Автономная некоммерческая образовательная организация
высшего образования
«Воронежский экономико-правовой институт»
(АНОО ВО «ВЭПИ»)

АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ

Подписано цифровой подписью: АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ
Дата: 2024.05.17 10:17:30 +03'00'

УТВЕРЖДЕН
Приказом АНОО ВО «ВЭПИ»
от 17.05.2024 № 02-02.17.05.24.02
Ректор С.Л. Иголкин

РЕГЛАМЕНТ
применения электронной подписи
в АНОО ВО «Воронежский экономико-правовой институт» и филиалах

1. Общие положения

1.1. Регламент применения электронной подписи в АНОО ВО «Воронежский экономико-правовой институт» и филиалах (далее – Регламент) разработан в соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

1.2. Регламент определяет порядок использования электронной подписи (далее – ЭП) при работе с электронными документами в информационных системах АНОО ВО «Воронежский экономико-правовой институт» и филиалах (далее – Институт) и при взаимодействии с внешними информационными системами. А также содержит порядок использования ЭП в Институте и определяет обязанности, права и ответственность участников электронного документооборота.

1.3. Настоящий Регламент является обязательным для исполнения всеми участниками электронного взаимодействия, обеспеченными ЭП в Институте.

1.4. Действие настоящего Регламента не распространяется на организацию работы с документами, содержащими сведения, отнесенные к государственной тайне.

2. Термины, определения и сокращения

2.1. Основные термины и определения, применяемые в настоящем Регламенте:

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Простая электронная подпись (далее – ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным

лицом. ПЭП представляет собой уникальную комбинацию логина и пароля, известную только участнику электронного взаимодействия и однозначным образом сопоставленная с учетной записью пользователя домена Института (Active Directory). ПЭП используется участником электронного взаимодействия для подписания электронных документов.

Неквалифицированная электронная подпись (далее – НЭП) – это электронная подпись, которая:

1. Получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2. Позволяет определить лицо, подписавшее электронный документ;

3. Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4. Создается с использованием средств электронной подписи.

Выдается отделом информационных технологий Института. Применяется в рамках организации внутреннего документооборота Института. НЭП также может быть получена через приложение «Госключ» или сервис электронного документооборота Контур Сайн.

Квалифицированная электронная подпись (далее – КЭП) – электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1. Ключ проверки электронной подписи указан в квалифицированном сертификате;

2. Для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

КЭП подтверждена сертификатом, выданным аккредитованным удостоверяющим центром Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Может применяться как во внутренних, так и внешних информационных системах.

Владелец ЭП – участник электронного взаимодействия, которому в установленном порядке выдана ЭП.

Ключ проверки НЭП или КЭП – уникальная последовательность символов, однозначно связанная с ключом НЭП или КЭП, и предназначенная для проверки подлинности НЭП или КЭП. Является общедоступным.

Ключ НЭП и КЭП – уникальная последовательность символов, предназначенная для создания НЭП или КЭП.

Ключевой носитель – отчуждаемый носитель, содержащий один или несколько ключей ЭП (НЭП или КЭП).

Госключ – мобильное приложение, разработанное Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, предназначенное для подписания документов в электронном виде.

Контур Сайн – это сервис электронного документооборота между юридическими и физическими лицами, а также самозанятыми.

Отдел информационных технологий (далее – ОИТ) – структурное подразделение Института, наделенное функциями удостоверяющего центра.

Работник отдела информационных технологий – ответственное лицо за защиту информации и обеспечение безопасности всех форм и средств обработки информации.

Сертификат ключа проверки НЭП или КЭП – электронный документ или документ на бумажном носителе, выданный ОИТ.

Средства НЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание НЭП, проверка НЭП, создание ключа НЭП и ключа проверки НЭП в СЭД.

Участники электронного взаимодействия – работники, обучающиеся, абитуриенты Института и/или их представители, заказчики платных образовательных услуг и/или их представители, осуществляющие обмен информацией в информационных системах Института.

Обучающийся – к обучающимся в Институте относятся студенты, аспиранты, слушатели и другие категории лиц в соответствии с законодательством Российской Федерации.

Электронный документ – документированная информация, представленная в электронной форме.

Копия электронного документа на бумажном носителе (бумажная копия электронного документа) – документ на бумажном носителе, полученный посредством распечатки электронного документа с указанием реквизитов электронной подписи и заверенный лицом, обладающим полномочиями на заверение электронных документов.

Корпоративные информационные системы – масштабируемый комплекс программных и технических средств, предназначенный для автоматизации бизнес-процессов Института.

Лицо, присоединяющееся к ЭДО – работник, обучающийся, абитуриент, либо физическое лицо, находящееся с Институтом в договорных отношениях, присоединяющееся к электронному документообороту на условиях настоящего Регламента.

Информационные системы Института – системы, которые автоматизируют все бизнес-процессы всего Института или их значительную часть, достигая полной информационной согласованности и прозрачности, а также предназначена для хранения, поиска и обработки информации.

Сторонняя информационная система – это информационная система, не находящаяся в ведении Института на праве собственности, аренды и пр., в которой реализован механизм подписания и/или проверки электронных документов электронной подписью.

Виды сторонних информационных систем:

1. Государственные информационные системы, реализовавшие механизм электронной подписи, например, «Госключ» и другие;
2. Негосударственные информационные системы, например, «Контур Сайн» и другие;

Смешанное подписание документа – это подписание двумя и более лицами одного документа различными (рукописными и электронными подписями) способами.

2.2. Создание и приостановка действия НЭП осуществляется путём применения программного комплекса «Центр сертификации Microsoft Windows 2008 R2 Standard» или его аналогов.

2.3. Обеспечение использования КЭП в информационных системах осуществляется путём применения программного комплекса «КриптоПРО CSP» или его аналогов.

3. Порядок использования ЭП

3.1. Выполнение операций криптозащиты обеспечивается путём применения ключей НЭП, КЭП и ПЭП, которые являются известными только работнику Института, обладающему правом использования НЭП, КЭП и ПЭП в информационных системах, и ключа проверки НЭП, КЭП и ПЭП.

3.2. Для авторизации и работы в информационных системах участник электронного взаимодействия использует определенный вид ЭП. Вид ЭП, применяемых в информационных системах, определяется в соответствии нормативно-правовыми актами Российской Федерации и локально-правовыми актами Института.

3.3. Информация в электронной форме, подписанная ЭП, в том числе простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом равнозначным документу на бумажном носителе, подписанному собственноручной подписью в случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», кроме случаев, когда допускается исключительно бумажный документооборот.

3.4. При изготовлении экземпляра электронного документа, подписанного электронной подписью, на бумажном носителе, в графе «подпись» со стороны Института может быть сформирован скан-образ подписи подписанта, сертификату ключа проверки НЭП или КЭП, при подписании ПЭП на документе указывается следующая информация:

ПОДПИСАНО ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
В СООТВЕТСТВИИ С СОГЛАШЕНИЕМ ОБ ЭЛЕКТРОННОМ ВЗАИМОДЕЙСТВИИ

Дата, время подписи — ФИО участника электронного Взаимодействия

3.5. При наличии у лиц, присоединяющихся к ЭДО, технической возможности на подписание электронного документа, данный способ подписания признается приоритетным, но притом лица, присоединившиеся к ЭДО, признают, что допускают при электронном взаимодействии смешанный формат подписания документов, то есть подписание двумя и

более лицами одного документа различными (рукописными и электронными подписями) способами.

4. Основные функции отдела информационных технологий Института по работе ЭП

4.1. ОИТ осуществляет деятельность по обеспечению использования ЭП в информационных системах. Для обеспечения использования ЭП ОИТ выполняет следующие функции:

4.1.1. Создание по обращению работников Института (далее – заявители) ключей НЭП и ключей проверки НЭП;

4.1.2. ПЭП создается автоматически при получении информации об участнике электронного взаимодействия;

4.1.3. Запись на ключевые носители сгенерированной пары ключей НЭП;

4.1.4. Установка сроков действия сертификатов ключей проверки НЭП;

4.1.5. Приостановление и возобновление действия сертификатов ключей проверки НЭП;

4.1.6. Аннулирование выданных ОИТ сертификатов;

4.1.7. Приостановление и возобновление действия ПЭП;

4.1.8. Сопровождение и оформление документов при приобретении КЭП в аккредитованных удостоверяющих центрах;

4.1.9. Осуществление контроля за своевременным перевыпуском или приобретением новых КЭП и НЭП работникам, которым данные электронные подписи необходимы в соответствии с должностными обязанностями;

4.1.10. Ведение реестров выданных и аннулированных сертификатов ключей НЭП и КЭП (далее — реестр сертификатов) и обеспечение доступа лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием сети «Интернет»;

4.1.11. Осуществление по обращению участников электронного взаимодействия проверки НЭП и КЭП;

4.1.12. Осуществление иной деятельности, связанной с использованием ЭП.

5. Обязанности, права и ответственность участников электронного взаимодействия в информационных системах

5.1. При использовании ЭП участники электронного взаимодействия обязаны:

5.1.1. Обеспечивать конфиденциальность ЭП;

5.1.2. При работе с электронными документами, используя средства информационной системы, проверять подлинность ЭП участников электронного взаимодействия в целях исключения возможности фальсификации электронного документа;

5.1.3. Немедленно уведомлять ОИТ и иных участников электронного взаимодействия о нарушении конфиденциальности ключа и не использовать ключ ЭП в случае сомнения в его конфиденциальности.

5.2. Участник электронного взаимодействия имеет право:

5.2.1. Применять ЭП, владельцем которой он является, для формирования ЭП для электронных документов;

5.2.2. Получать актуальный список аннулированных и приостановленных сертификатов ключа проверки НЭП или КЭП, соответствующих его ключу НЭП или КЭП;

5.2.3. Обращаться в ОИТ за подтверждением подлинности НЭП или КЭП в электронных документах, подписанных другими участниками электронного взаимодействия;

5.2.4. Подавать заявления об аннулировании, приостановлении или возобновлении действия ПЭП, сертификатов ключей проверки НЭП или КЭП.

5.3. Участники электронного взаимодействия несут ответственность за неправомерное использование ЭП в соответствии с законодательством Российской Федерации.

6. Порядок предоставления и прекращения действия ЭП

6.1. Предоставление ЭП:

6.1.1. Создание и выдача пользователям НЭП и КЭП осуществляется по обращениям работников (Приложение № 1 к Регламенту). Заявка на создание и выдачу ЭП подаётся заявителем своему непосредственному руководителю;

6.1.2. Руководитель структурного подразделения Института рассматривает и направляет заявку в ОИТ для начала работ по созданию/приобретению НЭП или КЭП, а также при необходимости установки на персональный компьютер заявителя специализированного программного обеспечения;

6.1.3. ОИТ оформляет документы для получения ключа КЭП, консультирует о порядке получения КЭП в аккредитованном удостоверяющем центре, а также при необходимости осуществляет запись ключа КЭП на носитель или на мобильное устройство заявителя;

6.1.4. ОИТ формирует сертификат проверки ключа НЭП и ключ НЭП, осуществляет запись ключа НЭП на носитель или на мобильное устройство заявителя, осуществляет регистрацию сертификата ключа проверки НЭП в необходимых информационных системах, а также осуществляет регистрацию пользователя ЭП в реестре удостоверяющего центра и выдает ключ НЭП заявителю;

6.1.5. Информация о созданном ключе НЭП и сертификате ключа проверки НЭП должна быть внесена в реестр ОИТ не позднее даты начала его действия;

6.1.6. Сертификат ключа проверки ЭП может выдаваться любому работнику Института для подтверждения подлинности ЭП владельца ключа ЭП в каком-либо документе;

6.1.7. Сертификаты ключей проверки ЭП могут выдаваться как в форме электронных документов, так и в форме документов на бумажном носителе. Владелец сертификата ключа проверки ЭП, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки ЭП на бумажном носителе, заверенную ОИТ;

6.1.8. Сертификат ключа проверки ЭП должен содержать следующую информацию:

6.1.8.1. Даты начала и окончания срока его действия;

6.1.8.2. Фамилия, имя и отчество или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки ЭП;

6.1.8.3. Ключ проверки ЭП;

6.1.8.4. Наименование используемого средства ЭП и (или) стандарты, требованиям которых соответствуют ключ ЭП и ключ проверки ЭП;

6.1.9. Сертификат ключа проверки НЭП в форме электронного документа должен храниться в реестре ОИТ в обязательном порядке до аннулирования сертификата ключа проверки НЭП.

6.2. Прекращение действия ЭП:

6.2.1. Сертификат ключа проверки ЭП и ключ ЭП прекращают свое действие в следующих случаях:

6.2.1.1. В связи с истечением установленного срока его действия;

6.2.1.2. На основании заявления владельца сертификата ключа проверки ЭП, подаваемого в письменной или электронной форме (Приложение № 1 к Регламенту);

6.2.1.3. В случаях увольнения работника Института или изменения его должности;

6.2.1.4. В случаях обращения пользователя ЭП в ОИТ с уведомлением о нарушении конфиденциальности ключа.

6.2.2. При возникновении случаев, перечисленных в пункте 6.2.1. настоящего Регламента, с НЭП специалист ОИТ должен аннулировать действие сертификата ключа проверки НЭП и уведомить об этом владельцев сертификатов ключей проверки НЭП. Информация об аннулировании сертификата ключа проверки НЭП должна быть внесена в реестр сертификатов в течение одного рабочего дня с момента наступления обстоятельств, повлекших за собой прекращение действия сертификата ключа проверки НЭП в порядке, предусмотренном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

6.2.3. При возникновении случаев, перечисленных в пункте 6.2.1. настоящего Регламента, с КЭП специалист ОИТ должен оформить заявление на прекращение действия КЭП в аккредитованный удостоверяющий центр, выдавший данную КЭП.

6.2.4. При возникновении случаев, перечисленных в пункте 6.2.1. настоящего Регламента, с ПЭП специалист ОИТ должен аннулировать ПЭП и уведомить об этом владельцев ПЭП.

6.3. Приостановление действия сертификата ключа проверки НЭП:

6.3.1. Приостановление действия сертификата ключа проверки НЭП заявителя осуществляется специалистом ОИТ на основании заявления, подписанного собственноручной подписью или НЭП владельца (Приложение № 1 к Регламенту);

6.3.2. Специалист ОИТ не позднее одного рабочего дня с момента принятия заявления, указанного в пункте 6.3.1 настоящего Регламента, обязан уведомить владельца о приостановлении действия сертификата ключа НЭП.

6.4. Возобновление действия сертификата ключа проверки НЭП:

6.4.1. Возобновление действия сертификата ключа проверки НЭП заявителя осуществляется специалистом ОИТ на основании заявления в письменной или в электронной форме согласно Приложению № 1 к Регламенту.

6.4.2. Возобновление действия сертификата ключа проверки НЭП возможно только в течение срока, на который было приостановлено действие сертификата ключа проверки.

7. Порядок проверки НЭП, КЭП и ПЭП

7.1. Проверка НЭП или КЭП в электронном документе производится ОИТ на основании запроса участника электронного взаимодействия (далее – заявитель). К запросу заявителя должен прилагаться электронный документ, подписанный НЭП или КЭП.

7.2. Проверка ПЭП Институтом осуществляется в порядке, предусмотренном соглашением об электронном взаимодействии (Приложение № 2 к настоящему регламенту).

7.3. Срок проведения работ по проверке НЭП, КЭП и ПЭП составляет три рабочих дня с момента поступления запроса заявителя в ОИТ.

8. Конфиденциальность информации

8.1. К конфиденциальной информации участников электронного взаимодействия относятся:

8.1.1. Ключи НЭП и КЭП, соответствующие сертификату ключа проверки НЭП и КЭП, хранящемуся на ключевом носителе владельца;

8.1.2. Персональная информация об участниках электронного взаимодействия, хранящаяся в ОИТ;

8.1.3. Пароли доступа к ключевому носителю;

8.1.4. Сведения, информация и данные, признаваемые ключом его простой электронной подписи;

8.1.5. Иная информация в соответствии с законодательством Российской Федерации.

9. Обеспечение информационной безопасности электронных документов

9.1. Институт обеспечивает защиту от несанкционированного доступа и преднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных документах при электронного взаимодействии.

9.2. Соблюдение Институтом требований информационной безопасности при электронном взаимодействии обеспечивает:

9.2.1. Конфиденциальность информации (получить доступ к информации может получить только определенный круг лиц);

9.2.2. Целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);

9.2.3. Аутентификацию (когда передаваемую информацию может получить только то лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

9.3. Требования по информационной безопасности при электронном взаимодействии реализуются посредством применения программно-технических средств и организационных мер.

9.3.1. К программно-техническим средствам относятся:

9.3.1.1. Доменная политика с требованиями по длине, сложности и периодичности изменения пользовательских паролей;

9.3.1.2. Электронные журналы системных событий, пользовательских действий и ошибок приложений;

9.3.1.3. Разграничение доступа к техническим и программным средствам при электронном взаимодействии;

9.3.1.4. Средства антивирусной защиты с актуальными сигнатурными базами;

9.3.1.5. Средства резервного копирования информационных систем и средств электронного документооборота при электронном взаимодействии;

9.3.1.6. Специализированные средства работы с носителями ключевой информации (применимо при подписании документов УНЭП);

9.3.1.7. Дополнительная парольная защита информационной системы (применимо при подписании документов УНЭП);

9.3.2. К организационным мерам относятся:

9.3.2.1. Ограничение доступа к техническому и сетевому оборудованию;

9.3.2.2. Задание режима использования пользователями и администраторами паролей и идентификаторов;

9.3.2.3. Разработка, поддержание в актуальном состоянии и следование ЛНА, определяющему порядок резервного копирования, парольной политики, обновления средств антивирусной защиты;

9.3.2.4. Информирование персонала о порядке использования, хранения и обновления электронной подписи;

9.3.2.5. Поддержание программно-технических средств в исправном состоянии;

9.3.2.6. Защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.);

9.3.2.7. Ведение журнала учета ключевых носителей (применимо при подписании документов УНЭП);

9.3.2.8. Определение мест хранения ключевых носителей (применимо при подписании документов УНЭП);

9.3.2.9. Определение круга лиц, допущенных к работе с УКЭП (применимо при подписании документов УКЭП).

10. Хранение

10.1. Электронные документы при электронном взаимодействии после их исполнения подлежат хранению в течение сроков, предусмотренных законодательством для аналогичных документов на бумажных носителях. Допускается хранение подписанных документов в системе 1С: Предпиятие.

10.2. Хранение электронных документов, подписанных УНЭП осуществляется в формате .PDF, сигнатура подписи документа хранится в формате .SIG или .BIN. Документы, хранящиеся в электронной системе, не должны изменяться с момента формирования сигнатуры подписи.

10.3. К документам, подписанным ПЭП, и листам ознакомления с документами, подписанным ПЭП, требования п. 10.2 не предъявляются. Хранение документа осуществляется в формате, пригодным для воспроизведения.

10.4. После истечения срока оперативного хранения электронный документ вместе с сигнатурой подписи передается в архив (при наличии законодательного требования).

10.5. После истечения установленного срока хранения электронных документов в обязательном порядке проводится экспертиза ценности электронных документов аналогично документам на бумажных носителях.

10.6. По результатам экспертизы ценности на основании акта о выделении к уничтожению, утверждаемого ректором Института, внесенные в акт электронные документы подлежат уничтожению (удалению).

Приложение № 1
к Регламенту
применения электронной подписи в
АНОО ВО «Воронежский экономико-
правовой институт» и филиалах

Ректору АНОО ВО «Воронежский экономико-правовой институт»
С.Л. Иголкину
от _____
(наименование должности)
_____
(наименование структурного подразделения)
_____
(Фамилия)
_____
(Имя)
_____
(Отчество)
_____
(Телефон / email)

ЗАЯВЛЕНИЕ

Прошу создать/ перевыпустить/ прекратить/приостановить/возобновить
(нужное подчеркнуть)
действие /НЭП/КЭП в связи с_____
(нужное подчеркнуть) (указать основание (причину))
_____
_____

«__» _____20 __г. _____
(дата написания заявления) (подпись работника)

Руководитель подразделения

_____ _____
(подпись) (Ф.И.О.)

Приложение № 2
к Регламенту
применения электронной подписи в АНОО ВО «Воронежский экономико-правовой институт» и филиалах

СОГЛАШЕНИЕ
об электронном взаимодействии

Настоящее соглашение (далее – Соглашение) разработано Автономной некоммерческой образовательной организацией высшего образования «Воронежский экономико-правовой институт» (далее – Институт) в форме оферты и является официальным предложением Института стать участником электронного взаимодействия в соответствии с частью 2 статьи 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» для обмена информацией в электронной форме с использованием программно-информационных систем удаленного доступа, электронных документов, подписываемых простой электронной подписью.

Соглашение считается заключенным и приобретает силу после его подписания Пользователем.

Соглашение утверждено ректором Института либо уполномоченным им лицом и доступно для ознакомления в информационной телекоммуникационной сети Интернет на сайте www.vepi.ru.

Институт вправе в одностороннем порядке изменить условия Соглашения. При изменении условий Соглашения Институт уведомляет через личный кабинет всех участника электронного взаимодействия.

1. Термины и определения

Термины, используемые в Соглашении, применяются в следующих значениях:

1.1. Участники электронного взаимодействия – Институт и Пользователь.

1.2. Пользователь (пользователь Системы) – физическое лицо (работник, обучающийся и/или его представитель или абитуриент и/или его представитель, заказчик образовательных услуг), являющееся пользователем домена Института (Active Directory), заключившее с Институтом настоящее Соглашение.

1.3. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1.4. Институт – Автономная некоммерческая образовательная организация высшего образования «Воронежский экономико-правовой институт», являющаяся оператором Системы.

1.5. Система – совокупность программ, баз данных для ЭВМ (в том числе Сайт, Мобильное приложение, Личный кабинет), представляющих собой автоматизированную систему Института по учету действий (активности) Пользователя в ней, фактов подписания Пользователем документов электронной подписью, обмену и хранению электронных документов участников электронного взаимодействия.

1.6. Личный кабинет – информационный сервис Института, доступ к которому предоставляется после установления сеанса связи посредством сети Интернет каждому Пользователю, прошедшему Авторизацию, предназначенный для удаленного обслуживания Пользователя и обеспечивающий подготовку, защиту, прием, передачу и обработку электронных документов с использованием сети Интернет.

1.7. Мобильное приложение – программа, установленная на мобильное устройство, предоставляющее Пользователю возможность доступа к Системе с мобильного устройства.

1.8. Авторизация – процесс анализа Институтом введенных Пользователем идентификационных данных, по результатам которого в отношении последнего Институтом определяется объем прав на использование Системы. Виды идентификационных данных определяются Институтом.

1.9. Простая электронная подпись (далее – ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. ПЭП представляет собой уникальную комбинацию логина и пароля, известную только Пользователю и однозначным образом сопоставленная с учетной записью пользователя домена Института (Active Directory). ПЭП используется Пользователем для подписания электронных документов. Система обеспечивает конфиденциальность информации о ПЭП.

1.10. Ключ проверки (открытый) простой электронной подписи (Логин) – элемент ключа простой электронной подписи, представляющий собой уникальную последовательность символов, предназначенную для доступа в информационную систему Института и подтверждения принадлежности простой электронной подписи её владельцу.

1.11. Ключ (закрытый) простой электронной подписи (Пароль) – элемент ключа простой электронной подписи, представляющий собой уникальную последовательность символов, известную только владельцу ПЭП.

1.12. Электронный документ – информация в электронной форме, подписанная ПЭП, признаваемая равнозначной документу на бумажном носителе, подписанной собственноручной подписью Пользователя.

1.13. Журнал событий – электронный документ, содержащий информацию о фактах подписания Пользователем документов электронной подписью.

1.14. Учетная запись в Active Directory – это набор данных, определяющих участника системы безопасности Института.

1.15. Федеральный закон – Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», регулирующий отношения в области

использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальные услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Иные термины, используемые в Соглашении, применяются в значениях, определяемых Федеральным законом.

2. Предмет соглашения

2.1. Участники электронного взаимодействия подтверждают, что на основании Соглашения в соответствии с частью 2 статьи 6 Федерального закона информация в электронной форме, подписанная ПЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

2.2. Использование Системы и передача данных возможны только при наличии доступа к сети Интернет. Для бесперебойной работы Системы Пользователю необходимо обеспечить надлежащее качество доступа к сети Интернет на устройстве.

2.3. Пользователь уведомлен и соглашается с тем, что безопасность и конфиденциальность данных, обрабатываемых в Системе, обеспечивается непосредственно Пользователем. Пользователь понимает и принимает риски, связанные с передачей персональных данных и использованием сети Интернет.

2.4. Пользователь обязуется:

2.4.1. Соблюдать конфиденциальность сведений, информации и данных, признаваемых ключом его простой электронной подписи;

2.4.2. Не разглашать кому-либо сведения, информацию и данные, признаваемые ключом его простой электронной подписи.

2.5. Пользователь заверяет и гарантирует Институту, что будет тщательным образом проверять содержание и данные, имеющиеся в подписываемых ПЭП документах. Подписание Пользователем ПЭП документа свидетельствует о его осведомленности с содержанием данного документа, а также о его указании на совершение указанных в нем действий и (или) полным и безоговорочным согласием на заключение договора (соглашения) с Институтом. Визуальное представление подписанного электронного документа в Системе может сопровождаться соответствующими графическими образами (штампами)

2.6. Одной ПЭП могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании ПЭП пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

2.7. Использование ПЭП для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

3. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

3.1. Электронные документы, подписанные Пользователем простой электронной подписью, признаются участниками электронного взаимодействия равнозначными документу на бумажном носителе, подписанному собственноручной подписью Пользователя, если в Системе содержатся следующие данные:

3.1.1. Наличие электронного документа;

3.1.2. Факт формирования простой электронной подписи, как это определено в разделе 4 Соглашения, применительно к сформированному электронному документу;

3.1.3. В Журнале Событий, формируемом Институтом в порядке, предусмотренном пунктом 4.2. Соглашения, содержится информация, указывающая на Пользователя. Данная информация содержится в виде ключа проверки электронной подписи.

3.2. Информация о факте формирования и подписания электронного документа, а также указание на Пользователя содержатся в Журнале событий.

4. Порядок формирования ключа электронной подписи

4.1. Ключ электронной подписи состоит из публичной и конфиденциальной части ПЭП. Пара частей ПЭП являются уникальными последовательностями символов. В качестве публичной части ключа выступает логин к учетной записи, в качестве конфиденциальной – пароль к учетной записи, который создается Институтом по умолчанию и представляет собой набор символов с последними 6 цифрами номера паспорта Пользователя, которые после первого входа Пользователь должен сменить с целью повышения (обеспечения) безопасности.

4.2. Журнал событий должен содержать: ссылку на подписанный ПЭП документ, дату и время подписания и идентификатор пользователя (логин).

4.3. Дата и время подписания электронного документа ПЭП фиксируется в Журнале событий по московскому времени (UTC+3).

5. Правила определения лица, подписывающего электронный документ

5.1. Факт формирования электронной подписи именно Пользователем подтверждается: Авторизацией с использованием публичной и конфиденциальной части ПЭП Пользователя в Системах Института.

5.2. Пользователь, подписывающий документ ПЭП, определяется в Системе через Авторизацию путем ввода логина и пароля Пользователя. Информация, указывающая на Пользователя, помещается Институтом в Журнал событий. Институт обеспечивает хранение электронных документов и Журнал событий в Системе в условиях, позволяющих их извлечение в оперативном режиме уполномоченными лицами Института.

5.3. Проверка ПЭП Институтом осуществляется путем сравнения идентификатора пользователя в Журнале Событий с записями в учетной системе (кадровой или студенческой). Определение лица по его электронной подписи осуществляется путем сопоставления в Системе ключа проверки электронной подписи с данными Системы о подписавшем лице.

5.4. Участники электронного взаимодействия обязаны соблюдать конфиденциальность ключа электронной подписи.

6. Вид информации, обмен которой производится в электронной форме

6.1. Участники электронного взаимодействия установили, что документы могут быть подписаны в системе электронного документооборота и совершены юридически значимых действий с использованием ПЭП.

При этом, если возникнет необходимость, Пользователь вправе получить бумажный экземпляр электронного документа в соответствующем структурном подразделении.

6.2. При изготовлении экземпляра электронного документа, подписанного простой электронной подписью, на бумажном носителе, в графе «подпись» со стороны Института может быть сформирован скан-образ подписи подписанта, указанного в договоре. Со стороны Пользователя указывается:

ПОДПИСАНО ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
В СООТВЕТСТВИИ С СОГЛАШЕНИЕМ ОБ ЭЛЕКТРОННОМ ВЗАИМОДЕЙСТВИИ

Дата, время подписи ФИО Пользователя

7. Заключительные положения

7.1. Настоящее соглашение заключено участниками электронного взаимодействия на неопределенный срок и вступает в силу с даты получения Институтом полного и безоговорочного акцепта Пользователем условий настоящего соглашения по форме, являющейся Приложением № 1 к настоящему Соглашению.

7.2. Участник электронного взаимодействия имеет право в любое время в одностороннем порядке отказаться от настоящего соглашения, письменно уведомив об этом другую сторону не позднее, чем за 30 (Тридцать) календарных дней до предполагаемого момента отказа от настоящего соглашения.

7.3. С даты прекращения (расторжения) настоящего соглашения Институт вправе отказать в принятии и исполнении документов, подписанных простой электронной подписью Пользователя.

7.4. Прекращение (расторжение) настоящего соглашения не освобождает участников электронного взаимодействия от исполнения ими своих обязательств, возникших до момента расторжения соглашения, а также не влечет расторжение или прекращение договоров, соглашений или прекращения действия документов, подписанных простой электронной подписью Пользователя. Все документы, подписанные в порядке, предусмотренном настоящим соглашением, являются действующими.

7.5. Участники электронного взаимодействия установили рекомендуемый перечень электронных документов, подписываемых ПЭП, и юридически значимых действий, совершаемых с использованием ПЭП в соответствии с Приложением № 2 к настоящему соглашению.

Приложение № 1
к СОГЛАШЕНИЮ
об электронном взаимодействии

АКЦЕПТ: Я, _____
(Фамилия, имя, отчество Пользователя)
настоящим безоговорочно без каких-либо изъятий или ограничений на условиях присоединения принимаю условия СОГЛАШЕНИЯ об электронном взаимодействии, опубликованного на официальном сайте Института, и выражаю согласие на подписание электронных документов в личном кабинете.

Контактные и паспортные данные Пользователя:

1. Серия и номер паспорта, кем и когда выдан, дата рождения _____.
2. Номер мобильного телефона _____.
3. Адрес электронной почты _____.

В целях заключения СОГЛАШЕНИЯ об электронном взаимодействии, соблюдения законодательства Российской Федерации, нормативных правовых актов федеральных органов исполнительной власти, органов власти субъектов Российской Федерации, решений органов местного самоуправления, решений, поручений и выполнения запросов органов, осуществляющих функции и полномочия учредителей Института, лиц, осуществляющих контрольные, надзорные и иные проверочные мероприятия в отношении Института, в том числе аудиторов, Пользователь дает Институту согласие на осуществление последним со дня акцепта и в течение 3 (Трех) лет после прекращения действия настоящего соглашения об электронном взаимодействии записи, систематизации, накопления, хранения, уточнения, извлечения, использования, передачи (предоставления, распространения, доступа) третьим лицам персональных данных Пользователя, содержащихся в настоящем соглашении или становящихся известными Институту в связи с его исполнением, в частности фамилии, имени, отчества, паспортных данных, номера мобильного телефона, адреса электронной почты, в том числе путем автоматизированной обработки таких данных.

Пользователь согласен на обезличивание, блокирование, удаление и уничтожение указанных персональных данных в случаях, когда это необходимо и/или возможно при реализации указанных целей.

Согласие может быть отозвано Пользователем путем представления Институту письменного заявления Пользователя с указанием мотивированных причин его отзыва.

_____/ _____ /
Подпись Фамилия, имя, отчество Пользователя*

* Варианты оформления акцепта Пользователя:

- акцепт в электронном виде - удостоверяется кодами, паролями, иными средствами, позволяющими подтвердить, что указанный акцепт составлен Пользователем.
- акцепт на бумажном носителе - оформляется собственноручной подписью Пользователя и передается им в (структурное подразделение Института).

Приложение № 2
к СОГЛАШЕНИЮ
об электронном взаимодействии

РЕКОМЕНДУЕМЫЙ ПЕРЕЧЕНЬ
электронных документов, подписываемых простой электронной подписью, и юридически значимых действий, совершаемых с использованием простой электронной подписи в случае, если Пользователем является обучающийся или абитуриент Института, заказчик образовательных услуг

1. Договор об образовании, дополнительные соглашения к договору об образовании.

2. Заявления:

2.1. О восстановлении;
2.2. О переводе из других образовательных учреждений;
2.3. О приеме на обучение;
2.4. О распределении для освоения образовательных программ;
2.5. О согласии на обработку персональных данных;
2.6. Об изменении персональных данных;
2.7. О возврате денежных средств;
2.8. О предоставлении льготы по оплате за обучение.
2.9. Об отчислении из Института по инициативе обучающегося;
2.10. Заявление об отсрочке оплаты за обучение;
2.11. О предоставлении академического отпуска;
2.12. О выходе из академического отпуска.

3. Иные заявления и документы, оформляемые в процессах: участия в приемной кампании Института; обучения в Институте; осуществления уставной деятельности Института; реализации прав и обязанностей участников электронного взаимодействия, установленных действующим законодательством, локальными нормативными актами Института, настоящим соглашением, иными договорами и соглашениями, заключенными в установленном порядке.