Банк России

СТАНДАРТ БАНКА РОССИИ

СТО БР БФБО-1.8-2024

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФИНАНСОВЫХ СЕРВИСОВ ПРИ ПРОВЕДЕНИИ ДИСТАНЦИОННОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

МОСКВА
2024

ПРЕДИСЛОВИЕ

Принят и введен в действие приказом Банка России от 28.02.2024 № ОД-326.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт устанавливает состав и содержание мер для обеспечения доверия к результатам идентификации и аутентификации клиентов – получателей услуг при дистанционном предоставлении поставщиками финансовых продуктов и услуг в целях реализации требований Банка России на технологическом участке идентификации, аутентификации и авторизации клиентов при осуществлении банковской деятельности, деятельности в сфере финансовых рынков, предусмотренной частью первой статьи 76.1 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Федеральный закон № 86-ФЗ) [1], и переводов денежных средств (далее при совместном упоминании – финансовые операции).

Положения настоящего стандарта предназначены для использования кредитными организациями, некредитными финансовыми организациями, указанными в части первой статьи 76.1 Федерального закона № 86-ФЗ [1], субъектами национальной платежной системы (далее при совместном упоминании – финансовые организации). Также положения настоящего стандарта могут применяться иными организациями, реализующими технологические процессы, связанные с проведением идентификации или аутентификации при дистанционном предоставлении продуктов и услуг.

Настоящий стандарт служит для целей содействия соблюдению требований нормативных актов Банка России, устанавливающих требования к обеспечению защиты информации и технологии безопасной обработки защищаемой информации, при осуществлении финансовых операций, в том числе:

- нормативного акта Банка России, устанавливающего обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, принятого на основании статьи 57.4 Федерального закона № 86-ФЗ [5];
- нормативного акта Банка России, устанавливающего обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций, принятого на основании статьи 76.4-1 Федерального закона № 86-ФЗ [6];
- нормативного акта Банка России, устанавливающего требования к обеспечению защиты информации при осуществлении переводов денежных средств и порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств, принятого на основании части 3 статьи 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» [7].

Настоящий стандарт не распространяется на отношения, регулируемые Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ) [2]. При проведении идентификации клиента, представителя клиента и (или) выгодоприобретателя в соответствии с требованиями Федерального закона № 115-ФЗ положения настоящего стандарта могут применяться в дополнение к требованиям Федерального закона № 115-ФЗ.

Положения настоящего стандарта носят рекомендательный характер, если только обязательность применения отдельных из них не установлена нормативными правовыми актами, в том числе нормативными актами Банка России. Настоящий стандарт может быть использован для включения ссылок на него и (или) прямого включения содержащихся в нем положений во внутренние документы финансовых организаций, а также в договоры, заключенные между финансовыми организациями.

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использованы нормативные ссылки на следующие документы:

- ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения», утвержденный и введенный в действие приказом Росстандарта от 10.04.2020 № 159-ст (далее – ГОСТ Р 58833-2020);
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденный и введенный в действие приказом Росстандарта от 08.08.2017 № 822-ст (далее – ГОСТ Р 57580.1-2017);
- ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации», утвержденный и введенный в действие приказом Росстандарта от 05.08.2022 № 740-ст (далее – ГОСТ Р 70262.1-2022);
- ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения», утвержденный и введенный в действие приказом Росстандарта от 22.12.2022 № 1548-ст (далее – ГОСТ Р 57580.3-2022);
- Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации», утвержденные и введенные в действие приказом Росстандарта от 22.12.2017 № 2068-ст (далее – Р 1323565.1.012-2017).

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем стандарте термины «аутентификационная информация», «аутентификация», «верификация», «верифицирующая сторона», «вторичная идентификация», «доверие», «идентификационная информация», «идентификационный атрибут», «идентификация», «первичная идентификация», «протокол аутентификации», «среда функционирования», «средство аутентификации (аутентификатор)», «уверенность», «уровень доверия», «устройство аутентификации», «фактор» применены в значениях, определенных ГОСТ Р 58833-2020 и ГОСТ Р 70262.1-2022, а также используются следующие термины с соответствующими определениями:

Делегирование идентификации/аутентификации – процесс передачи поставщиком услуг обязанности или права проведения идентификации или аутентификации получателя услуг доверенной третьей стороне.

Доверенная третья сторона – организация, предоставляющая один сервис или более, участвующий при проведении идентификации или аутентификации получателя услуг, которой доверяют другие участники взаимодействия в отношении данных сервисов (поставщик услуг и получатель услуг).

Канал взаимодействия – физическое или логическое соединение, которое обеспечивает взаимодействие между сторонами информационного взаимодействия.

Метка времени – достоверная информация о моменте создания электронного сообщения, которая присоединена к нему или иным образом связана с ним.

Перенаправление (redirect) – процесс автоматической переадресации с одного URL-адреса на другой.

Получатель услуг – физическое или юридическое лицо, являющееся клиентом поставщика услуг в целях получения финансовых продуктов и услуг; поставщика услуг.

Поставщик услуг – финансовая организация, предоставляющая финансовые продукты и услуги дистанционным способом, для получения которых клиентам финансовой организации необходимо пройти идентификацию и аутентификацию.

Программный сервис – программный компонент, выполняющий операции от имени цифровой идентичности получателя услуг и с его разрешения, но без его личного участия.

Протокол взаимодействия[1] – прикладной протокол, в рамках которого стороны информационного взаимодействия последовательно выполняют определенные действия и обмениваются сообщениями в соответствии с заданным форматом.

Процедура[2] – установленный способ осуществления процесса.

Процесс[3] – совокупность взаимосвязанных и (или) взаимодействующих видов деятельности, использующих входы для получения намеченного результата.

Сведения об идентификации/аутентификации – данные о фактах и результатах проведения идентификации/аутентификации получателя услуг в рамках цифровой идентичности и цифровой среды.

Служба идентификации/аутентификации – компонент собственной информационной системы поставщика услуг, осуществляющий проведение идентификации/аутентификации получателей услуг.

Сервис идентификации/аутентификации – компонент информационной системы идентификации/аутентификации доверенной третьей стороны, дистанционно предоставляемый для

---

[1] В рамках данного стандарта термин используется в отношении протоколов взаимодействия, реализующих процессы идентификации и аутентификации.

[2] В рамках данного стандарта термин используется в отношении процедур, устанавливающих процессы идентификации и аутентификации.

[3] В рамках данного стандарта термин используется в отношении процессов идентификации и аутентификации.

проведения идентификации/аутентификации получателей услуг при их делегировании доверенной третьей стороне.

Состояние идентификационной/аутентификационной информации – характеристика идентификационной/аутентификационной информации, определяющая, на каком этапе жизненного цикла находится идентификационная или аутентификационная информация.

Цифровая идентичность – цифровое представление получателя услуг в виде набора атрибутов, характеризующих данного получателя услуг, и их значений, каждый из которых имеет свой уникальный идентификатор в рамках конкретной цифровой среды.

Цифровая среда – среда функционирования, в которой поставщиком услуг осуществляется предоставление получателям финансовых продуктов и услуг.

4. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ГИС – государственная информационная система
ДТС – доверенная третья сторона
ЕСИА – федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
СКЗИ – средство криптографической защиты информации
УДА – уровень доверия аутентификации
УДИ – уровень доверия идентификации
ФЛ – физическое лицо
ЮЛ – юридическое лицо
CAPTCHA – completely automated public Turing test to tell computers and humans apart (полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей)
DFP – device fingerprint (цифровой отпечаток устройства)
IMSI – international mobile subscriber identity (международный идентификатор мобильного абонента, индивидуальный номер абонента)
OSI – open systems interconnection (взаимодействие открытых систем)
PIN – personal identification number (персональный идентификационный номер, ПИН-код)
SIM – subscriber identification module (модуль идентификации абонента, сим)
TLS – transport layer security (протокол защиты транспортного уровня)

5. ОБЩИЕ ПОЛОЖЕНИЯ

Под средой доверия при проведении идентификации и аутентификации в целях предоставления финансовых продуктов и услуг понимают такое состояние среды взаимодействия между финансовой организацией – поставщиком услуг и клиентом – получателем услуг, а также при возможном участии организаций, предоставляющих один сервис или более, участвующий в идентификации и аутентификации, при котором обеспечена необходимая уверенность в том, что получатель услуги соответствует представленной идентификационной информации (идентифицирован), а также является тем, за кого себя выдает (аутентифицирован).

Настоящий стандарт развивает положения ГОСТ Р 58833-2020 в части организации процессов дистанционной идентификации и аутентификации и обеспечения необходимой уверенности в результатах, а также нормативных актов Банка России, устанавливающих требования к обеспечению защиты информации при осуществлении финансовых операций [5, 6, 7] в части технологии безопасной обработки защищаемой информации на технологическом участке идентификации, аутентификации и авторизации клиентов при осуществлении финансовых операций в целях противодействия осуществлению незаконных финансовых операций.

В рамках настоящего стандарта процессы идентификации и аутентификации применяются в соответствии с описанием, приведенным в ГОСТ Р 58833-2020, и включают в себя следующие составляющие:

- первичная идентификация (регистрация);
- вторичная идентификация;
- аутентификация;
- делегирование идентификации или аутентификации;
- передача идентификационной или аутентификационной информации и сведений об идентификации или аутентификации.

Описание указанных процессов, их цели, этапы и ожидаемые результаты установлены ГОСТ Р 58833-2020, если в настоящем стандарте не указано иное.

В рамках настоящего стандарта рассматривается только дистанционное предоставление финансовых продуктов и услуг финансовой организацией, в связи с чем идентификация и аутентификация также являются дистанционными, то есть осуществляются без личного присутствия клиента в финансовой организации. Далее по тексту настоящего стандарта под терминами «идентификация» и «аутентификация» подразумеваются дистанционные процессы.

В процессах идентификации и аутентификации участники взаимодействия могут выступать в следующих ролях: поставщик услуг, получатель услуг, доверенная третья сторона. Наличие или отсутствие указанных ролей в процессах идентификации и аутентификации зависит от конкретной реализации процессов предоставления финансового продукта или услуги.

6. ПОРЯДОК ПРИМЕНЕНИЯ НАСТОЯЩЕГО СТАНДАРТА

Настоящий стандарт определяет состав и содержание мер защиты информации для обеспечения доверия к результатам идентификации и аутентификации получателей услуг при осуществлении финансовых операций. Уровень доверия идентификации и аутентификации определяется степенью уверенности в результатах идентификации и степенью уверенности в результатах аутентификации, как определено в ГОСТ Р 58833-2020.

Для использования дифференцированного подхода в рамках системы обеспечения доверия применяются предопределенные уровни доверия, которые определяют уверенность в результатах идентификации и аутентификации получателей услуг. Минимальный состав мер защиты информации, которому должны соответствовать процессы идентификации и аутентификации для достижения необходимой уверенности, определяется для каждого из уровней доверия.

Выбор уровня доверия осуществляется исходя из критичности финансовой операции, которая будет проведена после идентификации и аутентификации. Основным критерием при выборе наиболее подходящего уровня доверия должен являться результат оценки операционного риска, то есть должен применяться риск-ориентированный подход. Оценка операционного риска критичности операции при выборе уровня доверия должна осуществляться кредитными организациями с учетом требований к системе управления операционным риском, установленных Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» [8], а иными финансовыми организациями – в соответствии с установленной внутренними документами политикой управления операционным риском.

В соответствии с риск-ориентированным подходом финансовые организации должны установить во внутренних документах уровни доверия в разрезе осуществляемых финансовых операций. Также, так как одна и та же финансовая операция в зависимости от ее характера и параметров может иметь различную критичность, финансовые организации должны установить во внутренних документах конкретные показатели оценки операционного риска, характеризующие принадлежность финансовой операции к конкретному уровню доверия (далее – показатели оценки операционного риска).

Дополнительно результаты идентификации и аутентификации с учетом выбранного уровня доверия могут применяться в рамках системы управления рисками для определения остаточного риска в целях противодействия осуществлению финансовых услуг без согласия клиента.

Настоящий стандарт определяет состав и содержание мер защиты информации, применяемых к:

- процессу идентификации в разрезе УДИ;
- делегированию идентификации ДТС;
- процессу аутентификации в разрезе УДА;
- процессу аутентификации при использовании отдельных аутентификаторов (приложение 2 к стандарту);
- делегированию аутентификации ДТС.

Финансовые организации должны учитывать при разработке модели угроз безопасности информации в отношении технологических процессов, реализующих финансовые операции, угрозы безопасности процессов идентификации и аутентификации. Для нейтрализации выявленных угроз финансовые организации должны обеспечивать реализацию мер защиты информации, установленных настоящим стандартом (таблицы 3, 6, 7, 8).

При этом для мер защиты информации, предусматривающих конкретные контрольные значения для реагирования (например, ограничение времени пользовательского сеанса или доверительный интервал метки времени), финансовой организации необходимо установить во внутренних документах конкретные контрольные значения для каждой такой меры защиты исходя из модели угроз безопасности информации, а также из установленных показателей оценки операционного риска.

При невозможности реализации отдельных выбранных мер защиты информации, а также с учетом экономической целесообразности финансовая организация может применять компенсирующие меры, направленные на обработку операционного риска, связанного с реализацией тех же угроз безопасности информации, на нейтрализацию которых направлены меры из настоящего стандарта, не применяемые финансовой организацией в связи с невозможностью реализации и (или) экономической нецелесообразностью. При этом финансовая организация должна во внутренних документах обосновать применение компенсирующих мер защиты информации, в том числе в части подтверждения нейтрализации определенных угроз безопасности информации, а также определить порядок и периодичность контроля за реализацией компенсирующих мер.

В случае если конкретная мера защиты информации является неактуальной в рамках конкретного технологического процесса, финансовая организация должна во внутренних документах обосновать неактуальность данной меры защиты информации.

Обоснование применения компенсирующих мер защиты информации или неактуальности мер защиты информации должно в том числе содержать:

- наименование технологического процесса, реализующего финансовые операции;
- описание неприменяемой или неактуальной меры защиты информации;
- перечень угроз безопасности информации, которые нейтрализует данная мера защиты информации;
- отсылку (выписку) на модель угроз безопасности информации технологических процессов, реализующих финансовые операции, подтверждающую актуальность или неактуальность данных угроз для технологического процесса;
- для обоснования применения компенсирующих мер защиты информации – перечень и описание компенсирующих мер защиты информации, содержащее в том числе подтверждение факта нейтрализации угроз безопасности информации для технологического процесса, которые были определены для неприменяемой меры защиты информации.

При применении настоящего стандарта также необходимо учитывать следующее.

В случае если идентификационная или аутентификационная информация содержит персональные данные, необходимо применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [3], постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [9], приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [11] и приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [12].

Использование СКЗИ и (или) средств электронной подписи при проведении идентификации и аутентификации должно осуществляться в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» [4], приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» [10] и технической документацией на СКЗИ и (или) средство электронной подписи.

Безопасность обработки, предоставления доступа, хранения и уничтожения идентификационной и аутентификационной информации после проведения идентификации и аутентификации необходимо обеспечивать с учетом требований ГОСТ Р 57580.1-2017.

7. СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ДИСТАНЦИОННОЙ ИДЕНТИФИКАЦИИ

7.1. УРОВНИ ДОВЕРИЯ ИДЕНТИФИКАЦИИ

УДИ устанавливаются в рамках процесса идентификации, включающего в себя:

- первичную идентификацию (регистрацию) получателей услуг, являющихся физическими лицами и представителями юридических лиц;
- вторичную идентификацию получателей услуг, являющихся физическими лицами и представителями юридических лиц.

Для финансовых организаций устанавливаются три УДИ, определяющих уверенность в результатах идентификации: низкий (УДИ 1), средний (УДИ 2) и высокий (УДИ 3). В таблице 1 приведены критерии для каждого УДИ, определяющие соответствующий уровень уверенности в результате идентификации.

КРИТЕРИИ, ОПРЕДЕЛЯЮЩИЕ СООТВЕТСТВУЮЩИЙ УРОВЕНЬ УВЕРЕННОСТИ В РЕЗУЛЬТАТАХ ИДЕНТИФИКАЦИИ *Табл. 1*

Критерий	**Уровень доверия идентификации**		
	УДИ 1	**УДИ 2**	**УДИ 3**
Уверенность в результатах идентификации	Некоторая уверенность	Умеренная уверенность	Значительная уверенность
Идентификационная информация верифицирована[4]	Нет	Да	Да[5]
Идентификационная информация соответствует получателю услуг, который ее заявил	Да	Да	Да
Идентификационная информация уникальна в контексте конкретной цифровой среды	Да	Да	Да
Цифровая идентичность однозначно определяется соотнесенным с ней предъявленным идентификатором	Да	Да	Да
Идентификатор имеет однозначную связь с получателем услуги	Нет	Да	Да

Поставщик услуг должен определять необходимый УДИ во внутренних документах для каждой предоставляемой финансовой операции на основании анализа рисков с учетом требований применения УДИ к финансовым операциям поставщика услуг, приведенных в таблице 2.

Осуществление финансовой операции при проведении идентификации в случае несоответствия процесса идентификации требованиям УДИ, установленного для данной финансовой операции, не допускается.

[4] В таблице П-1 приложения 1 приведены примеры реализации процесса верификации в разрезе уровней доверия идентификации, определенных в данном разделе.

[5] Для данного УДИ верификация должна проводиться с использованием сведений как минимум одной уполномоченной верифицирующей стороны, являющейся информационной системой органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования или иных ГИС.

ПРИМЕНЕНИЕ УДИ К ФИНАНСОВЫМ ОПЕРАЦИЯМ ПОСТАВЩИКА УСЛУГ *Табл. 2*

Финансовые операции поставщика услуг	Допустимые УДИ		
	УДИ 1	УДИ 2	УДИ 3
Предоставление информационных сервисов ФЛ	+	+	+
Предоставление информационных сервисов ЮЛ	–	+	+
Совершение финансовых операций ФЛ, оценка операционного риска которых не превышает установленных во внутренних документах показателей оценки операционного риска	–	+	+
Совершение высокорисковых (оценка операционного риска превышает установленные во внутренних документах показатели оценки операционного риска) финансовых операций ФЛ	–	–	+
Совершение финансовых операций ЮЛ	–	–	+

7.2. ТРЕБОВАНИЯ К ПРОЦЕССУ ИДЕНТИФИКАЦИИ

Состав мер защиты информации, применяемый к процессу идентификации, приведен в таблице 3[6].

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ К ПРОЦЕССУ ИДЕНТИФИКАЦИИ *Табл. 3*

№	Содержание меры защиты информации	УДИ 1	УДИ 2	УДИ 3
1. Состав мер защиты информации, применяемый к службе идентификации				
1.1	Служба идентификации должна предоставить получателю услуг информацию о прохождении первичной идентификации, в том числе о цели сбора и составе идентификационной информации, после чего получатель услуги должен подтвердить намерение пройти первичную идентификацию	ПИ	ПИ	ПИ
1.2	Служба идентификации должна осуществлять сбор минимально достаточного состава идентификационной информации, необходимой для проведения первичной идентификации получателя услуг, определенного во внутренних документах поставщика услуг	ПИ	ПИ	ПИ
1.3	Служба идентификации должна верифицировать идентификационную информацию получателя услуг в соответствии с положениями ГОСТ Р 70262.1-2022 и с использованием сведений как минимум одной верифицирующей стороны	Н	ПИ	–
1.4	Служба идентификации должна верифицировать идентификационную информацию получателя услуг в соответствии с положениями ГОСТ Р 70262.1-2022 и с использованием сведений как минимум одной уполномоченной верифицирующей стороны, являющейся информационной системой органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования или иных ГИС	Н	Н	ПИ
1.5	Служба идентификации для определения и поддержки уникальности цифровой идентичности в рамках конкретной цифровой среды должна использовать идентификаторы, которые имеют однозначную связь[7] с получателем услуг	Н	О	О

[6] В таблице 3 используются следующие обозначения обязательности реализации мер защиты:
О – обязательная мера защиты для УДИ;
ПИ – обязательная мера защиты для первичной идентификации получателей услуг, проводимой по УДИ;
ВИ – обязательная мера защиты для вторичной идентификации получателей услуг, проводимой по УДИ;
Н – необязательная мера защиты для УДИ;
«–» – мера защиты неприменима для УДИ.

[7] В качестве идентификаторов, обеспечивающих однозначную связь с получателем услуг, могут выступать номер документа, удостоверяющего личность, уникальный идентификатор ЕСИА, номер мобильного телефона, подтвержденный у оператора сотовой связи, и другое.

№	Содержание меры защиты информации	УДИ 1	УДИ 2	УДИ 3
1.6	Служба идентификации должна осуществлять подтверждение номеров мобильных телефонов и адресов электронной почты, предоставленных получателем услуг	ПИ	ПИ	ПИ
1.7	Служба идентификации должна осуществлять идентификацию за единый непрерывный пользовательский сеанс[8] на прикладном уровне модели OSI	О	О	О
1.8	Служба идентификации должна осуществлять идентификацию за единое непрерывное криптографическое соединение	Н	О	О
1.9	Служба идентификации должна контролировать время пользовательских сеансов при прохождении первичной идентификации и в случае превышения предельного периода, определенного поставщиком услуг на основании анализа рисков, направлять получателя услуг на повторную первичную идентификацию	Н	ПИ	ПИ
1.10	Служба идентификации должна реализовывать механизмы, позволяющие прервать процесс идентификации, в случае получения уведомления от получателя услуг или самостоятельного выявления факта компрометации идентификационной информации получателя услуг	О	О	О
1.11	Служба идентификации должна ограничить возможность прохождения первичной идентификации при превышении числа неудачных попыток первичной идентификации, определенного поставщиком услуг на основании анализа рисков, после чего должна проводить первичную идентификацию только при личном присутствии получателя услуг	ПИ	ПИ	ПИ
1.12	Служба идентификации может провести идентификацию по значению другого верифицированного идентификационного атрибута в случае потери получателем услуг идентификатора цифровой идентичности	ВИ	ВИ	–
1.13	Служба идентификации должна заново провести первичную идентификацию получателя услуг в случае потери получателем услуг идентификатора цифровой идентичности	–	–	ВИ
1.14	Служба идентификации должна разрешать обновление идентификационной информации получателя услуг только после аутентификации получателя услуг с УДА, соответствующего УДИ, по которому проводилась первичная идентификация получателя услуг	О	О	О
1.15	Служба идентификации не должна раскрывать факт существования или отсутствия цифровой идентичности, соответствующей идентификатору, при неуспешной попытке вторичной идентификации	О	О	О
1.16	Служба идентификации должна осуществлять передачу сведений об идентификации получателю услуг по результатам успешной первичной идентификации в том же пользовательском сеансе, в котором проводилась первичная идентификация, или с использованием альтернативного канала взаимодействия с получателем услуг	ПИ	ПИ	ПИ
1.17	Служба идентификации должна осуществлять сбор и последующее хранение аутентификационной информации устройства[9], на котором выполняется идентификация	Н	О	О
1.18	Служба идентификации должна позволять устанавливать настройки аудита и сроки хранения журнала событий в соответствии с установленными политиками безопасности, в том числе содержащего записи о создании цифровой идентичности, изменении, блокировке и уничтожении идентификационных данных, фактах попыток прохождения вторичной идентификации, а также инцидентов, произошедших по причине ошибок идентификации	О	О	О

[8] В качестве параметров, обеспечивающих непрерывность пользовательского сеанса, могут выступать идентификаторы сессии, токены доступа, cookie-идентификаторы и другое.

[9] В качестве аутентификационной информации могут выступать, например, сведения, идентифицирующие сертификат или публичный ключ устройства, а в случае отсутствия такой информации необходимо использовать цифровой отпечаток устройства, собранный в соответствии со стандартом Банка России СТО БР БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» [13].

№	Содержание меры защиты информации	УДИ 1	УДИ 2	УДИ 3
2. Состав мер защиты информации, применяемый к каналу взаимодействия между службой идентификации и получателем услуг				
2.1	Служба идентификации должна обеспечивать применение сетевых протоколов, обеспечивающих конфиденциальность и контроль целостности канала взаимодействия, между службой идентификации и получателем услуг	О	О	О
2.2	Служба идентификации должна использовать уникальные ключи сетевого соединения и токены доступа для каждой уникальной сетевой сессии в канале взаимодействия между службой идентификации и получателем услуг	О	О	О
2.3	Служба идентификации должна обеспечить использование технологии двухсторонней аутентификации для канала взаимодействия между службой идентификации и получателем услуг	Н	ЮЛ	ЮЛ
2.4	Служба идентификации должна обеспечивать применение сетевых протоколов, обеспечивающих конфиденциальность и контроль целостности канала взаимодействия, между службой идентификации и верифицирующей стороной	ПИ	ПИ	ПИ
2.5	Служба идентификации и верифицирующая сторона должны обеспечить использование технологии двухсторонней аутентификации в канале взаимодействия между службой идентификации и верифицирующей стороной	ПИ	ПИ	ПИ
3. Состав мер защиты информации, применяемый к протоколу взаимодействия между службой идентификации и получателем услуг				
3.1	Служба идентификации должна осуществлять структурный и логический контроль получаемых сообщений протокола взаимодействия	О	О	О
3.2	Протокол взаимодействия должен предусматривать обязательное направление ответного сообщения на каждый запрос участника взаимодействия	О	О	О
3.3	Протокол взаимодействия должен предусматривать обязательную передачу идентификатора цифровой идентичности получателя услуг	ВИ	ВИ	ВИ
3.4	Протокол взаимодействия должен предусматривать обязательную передачу факта получения согласия получателя услуг на обработку его персональных данных	ПИ	ПИ	ПИ
3.5	Протокол взаимодействия должен обеспечивать возможность передачи перечня верифицирующих сторон, которые использовались при первичной идентификации получателя услуг	ПИ	ПИ	ПИ
3.6	Протокол взаимодействия должен предусматривать обязательную передачу сведений об идентификации	О	О	О
3.7	Протокол взаимодействия должен предусматривать обязательную передачу связывающего запрос и ответ параметра при каждой процедуре идентификации	О	О	О
3.8	Протокол взаимодействия должен обеспечивать возможность передачи аутентификационной информации устройства, на котором выполняется идентификация	Н	О	О
3.9	Протокол взаимодействия должен предусматривать обязательную передачу метки времени при каждой процедуре идентификации с учетом доверительного временного интервала, определенного на основании анализа рисков поставщиком услуг	О	О	О
3.10	Протокол взаимодействия должен необратимо связывать идентификатор канала взаимодействия, который был согласован при установлении защищенного канала, с идентификационной информацией получателя услуг	Н	Н	О
3.11	Протокол взаимодействия должен обеспечивать конфиденциальность идентификационной информации путем ее шифрования	О	О	О
3.12	Протокол взаимодействия должен обеспечивать криптографическую целостность идентификационной информации	О	О	О
3.13	Протокол взаимодействия должен обеспечивать возможность подписания усиленной электронной подписью идентификационной информации	Н	ЮЛ	ЮЛ
3.14	Протокол взаимодействия должен обеспечивать возможность использования российских криптографических алгоритмов, предназначенных для шифрования и подписания	Н	О	О

8. СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ДИСТАНЦИОННОЙ АУТЕНТИФИКАЦИИ

8.1. УРОВНИ ДОВЕРИЯ АУТЕНТИФИКАЦИИ

УДА устанавливаются в рамках процесса аутентификации физических лиц, представителей юридических лиц и программных сервисов.

Для финансовых организаций устанавливается три УДА, определяющих уверенность в результатах аутентификации: низкий (УДА 1), средний (УДА 2) и высокий (УДА 3). В таблице 4 приведены критерии, определяющие соответствующий уровень уверенности в результатах аутентификации, для каждого УДА.

КРИТЕРИИ, ОПРЕДЕЛЯЮЩИЕ СООТВЕТСТВУЮЩИЙ УРОВЕНЬ УВЕРЕННОСТИ В РЕЗУЛЬТАТАХ АУТЕНТИФИКАЦИИ *Табл. 4*

Критерий	**Уровни доверия аутентификации**		
	УДА 1	**УДА 2**	**УДА 3**
Уверенность в результатах аутентификации	Некоторая уверенность	Умеренная уверенность	Значительная уверенность
Протокол аутентификации обеспечивает однофакторную аутентификацию получателя услуг	Да	Нет	Нет
Протокол аутентификации обеспечивает многофакторную аутентификацию получателя услуг	Нет	Да	Да
Протокол аутентификации является криптографическим	Нет	Нет	Да
Протокол аутентификации обеспечивает взаимную аутентификацию поставщика услуг и получателя услуг	Нет	Нет	Да
Каждый предъявленный аутентификатор[10] соответствует аутентификатору, привязанному к цифровой идентичности	Да	Да	Да
Хотя бы один из аутентификаторов является криптографическим средством аутентификации	Нет	Нет	Да
Получателем услуг подтверждены факт обладания и способность распоряжаться аутентификатором	Да	Да	Да

Поставщик услуг должен определять необходимый УДА во внутренних документах для каждой предоставляемой финансовой операции на основании анализа рисков с учетом требований применения УДА к финансовым операциям поставщика услуг, приведенных в таблице 5.

ПРИМЕНЕНИЕ УДА К ФИНАНСОВЫМ ОПЕРАЦИЯМ ПОСТАВЩИКА УСЛУГ *Табл. 5*

Финансовые операции поставщика услуг	**Допустимые УДА**		
	УДА 1	**УДА 2**	**УДА 3**
Предоставление информационных сервисов ФЛ	+	+	+
Предоставление информационных сервисов ЮЛ	+	+	+
Совершение финансовых операций ФЛ, оценка операционного риска которых не превышает установленных во внутренних документах показателей оценки операционного риска	–	+	+

[10] В таблице П-2 приложения 2 к стандарту приведены примеры аутентификаторов в разрезе уровней доверия аутентификации, определенных в данном разделе.

Финансовые операции поставщика услуг	Допустимые УДА		
	УДА 1	УДА 2	УДА 3
Совершение финансовых операций ФЛ, которые законодательно ограничены суммами проведения операции при использовании конкретных средств аутентификации	+	+	+
Совершение финансовых операций ФЛ в течение ограниченного периода, определенного на основании анализа рисков поставщиком услуг, после проведения на устройстве получателя услуг аутентификации по УДА 2 при условии дополнительной аутентификации устройства получателя услуг и экземпляра приложения	+	+	+
Совершение высокорисковых (оценка операционного риска превышает установленные во внутренних документах показатели оценки операционного риска) финансовых операций ФЛ	–	–	+
Совершение регулярных или характерных финансовых операций, оценка операционного риска которых не превышает установленных во внутренних документах показателей оценки операционного риска ЮЛ	–	+	+
Совершение иных или высокорисковых (оценка операционного риска превышает установленные во внутренних документах показатели оценки операционного риска) финансовых операций ЮЛ	–	–	+
Совершение финансовых операций ФЛ и ЮЛ с использованием программных сервисов, оценка операционного риска которых не превышает установленных во внутренних документах показателей оценки операционного риска	–	+	+
Совершение высокорисковых (оценка операционного риска превышает установленные во внутренних документах показатели оценки операционного риска) финансовых операций ФЛ и ЮЛ с использованием программных сервисов	–	–	+

Осуществление финансовой операции при проведении аутентификации в случае несоответствия процесса аутентификации требованиям УДА, установленного для данной финансовой операции, не допускается.

8.2. СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ К ПРОЦЕССУ АУТЕНТИФИКАЦИИ

Состав мер защиты информации, применяемый к процессу аутентификации, приведен в таблице 6[11].

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ К ПРОЦЕССУ АУТЕНТИФИКАЦИИ *Табл. 6*

№	Содержание меры защиты информации	УДА 1	УДА 2	УДА 3
1. Состав мер защиты информации, применяемый к службе аутентификации				
1.1	Служба аутентификации должна требовать предъявления всех необходимых аутентификаторов, определяемых на основании проводимой финансовой операции, УДА и перечня привязанных к учетной записи аутентификаторов	О	О	О
1.2	Служба аутентификации должна осуществлять процедуру аутентификации за единый непрерывный пользовательский сеанс на прикладном уровне модели OSI	О	О	О
1.3	Служба аутентификации должна осуществлять процедуру аутентификации за единое непрерывное криптографическое соединение	ПС	ЮЛ, ПС	О
1.4	Служба аутентификации должна реализовать механизмы, позволяющие прервать процедуру аутентификации или пользовательский сеанс, в случае получения уведомления от получателя услуг или самостоятельного выявления факта компрометации аутентификатора или канала взаимодействия	О	О	О

[11] В таблице 6 используются следующие обозначения обязательности реализации мер защиты:
О – обязательная мера защиты для УДА;
ФЛ – обязательная мера защиты для аутентификации получателей услуг – физических лиц, проводимой по УДА;
ЮЛ – обязательная мера защиты для аутентификации получателей услуг – юридических лиц, проводимой по УДА;
ПС – обязательная мера защиты для аутентификации программных сервисов, проводимой по УДА;
Н – необязательная мера защиты для УДА;
«–» – мера защиты неприменима для УДА.

№	Содержание меры защиты информации	УДА 1	УДА 2	УДА 3
1.5	Служба аутентификации должна устанавливать предельное время пользовательского сеанса, определяемое на основании анализа рисков поставщиком услуг, и в случае его превышения прерывать пользовательский сеанс	О	О	О
1.6	Служба аутентификации должна устанавливать предельное время бездействия получателя услуг в рамках пользовательского сеанса, определяемое на основании анализа рисков поставщиком услуг, и в случае его превышения прерывать пользовательский сеанс	О	О	О
1.7	Служба аутентификации должна инициировать проведение новой процедуры аутентификации получателя услуг в случае завершения или прерывания пользовательского сеанса	О	О	О
1.8	Служба аутентификации должна прервать все пользовательские сеансы, провести идентификацию и аутентификацию получателя услуг с использованием другого аутентификатора, привязанного к цифровой идентичности получателя услуг, в случае потери или компрометации одного из аутентификаторов, привязанных к цифровой идентичности получателя услуг, а также обеспечить отзыв такого аутентификатора и привязку нового аутентификатора, соответствующего УДА отозванного аутентификатора	ФЛ, ЮЛ	ФЛ, ЮЛ	ФЛ, ЮЛ
1.9	Служба аутентификации должна повторно провести первичную идентификацию получателя услуг и осуществить привязку новых аутентификаторов в случае потери или компрометации всех аутентификаторов, привязанных к цифровой идентичности получателя услуг	О	О	О
1.10	Служба аутентификации должна обеспечить временное блокирование возможности прохождения аутентификации при превышении числа неудачных попыток аутентификации, определенного на основании анализа рисков поставщиком услуг	О	О	О
1.11	Служба аутентификации должна требовать предъявления хотя бы одного аутентификатора, требующего конклюдентных действий[12] от получателя услуги	ФЛ, ЮЛ	ФЛ, ЮЛ	ФЛ, ЮЛ
1.12	Служба аутентификации позволяет устанавливать настройки аудита и сроки хранения журнала событий, в том числе содержащего записи об изменении аутентификационных данных, привязке или отзыве аутентификаторов, источниках неудачных попыток аутентификации, а также инцидентах, произошедших по причине ошибок аутентификации	О	О	О
1.13	Служба аутентификации должна вести учет всех аутентификаторов, которые связаны или были связаны с данной цифровой идентичностью на протяжении всего жизненного цикла цифровой идентичности	О	О	О
1.14	Служба аутентификации должна обеспечить защиту программных интерфейсов от воздействия некорректных или намеренно сформированных нестандартных запросов и ответов	О	О	О
1.15	Служба аутентификации должна учитывать несоответствие аутентификационной информации устройства при выборе УДА, по которому должна быть проведена аутентификация	Н	О	О
2. Состав мер защиты информации, применяемый к каналу взаимодействия между службой аутентификации и получателем услуг				
2.1	Служба аутентификации должна обеспечивать применение сетевых протоколов, обеспечивающих защиту подлинности и контроль целостности канала взаимодействия, между службой аутентификации и получателем услуг	О	О	О
2.2	Служба аутентификации должна использовать уникальные ключи сетевого соединения и токены доступа для каждой уникальной сетевой сессии в канале взаимодействия между поставщиком услуг и получателем услуг	О	О	О
2.3	Служба аутентификации должна обеспечить использование технологии двухсторонней аутентификации в канале взаимодействия между службой идентификации и получателем услуг	Н	ЮЛ	О
3. Состав мер защиты информации, применяемый к протоколу взаимодействия между службой аутентификации и получателем услуг				
3.1	Служба аутентификации должна осуществлять структурный и логический контроль получаемых сообщений, предусмотренных протоколом взаимодействия	О	О	О
3.2	Протокол взаимодействия должен предусматривать обязательное направление ответного сообщения на каждый запрос участника взаимодействия	О	О	О
3.3	Протокол взаимодействия должен предусматривать обязательную передачу идентификатора цифровой идентичности получателя услуг при каждой процедуре аутентификации	О	О	О
3.4	Протокол взаимодействия должен обеспечивать возможность передачи аутентификационной информации устройства, на котором выполняется аутентификация	Н	О	О

[12] Действий, которые подтверждают намерение получателя услуг предъявить конкретный аутентификатор, например ввод запоминаемого секрета, предъявление биометрических характеристик, активация внеполосного аутентификатора и другие.

№	Содержание меры защиты информации	УДА 1	УДА 2	УДА 3
3.5	Протокол взаимодействия должен предусматривать обязательную передачу сведений об аутентификации	О	О	О
3.6	Протокол взаимодействия должен предусматривать обязательную передачу связывающего запрос и ответ параметра при каждой процедуре аутентификации	О	О	О
3.7	Протокол взаимодействия должен предусматривать обязательную передачу метки времени при каждой процедуре аутентификации с учетом доверительного интервала метки времени, определенного на основании анализа рисков поставщиком услуг	Н	О	О
3.8	Протокол взаимодействия должен необратимо связывать идентификатор канала взаимодействия, который был согласован при установлении защищенного канала, с аутентификационной информацией получателя услуг	Н	Н	О
3.9	Протокол взаимодействия должен предусматривать возможность передачи счетчика процедур аутентификации, в случае если аутентификатор ведет внутренний счетчик процедур аутентификации	Н	ЮЛ, ПС	О
3.10	Протокол взаимодействия должен предусматривать обязательную передачу параметра в виде однократно используемой последовательности алфавитно-цифровых символов при каждой процедуре аутентификации службе аутентификации	Н	ЮЛ, ПС	О
3.11	Протокол взаимодействия должен обеспечивать конфиденциальность аутентификационной информации путем ее шифрования	О	О	О
3.12	Протокол взаимодействия должен обеспечивать криптографическую целостность аутентификационной информации	О	О	О
3.13	Протокол взаимодействия должен предусматривать возможность подписания усиленной электронной подписью идентификационной и аутентификационной информации	Н	ЮЛ	ЮЛ
3.14	Протокол взаимодействия должен обеспечивать возможность использования российских криптографических алгоритмов, применяемых для шифрования и подписания	Н	О	О
4. Состав мер защиты информации, применяемый к аутентификаторам и процедурам их привязки и отзыва				
4.1	Служба аутентификации должна ознакомить получателя услуг с правилами обращения с аутентификаторами, мерами по обеспечению их безопасности, а также действиями в случае их компрометации или потери	О	О	О
4.2	Служба аутентификации должна поддерживать актуальность состояния аутентификационной информации получателя услуг, в том числе последнего известного состояния аутентификатора	О	О	О
4.3	Служба аутентификации при каждой процедуре аутентификации должна проверять состояние аутентификационной информации получателя услуг и состояние аутентификаторов, в том числе актуальность и срок действия аутентификатора	О	О	О
4.4	Служба аутентификации должна аутентифицировать аппаратные и программные аутентификаторы	Н	ЮЛ	О
4.5	Служба аутентификации должна использовать список разрешенных аутентификаторов или применять иные механизмы фильтрации аутентификаторов	ПС	ЮЛ, ПС	О
4.6	Служба аутентификации должна использовать аутентификаторы, обеспечивающие устойчивость программных и аппаратных интерфейсов (при их наличии) к воздействию некорректных или намеренно сформированных нестандартных запросов и ответов	О	О	О
4.7	Служба аутентификации должна обеспечить возможность привязки аутентификаторов к цифровой идентичности получателя услуг только в рамках пользовательского сеанса, в котором была проведена либо первичная идентификация, либо аутентификация по УДА не ниже УДА привязываемого аутентификатора	ФЛ, ЮЛ	ФЛ, ЮЛ	ФЛ, ЮЛ
4.8	Служба аутентификации должна обеспечить возможность привязки аутентификаторов к цифровой идентичности получателя услуг только в рамках пользовательского сеанса, в котором была проведена либо первичная идентификация, либо аутентификация по УДА не ниже УДА привязываемого аутентификатора	Н	ФЛ, ЮЛ	ФЛ, ЮЛ
4.9	Служба аутентификации должна уведомлять получателя услуг о привязке к его цифровой идентичности новых аутентификаторов	ФЛ, ЮЛ	ФЛ, ЮЛ	ФЛ, ЮЛ
4.10	Служба аутентификации должна осуществлять проверки безопасности среды, в которой осуществляются привязка или предъявление аутентификатора (например, проверка наличия вредоносных программ, контроль обновлений программного обеспечения и другое)	О	О	О

8.3. СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ К ПРОЦЕССУ АУТЕНТИФИКАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОТДЕЛЬНЫХ АУТЕНТИФИКАТОРОВ

В таблице 7 приведен состав мер, применяемый в случаях использования в процессе аутентификации отдельных аутентификаторов, приведенных в приложении 2 к стандарту.

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ К ПРОЦЕССУ АУТЕНТИФИКАЦИИ ПРИ ПРИМЕНЕНИИ ОТДЕЛЬНЫХ АУТЕНТИФИКАТОРОВ *Табл. 7*

№	Содержание меры защиты информации	УДА 1	УДА 2	УДА 3
1. Меры защиты информации при использовании аутентификаторов, основанных на факторе знания: запоминаемый секрет (например, ПИН-код, пароль)				
1.1	Служба аутентификации должна позволять устанавливать критерии сложности (длина, размер алфавита, обязательность различных типов символов и так далее) запоминаемого секрета, которые должны определяться на основании анализа рисков поставщиком услуг, осуществлять проверку на сложность запоминаемого секрета в соответствии с установленными критериями сложности, а также информировать получателя услуг об уровне сложности выбранного им запоминаемого секрета	0	0	0
1.2	Служба аутентификации должна скрывать вводимые символы запоминаемого секрета	0	0	0
1.3	Служба аутентификации должна осуществлять контроль смены запоминаемого секрета, сгенерированного службой аутентификации при первичной идентификации получателя услуг или после истечения его срока действия, определяемого на основании анализа рисков поставщиком услуг	0	0	0
1.4	Служба аутентификации должна ограничивать максимальное количество неудачных попыток аутентификации с использованием запоминаемого секрета, которое определяется на основании анализа рисков поставщиком услуг	0	0	0
1.5	Служба аутентификации должна применять механизм CAPTCHA (или аналогичные меры защиты от перебора) после установленного количества неудачных попыток аутентификации, определенного на основании анализа рисков поставщиком услуг	0	0	0
1.6	Служба аутентификации должна требовать изменения запоминаемого секрета при получении информации о его компрометации, в том числе из открытых источников информации	0	0	0
1.7	Служба аутентификации должна обеспечить невозможность повторного использования запоминаемых секретов получателя услуг, количество неповторяемых запоминаемых секретов определяется на основании анализа рисков поставщиком услуг	0	0	0
1.8	Служба аутентификации должна хранить запоминаемые секреты в форме, которая является стойкой к офлайн-атакам на запоминаемый секрет	0	0	0
2. Меры защиты информации при использовании аутентификаторов, основанных на аутентификации по отдельному каналу связи: внеполосный аутентификатор (физическое устройство, которое имеет однозначную адресацию и может безопасно связываться со службой аутентификации по отдельному каналу связи)				
2.1	Служба аутентификации должна аутентифицировать внеполосный аутентификатор с помощью либо случайно сгенерированного зашитого ключа, либо сим-карты (IMSI)	0	0	0
2.2	Внеполосный аутентификатор должен иметь однозначную адресацию по каждому каналу взаимодействия со службой аутентификации	0	0	0
2.3	Внеполосный аутентификатор должен обеспечивать возможность подтверждения факта владения внеполосным аутентификатором	0	0	0
2.4	Служба аутентификации должна ограничивать период ответа на запрос аутентификации на внеполосный аутентификатор, определяемый на основании анализа рисков поставщиком услуг	0	0	0
2.5	Служба аутентификации должна ограничивать количество использований внеполосного аутентификатора в период времени, определяемый на основании анализа рисков поставщиком услуг	0	0	0
2.6	Служба аутентификации при аутентификации внеполосного аутентификатора должна осуществлять дополнительные проверки на несоответствие параметров внеполосного аутентификатора или повторного воспроизведения внеполосного аутентификатора	0	0	0

№	Содержание меры защиты информации	УДА 1	УДА 2	УДА 3
3. Меры защиты информации при использовании аутентификаторов, основанных на биометрических характеристиках человека[13]				
3.1	Служба аутентификации в случае использования изображения лица человека или записи голоса человека должна обеспечивать соответствие биометрических образцов требованиям приказа Минцифры России от 12.05.2023 № 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц» [14], для иных модальностей необходимо применять критерии качества, установленные российскими и международными стандартами и практиками	0	0	0
3.2	Служба аутентификации должна обеспечить вероятность ложного или ложноположительного результата аутентификации с использованием биометрических характеристик на уровне, не превышающем установленные законодательством показатели, а в случае отсутствия таких показателей на уровне, установленном российскими и международными стандартами и практиками	0	0	0
3.3	Служба аутентификации должна использовать методы обнаружения атак на биометрическое предъявление в процессе биометрического предъявления и сбора соответствующих биометрических параметров в соответствии со стандартами ГОСТ Р 58624[14]	0	0	0
3.4	Служба аутентификации должна обеспечивать защиту от несанкционированного доступа хранилища биометрических образцов[15] и векторов биометрических параметров	0	0	0
3.5	Служба аутентификации должна обеспечивать защиту каналов взаимодействия между внутренними датчиками, системой извлечения признаков (биометрических векторов) и прикладным программным обеспечением	0	0	0
4. Меры защиты информации при использовании аутентификаторов, основанных на генерации одноразового пароля: • поисковый секрет (физическая или электронная запись, в которой хранится набор одноразовых паролей); • средство аутентификации, реализующее передачу одноразового пароля через альтернативный канал; • однофакторный генератор одноразовых паролей, основанный на криптографических методах; • многофакторный генератор одноразовых паролей, основанный на криптографических методах				
4.1	Служба аутентификации должна использовать надежный генератор случайных чисел, соответствующий требованиям безопасности, определяемым на основании анализа рисков поставщиком услуг, для генерации одноразового пароля	0	–	–
4.2	Служба аутентификации должна использовать генератор случайных чисел, прошедший процедуру оценки соответствия требованиям[16], установленным федеральным органом исполнительной власти в области обеспечения безопасности, для генерации одноразового пароля	–	0	0
4.3	Служба аутентификации должна обеспечивать использование технологии, обеспечивающей невозможность раскрытия одноразового пароля третьим лицам при его передаче	0	0	0
4.4	Служба аутентификации должна использовать одноразовые пароли с учетом сложности (длина, размер алфавита, обязательность различных типов символов и так далее), которая должна определяться на основании анализа рисков поставщиком услуг	0	0	0

[13] Исходя из российской и международной практики использование биометрических характеристик человека в качестве единственного фактора аутентификации при проведении финансовых операций не допускается. Настоящий стандарт допускает использование биометрических характеристик человека в качестве единственного фактора аутентификации только в случаях проведения финансовых операций, в которых для данного аутентификатора законодательно ограничены суммы проведения операции.

[14] ГОСТ Р 58624.1-2019 «Национальный стандарт Российской Федерации. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура» [15], ГОСТ Р 58624.2-2019 «Национальный стандарт Российской Федерации. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных» [16], ГОСТ Р 58624.3-2019 «Национальный стандарт Российской Федерации. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний» [17].

[15] Биометрические образцы, хранимые для рассмотрения обращений субъектов персональных данных, предполагающих неправомерную обработку их биометрических персональных данных при проведении аутентификации и (или) оспаривающих результаты проведения аутентификации, в течение не более десяти суток с момента предоставления таких данных.

[16] Р 1323565.1.012-2017.

№	Содержание меры защиты информации	УДА 1	УДА 2	УДА 3
4.5	Одноразовый пароль должен иметь ограниченный период действия, определяемый на основании анализа рисков поставщиком услуг	О	О	О
4.6	Служба аутентификации должна ограничивать количество запросов одноразового пароля за период, определяемый на основании анализа рисков поставщиком услуг	О	О	О
4.7	Служба аутентификации должна хранить одноразовые пароли в форме, которая является устойчивой к офлайн-атакам	О	О	О
4.8	Служба аутентификации должна передавать одноразовый пароль только на устройства, имеющие однозначную адресацию по каждому каналу взаимодействия со службой аутентификации	О	О	О
4.9	Служба аутентификации должна передавать одноразовый пароль только на устройства, которые были аутентифицированы службой аутентификации	Н	О	О
4.10	Служба аутентификации должна передавать одноразовый пароль только на устройства, которые были верифицированы службой идентификации при первичной идентификации	Н	Н	О
4.11	В случае использования программного датчика случайных чисел служба аутентификации должна обеспечить защиту инициализирующей последовательности такого генератора случайных чисел от атак на повторное воспроизведение	Н	О	О
5. Меры защиты информации при использовании криптографических программных аутентификаторов: • однофакторное криптографическое программное средство аутентификации или софт-токен; • многофакторное криптографическое программное средство аутентификации				
5.1	Криптографический ключ должен храниться в безопасном хранилище, доступном только для приложения криптографического программного средства аутентификации	О	О	О
5.2	Криптографический ключ криптографического программного средства аутентификации должен иметь ограниченный период действия, определяемый на основании анализа рисков поставщиком услуг	О	О	О
5.3	Служба аутентификации должна обеспечивать формирование аутентификационной информации с использованием генератора случайных чисел, соответствующего требованиям безопасности, определяемым на основании анализа рисков поставщиком услуг, для генерации одноразового пароля	О	ФЛ	–
5.4	Служба аутентификации должна обеспечивать формирование аутентификационной информации с использованием генератора случайных чисел, прошедшего процедуру оценки соответствия требованиям[17], установленным федеральным органом исполнительной власти в области обеспечения безопасности, для генерации одноразового пароля	–	ЮЛ	О
6. Меры защиты информации при использовании криптографических технических аутентификаторов: • однофакторное криптографическое техническое средство аутентификации; • многофакторное криптографическое техническое средство аутентификации; • многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом				
6.1	Служба аутентификации должна обеспечивать ведение реестра и фильтрацию по указанному реестру криптографических технических аутентификаторов	О	О	О
6.2	Криптографический ключ криптографического технического аутентификатора должен иметь ограниченный период действия, определяемый на основании анализа рисков поставщиком услуг	О	О	О
6.3	Криптографический ключ должен храниться в безопасном хранилище криптографического технического средства аутентификации	О	О	О
6.4	Служба аутентификации должна обеспечивать формирование аутентификационной информации с использованием генератора случайных чисел, прошедшего процедуру оценки соответствия требованиям[17], установленным федеральным органом исполнительной власти в области обеспечения безопасности, для генерации одноразового пароля	Н	ЮЛ	О

[17] Р 1323565.1.012-2017.

9. СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ ПРИ ДЕЛЕГИРОВАНИИ ДИСТАНЦИОННЫХ ИДЕНТИФИКАЦИИ И (ИЛИ) АУТЕНТИФИКАЦИИ

В случаях когда поставщик услуг делегирует проведение идентификации и (или) аутентификации ДТС, он должен руководствоваться следующими подходами для минимизации риска использования сторонних поставщиков услуг:

- поставщик услуг несет ответственность за управление рисками делегирования идентификации и (или) аутентификации ДТС;
- поставщик услуг должен включить в систему управления рисками сторонних поставщиков услуг риски делегирования проведения идентификации и (или) аутентификации, в том числе в части политики и процессов по выявлению и снижению рисков, управлению ими, мониторингу и отчетности о данных рисках;
- поставщик услуг должен проводить оценку рисков делегирования проведения идентификации и (или) аутентификации до заключения договора, а также периодически проводить оценку рисков после заключения договора;
- поставщик услуг должен получить от ДТС подтверждение наличия действующей лицензии на осуществление лицензируемой деятельности, в случаях если это предусмотрено законодательством Российской Федерации или нормативными актами Банка России;
- поставщик услуг должен определить в договоре с ДТС перечень финансовых операций и соответствующие им УДИ и (или) УДА, которые будут использоваться при делегировании идентификации и (или) аутентификации;
- поставщик услуг должен получить от ДТС документированное подтверждение соответствия составу мер, приведенных в таблицах 3 и (или) 6, 7, для наиболее высокого утвержденного УДИ и (или) УДА или компенсирующим мерам, а также требованиям ГОСТ Р 57580.1-2017, в случаях если это предусмотрено законодательством Российской Федерации или нормативными актами Банка России;
- поставщик услуг совместно с ДТС должен обеспечить реализацию мер, приведенных в таблице 8;
- поставщик услуг должен определить в договоре с ДТС зоны ответственности между поставщиком услуг и ДТС для случаев непреднамеренных ошибок или инцидентов защиты информации при проведении идентификации и (или) аутентификации;
- поставщик услуг должен определить в договоре с ДТС порядок информирования о выявленных инцидентах защиты информации при проведении идентификации и (или) аутентификации и реагирования на них.

Состав мер защиты информации, применяемый при делегировании идентификации и (или) аутентификации, приведен в таблице 8.

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЙ ПРИ ДЕЛЕГИРОВАНИИ ИДЕНТИФИКАЦИИ И (ИЛИ) АУТЕНТИФИКАЦИИ *Табл. 8*

№	Содержание меры защиты информации
1	Поставщик услуг должен предоставить получателю услуг информацию о намерении проведения идентификации и (или) аутентификации с использованием сервиса ДТС до перенаправления на ресурсы ДТС, после чего получатель услуги должен подтвердить намерение пройти идентификацию и (или) аутентификацию с использованием сервиса ДТС
2	Поставщик услуг при переадресации на сервис ДТС должен передавать необходимые УДИ и (или) УДА, по которым должна проводиться идентификация и (или) аутентификация получателя услуг, если договором предусмотрено проведение идентификации и (или) аутентификации по различным УДИ и (или) УДА
3	Перенаправление на сторонний ресурс (ресурсы поставщика услуг или ДТС) должно осуществляться защищенным образом в соответствии с российскими и международными стандартами и практиками
4	Поставщик услуг должен вести закрытый перечень адресов ресурсов ДТС, на которые осуществляется перенаправление, и обеспечивать перенаправление только на ресурсы из данного перечня

№	Содержание меры защиты информации
5	Канал взаимодействия между поставщиком услуг и ДТС должен обеспечивать криптографическую защиту сетевого взаимодействия и взаимную аутентификацию сторон
6	Поставщик услуг и ДТС при передаче идентификационной и (или) аутентификационной информации, а также сведений об идентификации и (или) аутентификации должны обеспечить целостность и достоверность передаваемой информации
7	Поставщик услуг и ДТС должны обмениваться состоянием идентификационной и (или) аутентификационной информации получателя услуг с периодичностью, определенной на основании анализа рисков поставщиком услуг и предусмотренной договором между поставщиком услуг и ДТС
8	Поставщик услуг должен установить в договоре с ДТС минимальный и достаточный состав идентификационной информации, предоставляемой получателем услуг в процессе первичной идентификации
9	При делегировании идентификации поставщик услуг должен обеспечить получение от ДТС факта получения согласия на обработку персональных данных получателя услуг, содержащее согласие на передачу персональных данных поставщику услуг
10	Поставщик услуг при переадресации на сервис ДТС может передавать наименование верифицирующей стороны (перечень верифицирующих сторон), с использованием которых должна проводиться верификация получателя услуг
11	Поставщик услуг должен обеспечить получение от ДТС журналов событий идентификации, в том числе содержащих записи о создании цифровой идентичности, изменении, блокировке и уничтожении идентификационных данных, фактах попыток прохождения вторичной идентификации, а также инцидентов, произошедших по причине ошибок идентификации или нарушения пользовательского сеанса
12	Поставщик услуг при переадресации на сервис ДТС может передавать необходимый тип (список типов) или наименование аутентификатора, по которому должна проводиться аутентификация получателя услуг
13	Поставщик услуг должен обеспечить получение от ДТС журналов событий аутентификации, в том числе содержащих записи об изменении аутентификационной информации, привязке или отзыве аутентификаторов, источниках неудачных попыток аутентификации, а также инцидентах, произошедших по причине ошибок аутентификации или нарушения пользовательского сеанса

10. ИСПОЛЬЗОВАНИЕ СТАНДАРТА ДЛЯ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ К ПОДПРОЦЕССУ «ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ, АВТОРИЗАЦИЯ (РАЗГРАНИЧЕНИЕ ДОСТУПА) ПРИ ОСУЩЕСТВЛЕНИИ ЛОГИЧЕСКОГО ДОСТУПА» ГОСТ Р 57580.1-2017

Положения настоящего стандарта могут применяться в сценариях, отличных от предоставления финансовых продуктов и услуг клиентам финансовой организации. Одним из альтернативных сценариев применения может выступать реализация требований ГОСТ Р 57580.1-2017 к подпроцессу «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»:

- при проведении идентификации и (или) аутентификации работников или программных сервисов финансовой организации с целью предоставления финансовых услуг из-за пределов вычислительных сетей финансовой организации;
- при проведении идентификации и (или) аутентификации работников, эксплуатационного персонала или программных сервисов финансовой организации при осуществлении логического доступа к инфраструктуре финансовой организации из-за пределов вычислительных сетей финансовой организации;
- при проведении идентификации и (или) аутентификации представителей аутсорсинговых организаций при осуществлении логического доступа к инфраструктуре финансовой организации из-за пределов вычислительных сетей финансовой организации;
- при проведении идентификации и (или) аутентификации работников, эксплуатационного персонала или программных сервисов при осуществлении логического доступа к совместно используемым физическим или виртуальным (облачным) ресурсам;
- при проведении идентификации и (или) аутентификации в рамках других сценариев, определяемых организациями.

Выбор уровня доверия осуществляется организациями самостоятельно в рамках системы управления рисками исходя из критичности операции. В таблице 9 приведены рекомендованные критерии применения УДИ и УДА к указанным сценариям.

ПРИМЕНЕНИЕ УДИ И УДА К СЦЕНАРИЯМ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ РАБОТНИКОВ ФИНАНСОВОЙ ОРГАНИЗАЦИИ, ЭКСПЛУАТАЦИОННОГО ПЕРСОНАЛА И ПРЕДСТАВИТЕЛЕЙ АУТСОРСИНГОВЫХ ОРГАНИЗАЦИЙ *Табл. 9*

Субъекты доступа	**Осуществление логического доступа**	
	к некритичным процессам	**к критичным процессам**
Работники финансовой организации	УДИ 1, УДА 1	УДИ 2, УДА 2
Эксплуатационный персонал	УДИ 2, УДА 2	УДИ 3, УДА 3
Представители аутсорсинговых организаций	УДИ 2, УДА 2	УДИ 3, УДА 3
Программные сервисы	УДА 2	УДА 2

Состав мер защиты информации, применяемый к процессам идентификации и аутентификации, к указанным УДИ и УДА, приведен в разделах 7 и 8 настоящего стандарта. Организации самостоятельно принимают решение о необходимости реализации той или иной меры на основе результатов анализа рисков для конкретного процесса, к которому предоставляется доступ.

БИБЛИОГРАФИЯ

1. Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».
2. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
5. Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».
6. Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».
7. Положение Банка России от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», документ утрачивает силу с 1 апреля 2024 года в связи с изданием Положения Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».
8. Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».
9. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
10. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
11. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
13. БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств».
14. Приказ Минцифры России от 12.05.2023 № 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц».

15. ГОСТ Р 58624.1-2019 «Национальный стандарт Российской Федерации. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура».
16. ГОСТ Р 58624.2-2019 «Национальный стандарт Российской Федерации. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных».
17. ГОСТ Р 58624.3-2019 «Национальный стандарт Российской Федерации. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний».

ПРИЛОЖЕНИЕ 1 (ОБЯЗАТЕЛЬНОЕ)

ПРИМЕРЫ РЕАЛИЗАЦИЙ ПРОЦЕССА ВЕРИФИКАЦИИ В РАЗРЕЗЕ УРОВНЕЙ ДОВЕРИЯ ИДЕНТИФИКАЦИИ

Данное приложение содержит примеры реализации процесса верификации в разрезе уровней доверия идентификации, определенных в разделе 7. Приведенный перечень примеров не является исчерпывающим, поставщики услуг могут реализовывать иные процессы верификации в рамках процесса идентификации. При этом возможность применения иных процессов верификации в рамках выбранного УДИ должна определяться исходя из разработанной модели угроз безопасности информации и установленных показателей оценки операционного риска, а также устанавливаться во внутренних документах финансовой организации.

ПРИМЕРЫ РЕАЛИЗАЦИЙ ПРОЦЕССА ВЕРИФИКАЦИИ В РАЗРЕЗЕ УРОВНЕЙ ДОВЕРИЯ ИДЕНТИФИКАЦИИ *Табл. П-1*

Реализация процесса верификации	УДИ 1	УДИ 2	УДИ 3
Подтверждение сведений о получателе услуг через оператора сотовой связи с использованием номера мобильного телефона	+	–	–
Подтверждение сведений о получателе услуг путем проверки документа, удостоверяющего личность, с использованием видео-конференц-связи	+	–	–
Подтверждение сведений о получателе услуг путем самостоятельной проверки полученных сведений поставщиком услуг	+	–	–
Подтверждение сведений о получателе услуг с использованием неподтвержденной учетной записи ЕСИА	+	–	–
Подтверждение сведений о получателе услуг с использованием действующего квалифицированного сертификата электронной подписи	+	+	–
Подтверждение сведений о получателе услуг с использованием подтвержденной учетной записи ЕСИА с установленной двухфакторной аутентификацией	+	+	+
Подтверждение сведений о получателе услуг с использованием информационных систем органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования или иных государственных информационных систем, определенных Правительством Российской Федерации	+	+	+
Подтверждение сведений о получателе услуг с использованием удостоверения личности, содержащего электронный носитель информации с записанными на нем персональными данными владельца паспорта	+	+	+
Подтверждение сведений о получателе услуг с использованием государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»	+	+	+

Предложения в рамках компетенций отсутствуют.

ПРИЛОЖЕНИЕ 2
(ОБЯЗАТЕЛЬНОЕ)

ПРИМЕРЫ АУТЕНТИФИКАТОРОВ В РАЗРЕЗЕ УРОВНЕЙ ДОВЕРИЯ АУТЕНТИФИКАЦИИ

Данное приложение содержит примеры аутентификаторов в разрезе уровней доверия аутентификации, определенных в разделе 8. Приведенный перечень примеров аутентификаторов не является исчерпывающим, поставщики услуг могут использовать иные аутентификаторы в рамках процесса аутентификации. При этом возможность применения иных аутентификаторов в рамках выбранного УДА должна определяться исходя из разработанной модели угроз безопасности информации и установленных показателей оценки операционного риска, а также устанавливаться во внутренних документах финансовой организации.

ПРИМЕРЫ АУТЕНТИФИКАТОРОВ В РАЗРЕЗЕ УРОВНЕЙ ДОВЕРИЯ АУТЕНТИФИКАЦИИ *Табл. П-2*

Аутентификаторы	УДА 1	УДА 2	УДА 3
Запоминаемый секрет (например, ПИН-код, пароль)	+	–	–
Поисковый секрет (физическая или электронная запись, в которой хранится набор одноразовых паролей)	+	–	–
Внеполосный аутентификатор (физическое устройство, которое имеет однозначную адресацию и может безопасно связываться со службой аутентификации по отдельному каналу связи)	+	–	–
Биометрические характеристики человека	+	–	–
Средство аутентификации, реализующее передачу одноразового пароля через альтернативный канал	+	–	–
Однофакторный генератор одноразовых паролей, основанный на криптографических методах	+	–	–
Однофакторное криптографическое техническое средство аутентификации	+	–	–
Однофакторное криптографическое программное средство аутентификации или софт-токен (при наличии дополнительной аутентификации на устройстве для доступа к криптографическому программному средству аутентификации или софт-токену)	+	+	–
Комбинация средств аутентификации (не менее двух аутентификаторов), разных по факторам	+	+	–
Многофакторный генератор одноразовых паролей, основанный на криптографических методах	+	+	+
Многофакторное криптографическое программное средство аутентификации	+	+	+
Многофакторное криптографическое техническое средство аутентификации	+	+	+
Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом	+	+	+
Комбинации средств аутентификации (не менее двух), одно из которых является криптографическим, а второе отличается от первого по фактору аутентификации	+	+	+