ЮЗГУ	**МИНОБРНАУКИ РОССИИ** **Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»**
	Система менеджмента качества

УТВЕРЖДАЮ

Ректор университета

(должность)

С.Г. Емельянов

(подпись)

«03» октября 2023 г.

ПОЛОЖЕНИЕ

Об использовании в служебных целях ключей электронной подписи

П 96.217–2023

(Издание 1)

Введено в действие **Приказом от** «03» октября 2023 г. № 1344

Дата введения «03» октября 2023 г.

Срок действия до «03» октября 2028 г.

Введено впервые

Содержание

1 Область применения

1.1 Настоящее положение об использовании в служебных целях ключей электронной подписи (далее – положение) устанавливает порядок работы с электронной подписью (далее – ЭП), выданной на должностное лицо или юридическое лицо, ответственность и обязанности работников при использовании ЭП в ФГБОУ ВО «Юго-Западный государственный университет» (далее – университет).

1.2 Все изменения и дополнения настоящего положения вступают в силу с момента их утверждения приказом по университету.

2 Нормативные ссылки

2.1 Настоящее положение разработано на основе Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ (далее – ФЗ № 63-ФЗ).

2.2 Положение разработано в соответствии со следующими нормативно-правовыми документами:

Электронная подпись. Действующие нормативные акты, регулирующие вопросы получения и использования электронной подписи (ЭП; ранее - электронная цифровая подпись, ЭЦП):

– Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

– Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

– Постановление Правительства Российской Федерации от 25.06.2012 № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг».

– Постановление Правительства Российской Федерации от 25.08.2012 № 852 «Об утверждении Правил использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг и о внесении изменения в Правила разработки и утверждения административных регламентов предоставления государственных услуг».

– Постановление Правительства Российской Федерации от 09.02.2012 №111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

– Постановления Правительства Российской Федерации от 25.01.2013 № 33 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

– Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

– Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

– Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

– Приказ Минкомсвязи России от 22.08.2017 № 436 «Об утверждении Порядка формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

– Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.08.2018 № 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей».

– Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.08.2021 № 857 «Об утверждении единых требований к формам доверенностей, необходимых для использования квалифицированной электронной подписи.

Электронные торги. Действующие нормативные акты, регулирующие государственные и коммерческие закупки, а также реализацию имущества с использованием электронной подписи:

– Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

– Федеральный закон от 21.12.2001 № 178-ФЗ «О приватизации государственного и муниципального имущества».

– Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

– Федеральный закон от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)».

– Постановление Правительства Российской Федерации от 30.12.2018 № 1752 «О порядке регистрации участников закупок в единой информационной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд и ведения единого реестра участников закупок и внесении изменений в постановление Правительства Российской Федерации от 8 июня 2018 г. № 656».

– Постановление Правительства Российской Федерации от 25.12.2018 № 1663 «Об утверждении Положения об особенностях документооборота при осуществлении закрытых конкурентных закупок в электронной форме и порядке аккредитации на электронных площадках для осуществления закрытых конкурентных закупок».

– Постановление Правительства Российской Федерации от 27.08.2012 № 860 «Об организации и проведении продажи государственного или муниципального имущества в электронной форме».

– Постановление Правительства Российской Федерации от 28.02.2019 № 223 «Об особенностях проведения закрытых электронных процедур и порядке аккредитации на специализированных электронных площадках».

– Постановление Правительства Российской Федерации от 10.05.2018 № 564 «О взимании операторами электронных площадок, операторами специализированных электронных площадок платы при проведении электронной процедуры, закрытой электронной процедуры и установлении ее предельных размеров».

– Постановление Правительства РФ от 30.05.2018 № 626 «О требованиях к договору специального счета и порядку использования имеющегося у участника закупки банковского счета в качестве специального счета, требованиях к условиям соглашения о взаимодействии оператора электронной площадки с банком, правилах взаимодействия участника закупки, оператора электронной площадки и заказчика в случае предоставления участником закупки банковской гарантии в качестве обеспечения заявки на участие в открытом конкурсе в электронной форме, конкурсе с ограниченным участием в электронной форме, двухэтапном конкурсе в электронной форме, электронном аукционе».

– Распоряжение Правительства Российской Федерации от 28.04.2018 № 824-р «О создании единого агрегатора торговли».

– Приказ Минэкономразвития России от 23.07.2015 № 495 «Об утверждении Порядка проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, Требований к операторам электронных площадок, к электронным площадкам, в том числе технологическим, программным, лингвистическим, правовым и организационным средствам, необходимым для проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, внесении изменений в приказ Минэкономразвития России от 05.04.2013 № 178 и признании утратившими силу некоторых приказов Минэкономразвития России».

Электронный документооборот. Действующие нормативные акты, связанные с правовым регулированием электронного документооборота:

– Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Постановление Правительства Российской Федерации от 22.09.2009 № 754 «Об утверждении Положения о системе межведомственного электронного документооборота».

– Приказ Минфина России от 10.11.2015 № 174н «Об утверждении Порядка выставления и получения счетов-фактур в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи».

Электронная отчетность. Действующие нормативные акты, регулирующие использование электронной подписи при сдаче отчетности через информационно-телекоммуникационную сеть «Интернет»:

– Постановление Правительства Российской Федерации от 26.12.2011 № 1137 «О формах и правилах заполнения (ведения) документов, применяемых при расчетах по налогу на добавленную стоимость».

– Приказ ФНС России от 05.12.2016 N ММВ-7-21/668 «Об утверждении формы и формата представления налоговой декларации по транспортному налогу в электронной форме и порядка ее заполнения».

– Приказ Фонда социального страхования России от 12.02.2010 № 19 «О внедрении защищенного обмена документами в электронном виде с применением электронной цифровой подписи для целей обязательного социального страхования».

– Приказ Федеральной налоговой службы России от 17.12.2008 № ММ-3-6/665 «Об утверждении Порядка ведения единого пространства доверия сертификатам ключей ЭЦП».

– Приказ ФНС России от 30.01.2012 № ММВ-7-6/36@ «Об утверждении форматов представления документов, используемых при выставлении и получении счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной подписи».

Защита информации. Действующие нормативные акты, содержащие правовые основы защиты информации:

– Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне».

– Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

– Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Указ Президента России от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

– Приказ ФСБ России и Федеральной службы по техническому и экспортному контролю России от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

– Приказ Федеральной службы по техническому и экспортному контролю 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».

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи. Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Заявка на регистрацию ключа - служебное сообщение, содержащее новый открытый ключ, подписанное электронной цифровой подписью.

Информационная система общего пользования (ИС) - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Квалифицированная электронная подпись (КЭП) - аналог собственноручной подписи руководителя. Технически КЭП это файл с данными владельца подписи и информацией о подписанном документе в зашифрованном виде. КЭП используется для участия в электронных торгах, работы в госсистемах и на госпорталах, отчетности, обмена электронными документами с сотрудниками и партнерами. Собственноручная и электронная подписи имеют одинаковую юридическую силу. КЭП соответствует следующим требованиям:

– получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

– позволяет определить лицо, подписавшее электронный документ;

– позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

– создается с использованием средств электронной подписи;

– ключ проверки электронной подписи указан в квалифицированном сертификате;

– для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с законом

Работник организации получает КЭП самостоятельно в удостоверяющем центре на своё имя как физическое лицо. Ключ защищён от передачи другим лицам, что повышает безопасность операций.

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

Классификатор полномочий – портал с перечнем полномочий сотрудника, которые следует указывать в машиночитаемой доверенности. Каждое полномочие содержит наименование, дату включения в классификатор и уникальный идентификационный номер – именно он дает право подписи. Классификатор позволяет быстро определить полномочия сотрудника и корректно отобразить их в МЧД. (Актуальный классификатор полномочий размещен на сайте «Единой системы нормативной справочной информации (ЕСНСИ) Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

Ключ шифрования – ключ, предназначенный для закрытия электронного документа при электронных взаимодействиях.

Ключевой носитель (носитель ключевой информации) (НКИ) - физический носитель для ЭП. Выполнен в виде флэш-карты, вставляемой в USB-порт любого компьютера.

Компрометация закрытого ключа ЭП - любая ситуация, свидетельствующая об утере владельцем или пользователем ЭП исключительного права владения и распоряжения ключевым носителем и/или его PIN-кодом. Причины компрометации ключа ЭП могут быть совершенно различными: от невнимательности владельца до хакерской атаки. Поэтому, обладая ключевым носителем, нужно знать его характеристики, чтобы лучше понимать, как и когда ваш ключ может быть скомпрометирован. За компрометацию ключа несет ответственность не только ее владелец, но и удостоверяющий центр.

Компрометация ключевой информации - утрата, хищение, несанкционированное копирование или подозрение на копирование носителя ключевой информации НКИ или любые другие ситуации, при которых достоверно не известно, что произошло с НКИ. К компрометации ключевой информации также относится увольнение сотрудников, имевших доступ к ключевой информации.

Корпоративная информационная система (КИС) - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Крипто-программа - компьютерная программа позволяющая осуществлять операции с ЭП: устанавливать сертификаты, проверять подписи других работников под документом и др.

Машиночитаемая доверенность (МЧД) - доверенность в электронном виде в формате XML, подписанная усиленной квалифицированной электронной подписью (УКЭП) руководителя организации, где описаны полномочия сотрудника организации подписывать документы от имени организации и позволяет сотрудникам предоставлять интересы организации в электронном документообороте с контрагентами, сдавать отчетность, выставлять счета, оформлять закрывающие документы. Одна МЧД может выдаваться сразу на группу сотрудников организации, а в одной МЧД можно указать сразу несколько полномочий: по одной доверенности сотрудник может выполнять разные операции. Подписывать документы без МЧД могут только руководители организаций. С 1 сентября 2023 года юридические лица обязаны передавать все выданные МЧД в единый реестр машиночитаемых доверенностей ФНС России. Хранение МЧД осуществляется в едином блокчейн хранилище машиночитаемых доверенностей распределенного реестра ФНС России. Помимо блокчейна хранить доверенность можно в информационных системах доверителя, оператора ЭДО, а также федеральных органов исполнительной власти. Главное, чтобы хранение МЧД было публичным и можно было без проблем получить информацию о статусе документа.

PIN-код - пароль доступа пользователя ЭП к функционалу ключевого носителя. Предотвращает несанкционированное использование ключевого носителя. Требования к паролю доступа: длинна пароля должна быть не меньше 8 символов, пароль должен включать в себя цифры и буквы в разных регистрах, а также специальные символы, не должны использоваться стандартные и легко вычисляемые комбинации символов, при смене пароля новый должен отличаться от старого как минимум по 4 знакам, периодичность смены пароля - не реже 6 месяцев.

Подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Пользователь ЭП - работник университета, наделенный полномочиями подписывать документацию с использованием ЭП.

Рабочее место пользователя ЭП - кабинет или аудитория, на территории университета оснащённая компьютерным оборудованием для использования ЭП.

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие

принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификация организации (юрлица) - с 1 сентября 2023 года выдаются два типа сертификата организации (юрлица) – 1) на руководителя (выдается один на организацию) и 2) обезличенный сертификат без реквизитов пользователя, который содержит в себе только реквизиты юрлица (выдается по количеству информационных систем). Оба типа сертификата организации выдаются только на защищенном токене в УЦ ФНС, УЦ Федерального казначейства и УЦ ЦБ, при этом: УЦ ФНС обеспечивает сертификатами все организации, УЦ Федерального казначейства выдает сертификаты всем бюджетным организациям УЦ ЦБ выдает сертификаты всем кредитным и финансовым организациям.

Сертификация ключа - процедура заверения (подписания) открытой части регистрируемого ключа электронной цифровой подписью.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Удостоверяющий центр (УЦ) - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законом. В обязанности УЦ входят следующее:

– удостоверить личность человека, который обратился за сертификатом электронной подписи,

– изготовить и выдать сертификат, в который включены данные о владельце сертификата и его открытый ключ проверки,

– управлять жизненным циклом сертификата (выпуск, приостановление, возобновление, окончание срока действия).

Усиленная квалифицированная электронная подпись (УКЭП) - цифровой аналог собственноручной подписи. Документы, подписанные от руки или с помощью **УКЭП** имеют равнозначную ценность, это файл, в котором хранится зашифрованная информация, подтверждающая личность человека и подлинность подписанного документа.

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

Центр управления ключевыми системами (ЦУКС) - место изготовления носителя ключевой информации НКИ.

Шифрование - специализированный метод защиты информации от ознакомления с ней третьих лиц, основанный на кодировании информации по алгоритму ГОСТ 28147-89 с использованием соответствующих ключей.

Электронная подпись (ЭП) — 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.

3.2 Сокращения и обозначения

ИС – информационная система общего пользования;
КИС – корпоративная информационная система;
КЭП–квалифицированная электронная подпись;
МЧД – машиночитаемая доверенность**;**
НКИ – носитель ключевой информации;
ОСАиТП – отдел системного администрирования и технической поддержки;
ОИБ – отдел информационной безопасности;
ЦУКС – центр управления ключевыми системами;
ЭП–электронная подпись;
УКЭП – усиленная квалифицированная электронная подпись**;**
УЦ– удостоверяющий центр.

4 Положения

4.1 Общие положения

4.1.1 Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

4.1.2 В случае необходимости использования ЭП работником университета для выполнения своих должностных (функциональных) обязанностей, данный работник должен обратиться с заявлением на использование ЭП служебной запиской установленной формы (приложение А) на имя ректора университета.

4.1.3 В случае утверждения (согласования) ректором университета заявления, оно передаётся начальнику ОСАиТП для выполнения им работ по формированию реестра пользователей ЭП и подготовке рабочего места для работы с ЭП.

4.1.4 В случае получения отказа в использовании ЭП по поступившему от работника заявлению, данное заявление обрабатывается в соответствии с правилами документооборота и делопроизводства университета.

4.1.5 Начальник ОСАиТП ведёт реестр пользователей ЭП с указанием следующей информации:

– ФИО;

– структурное подразделение, должность;

– наименование информационной системы, в которой используется ЭП;

– инвентарный номер компьютера, на котором установлена ЭП и компоненты для работы с ЭП;

– номер рабочего кабинета, где установлен компьютер с компонентами ЭП.

– идентификатор ЭП;

– идентификатор ключевого носителя;

– срок действия сертификата ключа проверки ЭП.

4.1.6 Работник университета, подучивший положительное, решение на использование ЭП, самостоятельно производит сбор пакета документов на выпуск ЭП (паспорт, СНИЛС и ИНН - в случае создания новой ЭП). Доверенность на получение документов и ЭП в удостоверяющем центре, делается по соответствующей форме на работника подавшего заявление на использование ЭП.

4.1.7 Пользователи ЭП имеют право допускать до работы с ЭП начальника ОСАиТП только в случаях проведения им работ по установке, настройке или восстановлению работы компонентов ЭП и доступа к информационным системам.

4.1.8 Начальнику ОСАиТП запрещается самостоятельно подписывать какие-либо документы ЭП.

4.1.9 Срок сертификата ключа проверки ЭП - 1 год с даты, его выдачи. По истечении этого срока сертификат необходимо продлить. Порядок продления срока действия ключа проверки ЭП описан в пункте 8 настоящего положения.

4.1.10 ЭП должна использоваться только на рабочем месте пользователя ЭП, указанном в заявлении (приложение А).

4.1.11 Не допускается использование одной ЭП несколькими пользователями ЭП на одном рабочем месте. Каждый пользователь должен иметь соответствующие полномочия (положительное решение по заявлению на использование ЭП).

4.1.12 Сотрудникам университета, не являющимся владельцами ЭП, запрещено использование ЭП.

4.2 Права и обязанности владельца (пользователя) ЭП

4.2.1 **Владелец ЭП имеет право:**

– обращаться к ответственному за техническую поддержку информационной системы для аннулирования (отзыва), приостановки (возобновления) действия принадлежащего ему ключа электронной подписи;

– в случае необходимости замены, восстановления ключа электронной подписи обратиться к ответственному за техническую поддержку информационной системы с соответствующей просьбой и получить новый ключ электронной подписи;

– обращаться к руководству университета для разбора конфликтных ситуаций (споров), возникающих при применении ЭП в информационной системе.

4.2.2 **Владелец ЭП обязан:**

– вести обработку внутренних электронных документов в информационной системе в соответствии со своими должностными обязанностями;

– принимать все возможные меры для предотвращения несанкционированного использования своего ключа электронной подписи;

– ни при каких условиях не передавать ключевой носитель с PIN-кодом сторонним лицам (включая работников университета);

– обеспечить сохранность и конфиденциальность ключей электронной подписи, не допускать использование ключей электронных подписей другими работниками университета;

– при утере или пропаже ключевого носителя, компрометации ключа электронной подписи незамедлительно обратиться к своему непосредственному руководителю, начальнику ОИБ и начальнику ОСАиТП ответственному за техническую поддержку информационной системы для приостановки действия принадлежащего ему ключа электронной подписи;

– уведомлять своего непосредственного начальника, начальника ОСАиТП и начальника ОИБ о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

– не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

– использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с ФЗ № 63-ФЗ;

– хранить в тайне закрытый ключ ЭП;

– самостоятельно контролировать срок действия сертификата проверки ключа ЭП.

4.3 Аннулирование (отзыв) сертификата ключа проверки ЭП

4.3.1 Аннулирование сертификата электронной подписи производится только удостоверяющим центром в случаях установленных ФЗ № 63-ФЗ:

– не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

– установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

– вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

4.3.2 До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи удостоверяющий центр обязан уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

4.3.3 При получении соответствующего уведомления об аннулировании сертификата ключа, данное уведомление должно быть доведено в течение одного рабочего дня до непосредственного руководителя, начальника ОСАиТП и начальник ОИБ.

4.3.4 При аннулировании сертификата ЭП, в течение трёх рабочих дней в университете создаётся комиссия по установлению причин, приведших к

аннулированию данного сертификата. Комиссию возглавляет ректор университета или по его решению – проректор по цифровой трансформации. Руководитель структурного подразделения, сертификат ЭП работника, которого аннулируется, а также начальник ОСАиТП и начальник ОИБ являются обязательными членами данной комиссии. По итогам работы комиссии готовится Протокол с описанием причин, приведших к аннулированию сертификата ЭП и установлением работников университета, действия которых привели к аннулированию сертификата ЭП.

4.4 Прекращение действия сертификата ключа проверки ЭП

4.4.1 Сертификат ключа проверки ЭП прекращает своё действие:

– в связи с истечением установленного срока его действия;

– на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

– в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

– в иных случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

4.4.2 При необходимости прекратить действие сертификата ключа проверки ЭП досрочно, пользователь ЭП информирует своего непосредственного руководителя, начальника ОСАиТП, начальника ОИБ о данном решении путём направления служебной записки в свободной форме с обязательным указанием причины возникновения необходимости в прекращении действия данного сертификата.

4.4.3 Заявление о прекращении действия сертификата проверки ключа ЭП в виде формируется пользователем ЭП, подписывается владельцем данного сертификата и направляется в удостоверяющий центр. Копия заявления передаётся пользователем ЭП начальнику ОСАиТП, о чем обязательно информируется начальник ОИБ.

4.5 Продление действия сертификата ключа проверки ЭП

4.5.1 Пользователь ЭП должен оповестить начальника ОСАиТП о необходимости продления сертификата ключа проверки ЭП не позднее 30-ти рабочих дней до даты прекращения действия данного сертификата служебной запиской.

4.5.2 После получения информации о необходимости продления сертификата, начальник ОСАиТП оказывает содействие пользователю ЭП в формировании перечня документов на продление сертификата.

4.5.3 Сбором документов на продление сертификата занимается пользователь ЭП.

4.5.4 Начальник ОСАиТП отслеживает факты продления сертификатов через ведение соответствующего реестра пользователей ЭП.

4.5.5 Установка нового сертификата на рабочее место пользователя ЭП производится работником ОСАиТП в течение двух рабочих дней со дня получения сертификата пользователем ЭП.

4.6 Перенос компонентов ЭП на новое рабочее место пользователя ЭП

4.6.1 В случае необходимости переноса компонентов ЭП на новое рабочее место, пользователь ЭП заблаговременно (служебной запиской) информирует об этом начальника ОСАиТП.

4.6.2 Перенос компонентов ЭП и соответствующая фиксация в реестре пользователей ЭП производится работником ОСАиТП.

4.7 Порядок хранения и выдачи ЭП

Порядок хранения ЭП должен строго соблюдаться и отвечать следующим правилам:

– Учет ключевых носителей ЭП осуществляется в специально заведенных журналах (приложение А, приложение Б) к «Инструкции о порядке обращения с шифровальными (криптографическими) средствами защиты информации, не содержащей сведений, составляющих государственную тайну», которые хранится в отделе информационной безопасности.

– Выдача ключевых носителей ЭП осуществляется на основании положительной резолюции ректора университета на заявлении работника под роспись работника в журнале поэкземплярного учета и движения носителей ключевой информации, который хранится в ОИБ. Необходимые записи о движении носителя ключевой информации производятся в части, касающейся работником ОИБ и работником ОСАиТП в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним.

– Хранение ключевого носителя ЭП работник университета (владелец ЭП) осуществляет только в сейфе или в запираемом рабочем столе таким образом, чтобы исключить любую возможность утраты или попадания ключевого носителя ЭП посторонним лицам.

– Установить **PIN-код** - на компьютер, токен и контейнер ключей. Также следует заменить заводские пароли токена и контейнера ключей ЭЦП.

– Категорически запрещено передавать носитель ЭП другому работнику. Каждый носитель ЭП определен под конкретного работника.

– Менять ЭП необходимо сразу же, как только работник уволился или поменялось название организации (учреждения).

– Пароль не должен храниться на бумаге и на видном месте.

– Необходимо осуществлять периодические проверки компьютера, на котором используется носитель ЭП на наличие компьютерных вирусов.

4.8 Ответственность пользователя ЭП

4.8.1 Пользователь ЭП несет персональную ответственность:

– за сохранность своего ключа ЭП и его защиту от несанкционированного использования;

– за полноту и достоверность сведений, находящихся на подписываемом электронной подписью документе;

– за возникновение причин, которые по его вине привели к аннулированию сертификата электронной подписи.

– за выполнение правил эксплуатации ключа ЭП при выполнении непосредственных работ.

4.8.2 Работник, нарушивший требования настоящего положения, несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение А

(обязательное)

Форма заявления на использование электронной подписи

Структурное подразделение

Ректору ЮЗГУ
проф. Емельянову С.Г.

СЛУЖЕБНАЯ ЗАПИСКА

20 г. № _____

Заявление на использование
электронной подписи

Прошу разрешить мне использование электронной подписи для выполнения своих должностных (функциональных) обязанностей.

Электронная подпись будет использоваться мною в следующих информационных системах:

1. *указать ссылку на сайт (информационную систему).*

2. ...

Место использования ЭП: *указать номер рабочего кабинета, номер учебного корпуса, инвентарный номер компьютера.*

С Положением об использовании в служебных целях ключей электронной подписи в ФГБОУ ВО «Юго-Западный государственный университет»» ознакомлен(а).

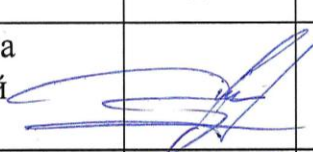
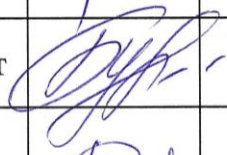
Должность *Личная подпись* *Инициалы и фамилия*

Виза согласования ректора университета

Лист согласования

Основание для разработки: План разработки и актуализации документации системы менеджмента качества на 2023 год

(наименование, дата и номер документа)

	Должность	Подпись	Фамилия, инициалы	Дата
Разработан:	Начальник отдела информационной безопасности		Жихорцев А.А.	26.09.2023
Проверен:	Проректор по цифровой трансформации		Пыхтин А.И.	26.09.23
Согласован:	Ведущий юрисконсульт		Будовская Е.В.	26.09.2023
	Начальник отдела менеджмента качества		Дмитракова Т.В.	26.09.2023г.
	Начальник отдела системного администрирования и технической поддержки		Крипачев А.В.	26.09.2023 г.

Лист ознакомления

С положением П 96.217–2023 «Об использовании в служебных целях ключей электронной подписи» ознакомлены:

Фамилия, инициалы	Дата ознакомления	Подпись

Лист регистрации изменений

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изме-ненных	заменен-ных	аннулиро-ванных	новых			