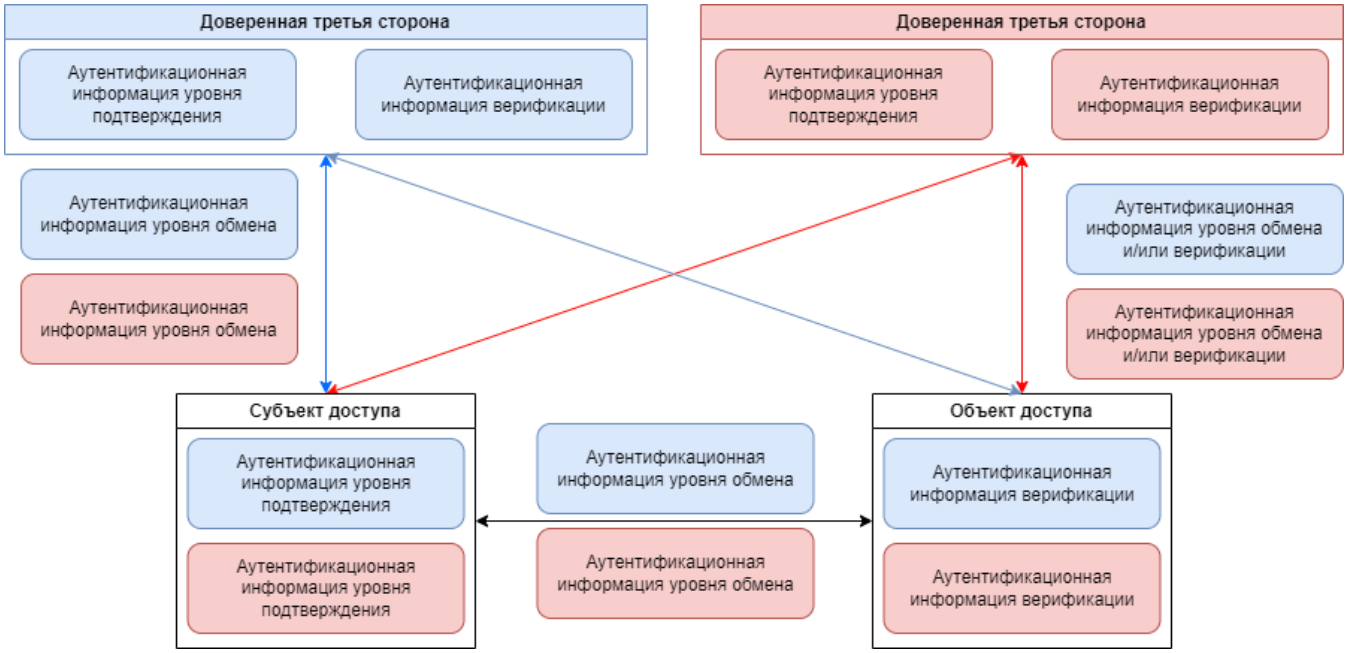

Рис. 6: Федеративная модель аутентификации

реализовывать методы ИА субъекта без его непосредственного участия. В таком случае, объект доступа может пытаться нарушить работу указанных методов с целью получить информацию о пользователе, выходящую за рамки аутентификации. В условиях обеспечения доверия к ДТС возможно обеспечить защиту аутентификационной информации субъекта с помощью защищенных методов ИА, однако необходимо обеспечить доверие субъекта к используемым методам, их корректной реализации и соответствию всем требованиям безопасности.

Также возможна ситуация, когда идентификационная и аутентификационная информация использует уже существующие данные о субъекте доступа. Классическим примером подобной ситуации является использование персональных данных субъекта при выполнении вторичной идентификации и аутентификации. В этом случае объект получает в хранение персональные данные субъекта, для которых должны обеспечиваться конфиденциальность, доступность и целостность. Но обобщенная модель ИА не включает в себя доверие субъекта к объекту доступа в части защиты аутентификационной информации, если объект не выполняет роль доверенной стороны, как, например, в изолированной модели. Поэтому проведение каких-либо мер по обеспечению доверия к объекту в таких случаях может не соответствовать ожиданиям, а чаще и требованиям субъекта доступа. Таким образом, необходимо решение, в котором субъект доступа может самостоятельно контролировать процесс регистрации и запросы на аутентификацию, чтобы быть уверенным в том, что его идентификационная информация не может быть раскрыта объектом доступа.

Модель, ориентированная на пользователя, является частной моделью ИА, в которой аутентификация субъекта доступа возможна только при получении аутентификационной информации уровня обмена объектом от субъекта. Название модели обусловлено тем, что субъект как пользователь системы приобретает дополнительный функционал, направленный на обеспечение защиты информации о нем. Примером реализации модели, ориентированной на пользователя, является ИКС-протокол [18], в котором для контроля аутентификации субъектом используется алгоритм цифровой подписи, а для защиты аутентифицируемой информации верификации, представленной в виде персональных данных, используется алгоритмы шифрования и согласования ключа с ДТС.

Для модели, ориентированной на пользователя, имеются следующие условия:

1) Роли участников не имеют дополнительных свойств в части количества участников и совмещения ролей. Любой участник, имеющий возможность выполнять роль доверенной стороны или субъекта/объекта доступа в соответствии с требованиями безопасности, может взять на себя соответствующую роль. Каждый участник может выполнять только одну роль;
2) Субъект самостоятельно выбирает идентификационную и аутентификационную информацию, которую предоставляет при регистрации;
3) У субъекта доступа должна быть возможность предотвратить атаки со стороны объекта доступа на получение аутентификационной информации верификации;
4) Субъект доступа не имеет доверия к ДТС в части попыток злоумышленников выполнить аутентификацию от имени субъекта доступа.

Модель, ориентированная на пользователя, является наиболее перспективной для применения в системах, где для аутентификации используется конфиденциальная информация пользователя. Однако модель не включает в себя требование по обеспечению анонимности субъекта.

E. Модель сервисной аутентификации

Дополнительные ограничения на модель ИА в свою очередь влекут за собой необходимость в дополнительном аппаратно-программном обеспечении участников с

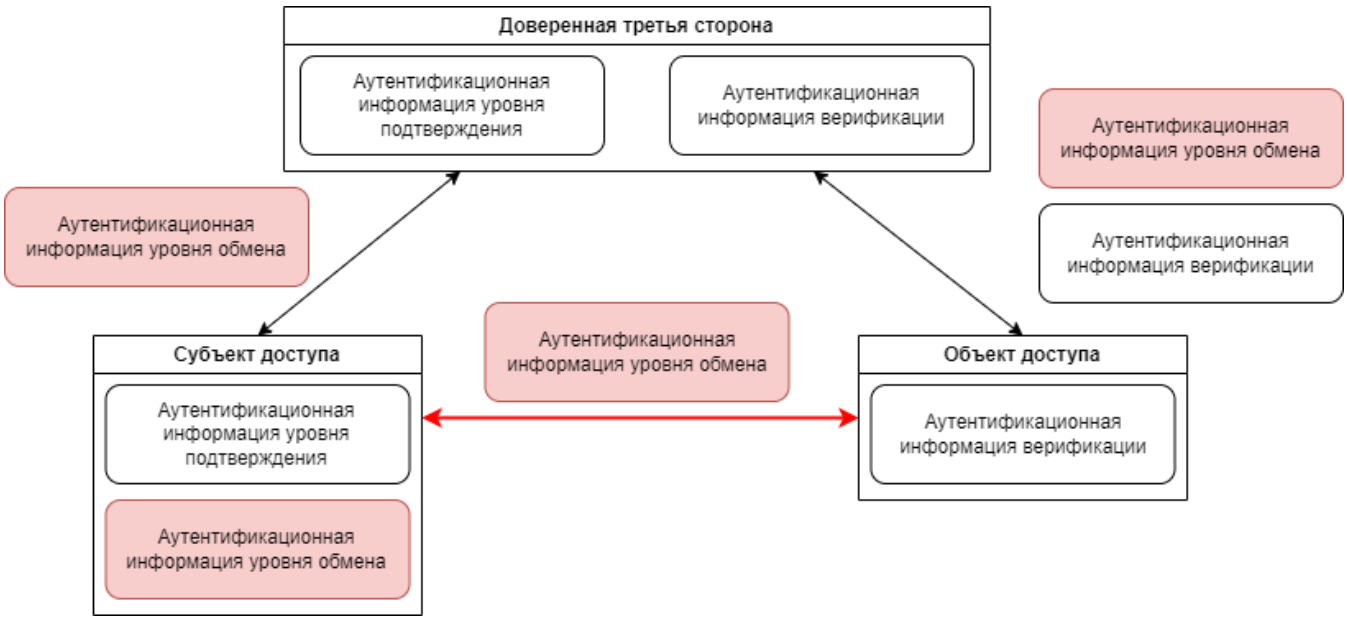

Рис. 7: Модель, ориентированная на пользователя

целью выполнения этих ограничений, что является очень сложной, трудозатратной, а иногда и невозможной задачей, связанной с контролем версий, установкой ПО, поддержкой СКЗИ и дополнительными функциями по сопровождению участников аппаратно-программным обеспечением. Возможным решением является построение системы ИА таким образом, чтобы от субъекта и объекта доступа не требовалось обеспечивать дополнительный функционал по работе с аутентификационной информацией.

Модель сервисной аутентификации является частной моделью ИА, в которой субъект и объект не имеют функционал для работы с аутентификационной информацией. Название модели обусловлено тем, что аутентификационная информация уровня обмена, передаваемая между субъектом и объектом, формируется на стороне ДТС, играющую роль сервиса обработки аутентификационных данных. Примером реализации модели сервисной аутентификации являются облачные решения [19], в рамках которых все вычисления производятся на удаленном от субъекта и объекта сервере.

Для модели сервисной аутентификации имеются следующие условия:

1) Роли участников не имеют дополнительных свойств в части количества участников. Любой участник, имеющий возможность выполнять роль доверенной стороны или субъекта/объекта доступа в соответствии с требованиями безопасности, может взять на себя соответствующую роль. Каждый участник может выполнять только одну роль;
2) Субъект и объект доступа должны взаимодействовать с ДТС для формирования аутентификационной информации;
3) Передаваемая аутентификационная информация уровня обмена должна формироваться с участием ДТС;
4) Субъект и объект доступа не могут самостоятельно формировать аутентификационные данные любого типа;
5) Доверие участников соответствует обобщенной модели.

Модель сервисной аутентификации является наиболее перспективной в ситуациях, когда разработчик АС не обладает средствами для предоставления аппаратно-программного обеспечения участникам информационного взаимодействия. Однако описанная модель не снимает требования полностью, поскольку ДТС, представляющая собой провайдера разработчика, обязана выполнять функционал, который отсутствует у субъекта и объекта. Также, несмотря на обеспечение доверия участников ДТС, отсутствие возможности самостоятельного контроля передаваемых данных и запросов ИА может оказаться критичным в части раскрытия доверенной стороной информации о взаимодействии субъекта и объекта.

F. Суверенная модель

Важным аспектом реализации модели ИА является обеспечение доверия. Однако само по себе обеспечение уверенности в выполнении целей безопасности не дает гарантии того, что аутентификационная информация надежно защищена и не будет использоваться в каких-либо целях, отличных от выполнения ИА. В таком случае субъект и объект заинтересованы в минимизации действий доверенных сторон при аутентификации, а также в понижении уровня доверия путем использования криптографических средств защиты информации и снижении количества доверенных объектов информатизации.

Суверенная модель является частной моделью ИА, в которой этап аутентификации выполняется без участия ДТС. Название модели обусловлено тем, что после этапа регистрации субъект и объект действуют независимо от остальных участников. Примером реализации модели является использование децентрализованных идентификаторов [20] и верифицируемых учетных данных [21] в качестве аутентификационной информации.

Для суверенной модели имеются следующие условия:

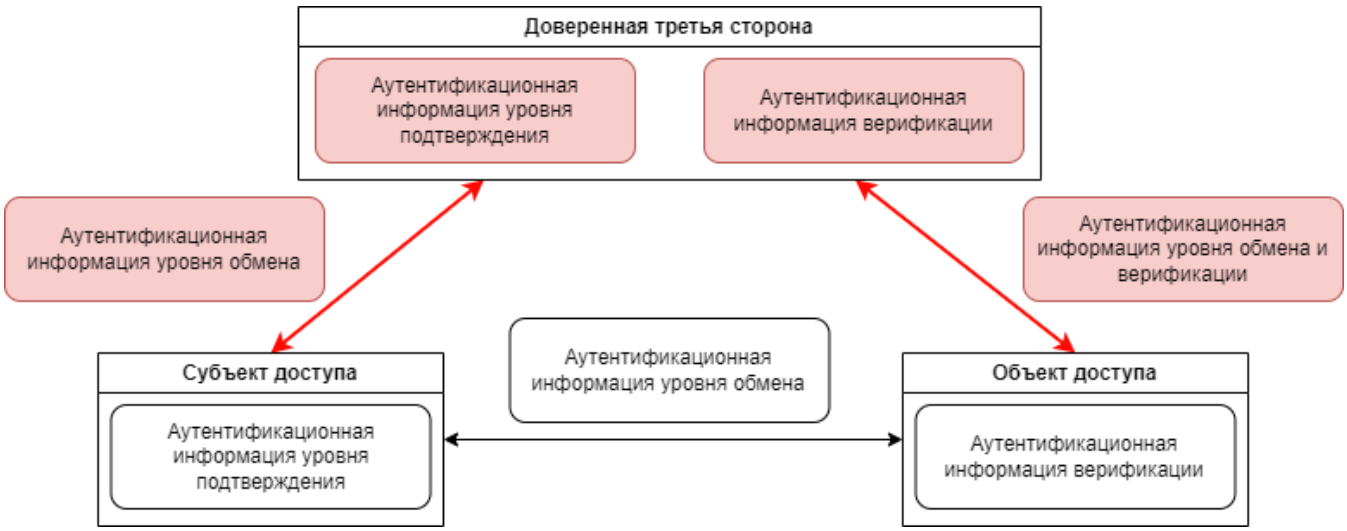

Рис. 8: Модель сервисной аутентификации

1) Роли участников не имеют дополнительных свойств в части количества участников. Любой участник, имеющий возможность выполнять роль доверенной стороны или субъекта/объекта доступа в соответствии с требованиями безопасности, может взять на себя соответствующую роль. Каждый участник может выполнять только одну роль;
2) Субъект и объект доступа не взаимодействуют с ДТС на этапе аутентификации;
3) Аутентификационная информация, соответствующая доступным субъекту и объекту доступа типам, может быть сформирована независимо от ДТС на этапе аутентификации;

Суверенная модель является наиболее перспективной моделью для обеспечения конфиденциальности информационного взаимодействия субъекта и объекта доступа. Однако из всех перечисленных моделей суверенная модель требует обеспечения дополнительных средств криптографической защиты информации, при которых верификация аутентификационной информации может быть выполнена объектом доступа независимо от ДТС.

VII. Сравнение моделей

На основе описания и свойств частных моделей ИА в этом разделе мы выводим несколько утверждений о моделях. При сравнении выделяются следующие критерии сравнения:

- выполнение требований безопасности;
- скорость выполнения ИА;
- простота реализации;
- удобство использования участниками;
- доверие между участниками.

Наиболее подходящей к использованию моделью ИА в АС с точки зрения обеспечиваемых свойств безопасности является суверенная модель. В суверенной модели не требуется установление доверия к третьей стороне на этапе аутентификации, в результате чего обеспечение соответствующих функций по защите аутентификационной информации на этапе аутентификации может быть осуществлено субъектом и объектом доступа самостоятельно, независимо от третьей стороны.

Если рассматривать лучшую модель по скорости выполнения ИА, то следует выбрать изолированную модель. Поскольку в изолированной модели объект доступа выполняет роль ДТС, субъект доступа устанавливает соединение только с объектом доступа. Все аутентификационная информация хранится на стороне объекта доступа, в результате чего для выполнения ИА достаточно выполнить две передачи аутентификационной информации, что является наименьшим значением среди приведенных моделей.

С точки зрения простоты реализации в зависимости от функционала участников информационного взаимодействия можно выделить несколько моделей. Если субъект доступа имеет необходимое аппаратно-программное обеспечение, удовлетворяющее требованиям АС, и имеется только один объект доступа, то изолированная модель является более простой в реализации, так как не требует от объекта доступа, выполняющего роль ДТС, предоставления пользователю соответствующего аппаратно-программного обеспечения на протяжении всего жизненного цикла АС. В противном случае, если имеется объект информатизации, имеющий весь необходимый функционал для выполнения роли ДТС, то наиболее подходящей является модель сервисной аутентификации, так как разработчику необходимо только обеспечить взаимодействие субъекта и объекта доступа с программным интерфейсом ДТС.

Если указанный объект информатизации отсутствует, но субъект и объект доступа обладают аппаратно-программным обеспечением, которое удовлетворяет требованиям или может быть использовано для выполнения требований безопасности ИА, наиболее подходящей является централизованная модель, в рамках которой разработчик формирует объект информатизации, выполняющий роль ДТС, на основе аппаратно-программного обеспечения участников. В случае невыполнения всех предыдущих условий, а именно отсутствия какого-либо аппаратно-программного обеспечения у участников информационного взаимодействия, наиболее подходящей с точки зрения простоты реализации является модель сервисной аутентификации, в рамках которой разработчик формирует весь необходимый функционал на сто-

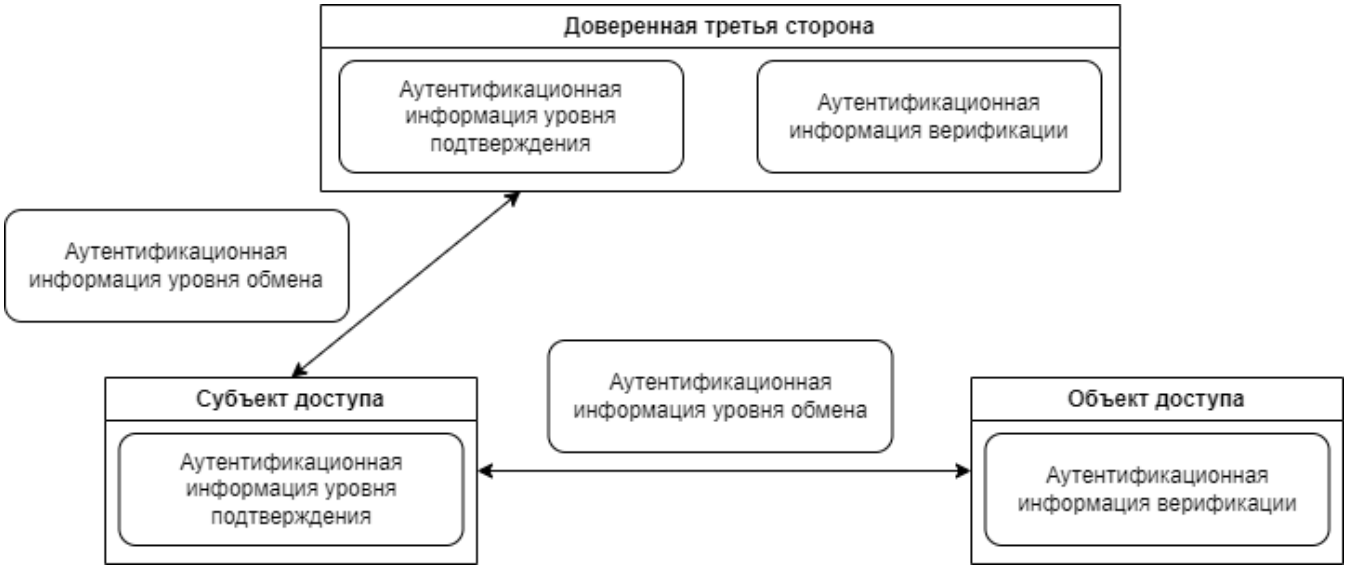

Рис. 9: Суверенная модель аутентификации

Свойства модели	**Оптимальная модель**			
Выполнение требований безопасности	Суверенная модель			
Скорость выполнения ИА	Изолированная модель			
Простота реализации	*Реализована ДТС*	*Не реализована ДТС*		
	Модель сервисной аутентификации	*Субъект с аппаратно-программным обеспечением, один объект*	*Субъект и объект с аппаратно-программным обеспечением*	*Субъект и объект без аппаратно-программного обеспечения*
		Изолированная модель	Централизованная модель	Модель сервисной аутентификации
Удобство использования	*Для субъекта*	*Для объекта*	*Для ДТС*	
	Модель сервисной аутентификации	Централизованная модель	Суверенная модель	
Доверие между участниками	Суверенная модель			

Таблица I: Сравнения частных моделей ИА

роне объекта информатизации, выполняющего роль ДТС. Мы обосновываем выбор модели сервисной аутентификации тем, что сопровождение участника необходимым аппаратно-программным обеспечением с соответствующим контролем версии является более трудоемкой задачей по сравнению с построением архитектуры взаимодействия участников с единым объектом информатизации посредством использования программного интерфейса [22].

По отношению к удобству использования можно выделить разные модели в зависимости от того, для какого участника важно обеспечить простоту работы. Если необходимо обеспечить удобство работы для ДТС, то наиболее подходящей является суверенная модель, так как в этапе аутентификации ДТС не участвует. Если необходимо обеспечить удобство работы для объекта доступа, то наиболее подходящей является централизованная модель, при которой вся информация о субъекте доступа хранится у единой ДТС. Если необходимо обеспечить удобство работы субъекта доступа, наиболее подходящей является модель сервисной аутентификации, при которой субъекту доступа достаточно обратиться к ДТС для осуществления аутентификации.

В части обеспечения минимального доверия между участниками наиболее предпочтительна суверенная модель, поскольку на этапе аутентификации не требуется участия ДТС и, следовательно, отсутствует требование абсолютного доверия субъекта и объекта доступа ДТС. В остальных моделях ДТС, так или иначе участвует в передаче аутентификационной информации.

Итоговые результаты сравнения приведены в таблице I. В рамках приведенных рассуждений мы рассмотрели крайние случаи, когда одна из моделей является наиболее подходящей для обеспечения того или иного требования. Однако на практике решение должно сочетать несколько требований и обладать оптимальным соотношением безопасности и производительности в интересах разработчика и пользователей.

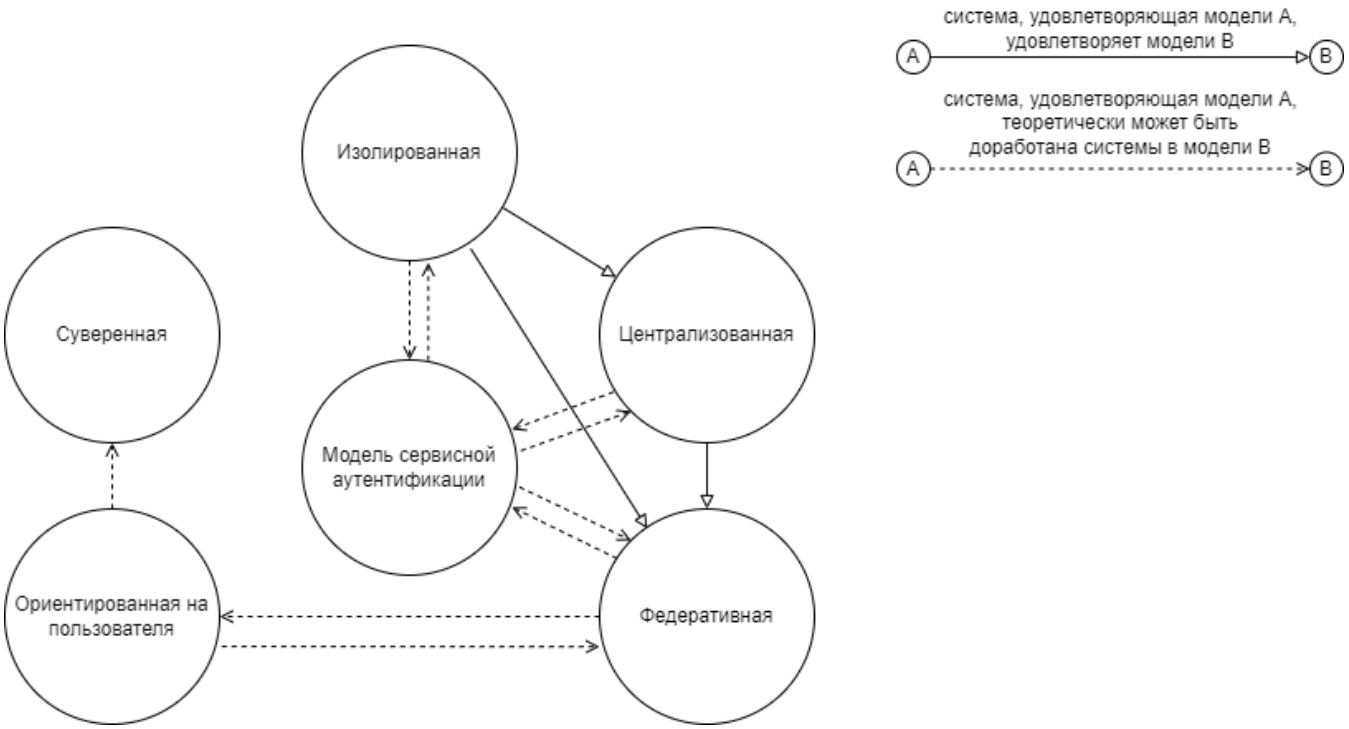

Рис. 10: Система отношений моделей аутентификации

Для помощи в обоснованном выборе модели ИА для каждого конкретного случая мы сформировали систему отношений между моделями, характеризующую наследуемость свойств при переходе от одной модели к другой, а также возможность доработки системы на основе одной модели до некоторой другой модели с сохранением изначальных свойств. В рамках системы отношений мы выделяем два типа связи между моделями. Первый тип отношения между двумя различными моделями A и B обозначен как $A \to B$ и означает, что система, построенная на основе модели A удовлетворяет требованиям модели B без дополнительных доработок системы. Второй тип отношения между двумя различными моделями A и B обозначен как $A \dashrightarrow B$ и означает, что система, построенная на основе модели A теоретически может быть доработана до системы в модели B с сохранением требований модели A. Система отношений указана на рисунке 10.

Отметим следующие особенности. Если выполнено $A \to B, A \neq B$, то выполнено $A \dashrightarrow B$. При этом, если выполнено $A \dashrightarrow B, A \neq B$, то $A \to B$ в общем случае неверно.

Если имеется система, построенная на основе модели A, отношение $A \to B, A \neq B$ и модель C, $C \neq A, C \neq B$, то для того, чтобы система удовлетворяла требованиям всех трех моделей A, B, C необходимо или наличие отношения $A \to C$, или $B \to C$:

$$A \to B \quad \wedge \quad \begin{bmatrix} A \to C \\ B \to C \end{bmatrix} \Rightarrow \quad \begin{array}{c}\text{Система на основе A} \\ \text{удовлетворяет A, B, C}\end{array} \qquad (1)$$

Если имеется система, построенная на основе модели A, отношение $A \dashrightarrow B, A \neq B$ и модель C, $C \neq A, C \neq B$, то для того, чтобы система удовлетворяла требованиям всех трех моделей A, B, C необходимо наличие отношений $A \dashrightarrow C$ и $B \dashrightarrow C$:

$$A \dashrightarrow B \quad \wedge \quad \begin{cases} A \dashrightarrow C \\ B \dashrightarrow C \end{cases} \Rightarrow \quad \begin{array}{c}\text{Система на основе A} \\ \text{дорабатываема до B, C}\end{array} \qquad (2)$$

Уточним отношения между моделями на рисунке 10

- Система на основе изолированной модели удовлетворяет требованиям централизованной и федеративной моделям, так как совмещение ролей ДТС и субъекта доступа не нарушает требование перечисленных моделей. Обратное неверно, так как при наличии нескольких объектов доступа необходимо объединение каждого объекта доступа.
- Система на основе централизованной модели удовлетворяет требованиям федеративной модели, в которой имеется единственная ДТС. Обратное неверно из-за возможного наличия двух или более доверенных сторон.
- Система на основе всех моделей кроме суверенной и ориентированной на пользователя может быть доработана до модели сервисной аутентификации при ограничении функционала субъекта и объекта доступа с сохранением уже выполненных условий. Аналогично система на основе модели сервисной аутентификации может быть доработана до всех моделей, кроме суверенной и ориентированной на пользователя.
- Система на основе суверенной модели не может быть доработана до модели сервисной аутентификации так как ДТС не может участвовать в процессе аутентификации, что требуется в модели сервисной аутентификации. Аналогично модель сервисной аутентификации не может быть доработана до суверенной модели.
- Система на основе модели сервисной аутентификации не может быть доработана до модели, ориенти-

рованной на пользователя, так как возможность ДТС генерировать аутентификационные данные субъекта доступа влечет за собой возможность аутентификации без субъекта доступа.Аналогично в обратную сторону.

- Система на основе суверенной модели не может быть доработана ни до одной модели, так как исключает абсолютное доверие к ДТС.

Приведенные результаты сравнения моделей и система отношений также могут быть использованы для любой частной модели ИА, не перечисленной в статье. Если в рамках обобщенной модели разработчиком добавлены свойства или требования, не указанные ни в одной из моделей, то на основе требуемых свойств и результатов сравнения частных моделей из таблицы I определяется предпочительная частная модель. Далее определяется, возможна ли доработка системы в новой частной модели до системы в выбранной модели. Если доработка возможна, то разработчик может опираться на существующие решения для выбранной модели. Если доработка невозможна, то на основе системы отношений берется другая модель, от которой на системе отношений существует путь до изначально выбранной модели.

Например, рассмотрим ситуацию, когда разработчику необходимо разделить роль ДТС на несколько составляющих ролей, таких как роль удостоверяющего центра и инспектора идентификационных данных, сохранив простоту реализации системы. В таком случае на основе таблицы I наиболее перспктивной являются модели, для которых не реализована ДТС, представляющая из себя две и более компонент. В зависимости от имеющего аппаратно-програмного обеспечения , разработчик выбирает одну из трех приведенных в таблице моделей и строит систему в соответствии с выбранной моделью, где ДТС представляет собой несколько составляющих компонент.

VIII. Заключение

В рамках статьи на основе обобщенной модели ИА рассмотрены частные модели, учитывающие различные аспекты построения систем управления идентификационными данными, в том числе обеспечение защиты аутентификационной информации участников, скорость выполнения вторичной идентификации и аутентификации, простоту реализации и удобство эксплуатации системы. С целью оптимального выбора модели, обеспечивающей выполнение поставленных перед разработчиком задач, и достижения наилучших характеристик работы системы выполнено краткое сравнение моделей по указанным параметрам.

В рамках сравнения были определены несколько моделей, имеющие наилучшие характеристики по рассмотренным свойствам. При этом полученная классификация моделей не является полной и не исключает появление новых решений по обеспечению ИА, для которых процесс аутентификации соответствует государственным стандартам [3, 4] и обобщенной модели [13], но не попадает под описание выделенных частных моделей. В таком случае предлагается соотнести обеспечиваемые свойства новой модели со свойствами уже описанных моделей на основе системы отношений раздела VII. Такой подход поможет разработчику определить не только уникальные для выбранного решения свойства, но и соотнести полученный результат с альтернативными системами на основе перечисленных в работе моделей. Дальнейшим направлением исследований является поиск решений и соответствующих криптографических механизмов, обеспечивающих наилучшие результаты в рамках перечисленных моделей, и систематизация процессов ИА в рамках имеющихся технологий.

Библиография

[1] Государственный стандарт ГОСТ Р 59583-2021 Информационная технология. Коммплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

[2] Государственный стандарт ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

[3] Государственный стандарт ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения.

[4] Государственный стандарт ГОСТ Р 54581-2011/ISO/IEC/TR15443-1:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.

[5] Walden D. C., Van Vleck T. The compatible time sharing system (1961-1973): Fiftieth anniversary commemorative overview. — IEEE Computer Society, 2011.

[6] Государственный стандарт ГОСТ Р ИСО/М ЭК ТО 10171-98 Информационная технология. Передача данных и обмен информацией между системами. Перечень стандартных протоколов уровня звена данных, использующих классы процедур HDLC, и перечень стандартных идентификаторов формата поля ИДС и набора частных параметров значений идентификацторов.

[7] Postel J. Internet protocol—DARPA internet program protocol specification, RFC 791 // (No Title). — 1981.

[8] Dierks T., Rescorla E. RFC 5246: The transport layer security (TLS) protocol version 1.2. — 2008.

[9] Kaufman C., Hoffman P., Nir Y. et al. RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2). — 2014.

[10] Openid connect core 1.0 / N. Sakimura, J. Bradley, M. Jones et al. // The OpenID Foundation. — 2014. — P. S3.

[11] Abadi M., Fournet C. Private authentication // Theoretical Computer Science. — 2004. — Vol. 322, no. 3. — P. 427–476.

[12] Randomizing RFID private authentication / Q. Yao, Y. Qi, J. Han et al. // 2009 IEEE International Conference on Pervasive Computing and Communications / IEEE. — 2009. — P. 1–10.

[13] ISO/IEC 9798-1:2010 Information technology. Security techniques. Entity authentication. — 2010.

[14] ISO/IEC 10181-2:1996 Information technology. Open Systems Interconnection. Security frameworks for open systems: Authentication framework. — 1996.

[15] ISO/IEC 29115:2013 Information technology. Security techniques. Entity authentication assurance framework. — 2013.

[16] Lloyd B., Simpson W. RFC1334: PPP Authentication Protocols. — 1992.

[17] Neuman C., Yu T., Hartman S., Raeburn K. RFC 4120: The Kerberos network authentication service (V5). — 2005.

[18] Протокол обмена персональными данными: ИКС / В. С. Бельский, И. Ю. Герасимов, К. Д. Царегородцев, И. В. Чижов // International Journal of Open Information Technologies. — 2020. — Vol. 8, no. 6. — P. 1–23.

[19] Identity-based authentication for cloud computing / H. Li, Y. Dai, L. Tian, H. Yang // Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1 / Springer. — 2009. — P. 157–166.

[20] Decentralized identifiers (dids) v1. 0 / D. Reed, M. Sporny, D. Longley et al. // Draft Community Group Report. — 2020.

[21] Digital identities and verifiable credentials / J. Sedlmeir, R. Smethurst, A. Rieger, G. Fridgen // Business & Information Systems Engineering. — 2021. — Vol. 63, no. 5. — P. 603–613.

[22] A study of the effectiveness of usage examples in rest api documentation / S. M. Sohan, F. Maurer, C. Anslow, M. P. Robillard // 2017 IEEE symposium on visual languages and human-centric computing (VL/HCC) / IEEE. — 2017. — P. 53–61.

Identification and authentication models analysis

V. Belsky, I. Gerasimov, A. Sabanov, K. Tsaregorodtsev

***Abstract*—Nowadays different processes for the users are provided with usage of digital services. Digitalization of the existing processes requires development of the user information processing systems. The system must provide user identification and authentication using registered identity data. For this task identity and access management systems are used. During the digital systems development, several models for user identity and access management systems were created. Starting from an isolated model where the service (sometimes called the registrar) generates a separate user account during the registration himself, ending with sovereign model, where after identity provider generates and gives the user his identity data, the user can register in the system himself and perform an authentication using registered data without identity provider.**

In some models used there exists a threat of the user authentication data theft by an adversary in order to achieve a service on behalf of the user. The problem is complicated by the fact that the switchover the digital services should not exclude their physical counterpart where an adversary also must not have an ability to use the user authentication data on behalf of the user. The paper considers identification and authentication systems according to the existing models and compares these models in terms of security properties, authentication process performance and the ease of use from each participant perspective.

***Keywords*—Identification, authentication, identity model**

References

[1] Government standard GOST R 59583-2021 Information technology. Set of standards for automated systems. Automated systems. Terms and definitions.

[2] Government standard GOST R 51275-2006 Protection of information. Object of informatisation. Factors influencing the information. General.

[3] Government standard GOST R 58833-2020 Information protection. Identification and authentication. General.

[4] Government standard GOST R 54581-2011/ISO/IEC/TR15443-1:2005 Information technology. Security techniques. A framework for IT security assurance. Part 1. Overview and framework.

[5] Walden D. C., Van Vleck T. The compatible time sharing system (1961-1973): Fiftieth anniversary commemorative overview. — IEEE Computer Society, 2011.

[6] Government standard GOST R ISO/IEC TO 10171-98 Information technology. Telecommunication and information exchange between system. List of standard data link layer protocols that utilize high-level data link control (HDLC) classes of procedures and list of standardized XID format identifiers and private parameter set identification values.

[7] Postel J. Internet protocol—DARPA internet program protocol specification, RFC 791 // (No Title). — 1981.

[8] Dierks T., Rescorla E. RFC 5246: The transport layer security (TLS) protocol version 1.2. — 2008.

[9] Kaufman C., Hoffman P., Nir Y. et al. RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2). — 2014.

[10] Openid connect core 1.0 / N. Sakimura, J. Bradley, M. Jones et al. // The OpenID Foundation. — 2014. — P. S3.

[11] Abadi M., Fournet C. Private authentication // Theoretical Computer Science. — 2004. — Vol. 322, no. 3. — P. 427–476.

[12] Randomizing RFID private authentication / Q. Yao, Y. Qi, J. Han et al. // 2009 IEEE International Conference on Pervasive Computing and Communications / IEEE. — 2009. — P. 1–10.

[13] ISO/IEC 9798-1:2010 Information technology. Security techniques. Entity authentication. — 2010.

[14] ISO/IEC 10181-2:1996 Information technology. Open Systems Interconnection. Security frameworks for open systems: Authentication framework. — 1996.

[15] ISO/IEC 29115:2013 Information technology. Security techniques. Entity authentication assurance framework. — 2013.

[16] Lloyd B., Simpson W. RFC1334: PPP Authentication Protocols. — 1992.

[17] Neuman C., Yu T., Hartman S., Raeburn K. RFC 4120: The Kerberos network authentication service (V5). — 2005.

[18] Personal data exchange protocol: X / Belsky V. S., Gerasimov I. Y., Tsaregorodtsev K. D., Chizhov I. V. // International Journal of Open Information Technologies. — 2020. — Vol. 8, no. 6. — P. 1–23.

[19] Identity-based authentication for cloud computing / H. Li, Y. Dai, L. Tian, H. Yang // Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1 / Springer. — 2009. — P. 157–166.

[20] Decentralized identifiers (dids) v1. 0 / D. Reed, M. Sporny, D. Longley et al. // Draft Community Group Report. — 2020.

[21] Digital identities and verifiable credentials / J. Sedlmeir, R. Smethurst, A. Rieger, G. Fridgen // Business & Information Systems Engineering. — 2021. — Vol. 63, no. 5. — P. 603–613.

[22] A study of the effectiveness of usage examples in rest api documentation / S. M. Sohan, F. Maurer, C. Anslow, M. P. Robillard // 2017 IEEE symposium on visual languages and human-centric computing (VL/HCC) / IEEE. — 2017. — P. 53–61.