УТВЕРЖДАЮ
Временно исполняющий обязанности
ректора ФГБОУ ВО СПбГАУ
И.В. Солонько
_____
«30» декабря 2016 г.

ИНСТРУКЦИЯ
ПО ПРАВИЛАМ УЧЕТА, ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ СПбГАУ

СМК-СТО- / -2016

Дата введения
«30» декабря 2016 г.

Санкт-Петербург
2016

	Должность	Фамилия И.О.	Дата
Разработал	Исполняющий обязанности директора Центра информатизации и дистанционных технологий	Чижиков А.С.	20.12.16
Проверил	Директор Центра управления качеством образования	Цыганова Н.А.	28.12.16

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАНО Центром информатизации и дистанционных технологий федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный аграрный университет»

2 ВВЕДЕНО в действие приказом временно исполняющего обязанности ректора федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный аграрный университет» №747 от 30 декабря 2016 г.

3 ВЕРСИЯ 1.0

ЛИСТ СОГЛАСОВАНИЯ

Разработано:

Исполняющий обязанности директора Центра информатизации и дистанционных технологий _____ А.С. Чижиков

Проверено:

Директор Центра управления качеством образования _____ Н.А. Цыганова

Экспертиза проведена:

Главный юрист _____ С.П. Байдов

Согласовано:

Главный бухгалтер _____ Г.И. Мартынова

СОДЕРЖАНИЕ

1 Назначение и область применения

1.1 Инструкция по правилам учета, хранения и использования электронной подписи ФГБОУ ВО СПбГАУ (далее – Инструкция) определяет порядок работы с носителями ключевой информации (далее – НКИ); порядок изготовления, учета, регистрации ключей электронной подписи (далее – ЭП) и ключей шифрования в системе электронных взаимодействий; порядок использования НКИ в системе электронных взаимодействий; порядок действий при компрометации ключевых материалов; порядок обеспечения режима безопасности при работе с НКИ в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный аграрный университет» (далее – Университет, СПбГАУ).

1.2 Настоящая инструкция разработана для обладателей и ответственных лиц Систем криптозащиты информации (далее – СКЗИ), осуществляющих электронные взаимодействия со сторонними организациями с использованием НКИ.

2 Нормативные ссылки

Настоящая инструкция разработана с учетом требований следующих документов:

- «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 №51-ФЗ;
- Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи»;
- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая.

3 Основные термины

Автоматизированное рабочее место (АРМ) - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида автоматизированных систем.

Администратор информационной безопасности – лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами.

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

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

Компрометация ключевой информации – утрата, хищение, несанкционированное копирование или подозрение на копирование 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.

Носитель ключевой информации (НКИ) – носитель информации (флеш-накопитель, флэш-карта, или другие носители) на которых хранится электронный ключ, предназначенный для защиты электронных взаимодействий.

Открытый (публичный) ключ подписи – ключ, автоматически формируемый при изготовлении секретного ключа подписи и однозначно зависящий от него; предназначен для проверки корректности электронной подписи электронного документа. Открытый ключ считается принадлежащим участнику электронных взаимодействий, если он был сертифицирован (зарегистрирован) установленным порядком.

Пользователь НКИ – лицо, осуществляющее использование носителя ключевой информации

Секретный (закрытый) ключ подписи – ключ, предназначенный для формирования им электронной подписи на электронных документах.

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

Уполномоченный абонент СКЗИ – должностное лицо Университета, осуществляющее использование средства контроля защищенности информации.

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

ЦУКС - центр управления ключевыми системами, 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.

4 Организация работы с носителями ключевой информации

4.1 Лица, имеющие доступ к носителям ключевой информации, несут за нее персональную ответственность в соответствии с законодательством РФ. Список лиц, имеющих доступ к флеш-накопителям с ключевой информацией, составляется Администратором информационной безопасности Центра информатизации и дистанционных технологий (ЦИДТ) и фиксируется в специальном «Журнале учета выдачи электронной подписи на носителях ключевой информации в казначейство» (приложение А).

4.2 В целях обеспечения идентификации отправителей и получателей информации, защиты ее от несанкционированного доступа:

4.2.1 Назначение ответственного работника ЦИДТ за осуществление электронных взаимодействий со сторонними организациями и наделение его правом установки электронной подписи осуществляется приказом ректора Университета.

4.2.2 Администратор информационной безопасности, по согласованию с директором ЦИДТ назначает работников ЦИДТ, ответственных за установку на автоматизированных рабочих местах (АРМ) соответствующих средств для обеспечения электронных взаимодействий и СКЗИ.

4.3 Контроль за электронными взаимодействиями и использование носителей ключевой информации осуществляют работники ЦИДТ.

5 Порядок изготовления, учета и использования носителей ключевой информации

5.1 Порядок организации и учета носителей ключевой информации

5.1.1 Персональный ключевой носитель (чаще всего – флеш-накопитель) обычно изготавливается в центре управления ключевыми системами (ЦУКС). Если ЦУКС обслуживается сторонней организацией, то ключевые флеш-накопители получаются работником ЦИДТ или назначенным приказом ректора Университета пользователем НКИ.

5.1.2 Генерация уникальной ключевой информации и ее запись на флеш-накопитель осуществляется на специально оборудованном автономном АРМ с наличием криптографической утилиты «Крипто-Про», программное обеспечение которого выполняет функции, регламентированные технологическим процессом формирования ключей электронной цифровой подписи, уполномоченными работниками ЦИДТ в присутствии самого пользователя НКИ, маркируется, учитывается в "Журнале учета выдачи электронной подписи на носителях ключевой информации в казначейство " и выдается ему под роспись. Оснащение АРМ с наличием криптографической утилиты «Крипто-Про» должно гарантировать, что уникальная секретная ключевая информация исполнителя записывается только на его персональный носитель.

5.1.3 Для обеспечения возможности восстановления ключевой информации пользователя НКИ в случае выхода ключевого флеш-накопителя из строя, обычно создается ее рабочая копия. Для того, чтобы при копировании с оригинала на рабочую копию ключевого флеш-накопителя ее содержимое не попадало на какой-либо промежуточный носитель,

копирование должно осуществляться только на "АРМ генерации ключей" уполномоченным работником ЦИДТ.

5.1.4 Ключевые флеш-накопители маркируются этикетками с номерами, присвоенными по «Журналу учета выдачи электронной подписи на носителях ключевой информации в казначейство» (Приложение А).

5.2 Порядок использования носителей ключевой информации

5.2.1 Каждому пользователю, которому в соответствии с его функциональными обязанностями предоставлено право постановки электронной подписи, выдается персональный носитель ключевой информации (например, флеш-накопитель), на который записана уникальная ключевая информация ("секретный ключ электронной подписи"), относящаяся к категории сведений ограниченного распространения.

5.2.2 Персональные ключевые флеш-накопители (рабочие копии) пользователь обязан хранить в специальном пенале-сейфе, который выдается уполномоченным работником ЦИДТ под роспись.

5.2.3 В подразделениях учет и хранение персональных ключевых флеш-накопителей пользователей НКИ осуществляется в установленном порядке самим пользователем НКИ (при наличии у него сейфа или металлического шкафа). Ключевые флеш-накопители хранятся в сейфе пользователя НКИ. В случае отсутствия указанного места для хранения Администратор информационной безопасности обеспечивает необходимые меры по приобретению данного места. Пеналы извлекаются из сейфа только на время приема (выдачи) рабочих копий ключевых флеш-накопителей пользователем.

5.2.4 Контроль за обеспечением безопасности технологии обработки электронных документов, в том числе за действиями пользователей НКИ, выполняющих свою работу с применением персональных ключевых флеш-

накопителей, порядок хранения и использования НКИ осуществляется ежеквартально ответственными работниками ЦИДТ.

6 Права пользователя носителей ключевой информации

6.1 Пользователь НКИ вправе обращаться к Администратору информационной безопасности за консультациями по вопросам использования ключевого флеш-накопителя и по вопросам обеспечения информационной безопасности процесса работы с ключевыми флеш-накопителями.

6.2 Пользователь НКИ вправе требовать от Администратора информационной безопасности создания необходимых условий для выполнения перечисленных выше требований.

6.3 Пользователь НКИ вправе представлять свои предложения по совершенствованию мер защиты на своем рабочем месте.

7 Обязанности пользователя носителей ключевой информации

7.1 Пользователь НКИ, которому в соответствии с его должностными функциями предоставлено право постановки электронной подписи, несет персональную ответственность за сохранность и правильное использование вверенной ему ключевой информации и содержание документов, на которых стоит его ЭП.

7.2 Пользователь носителей ключевой информации обязан:

- Лично присутствовать при изготовлении своей ключевой информации, чтобы быть уверенным в том, что содержание его ключевых флеш-накопителей (оригинала и копии) не компрометировано.
- Под роспись в «Журнале учета выдачи электронной подписи на носителях ключевой информации в казначейство» получить рабочую копию ключевого флеш-накопителя, убедиться, что он правильно маркирован и на нем установлена защита от записи.
- Использовать для работы только рабочую копию ключевого флеш-накопителя.
- В случае хранения НКИ у Администратора информационной безопасности, в начале рабочего дня получать, а в конце рабочего дня сдавать Администратору информационной безопасности свой ключевой флеш-накопитель. При первом вскрытии пенала, обязан убедиться в целостности и подлинности печати на пенале. Если печать на пенале нарушена, то флеш-накопитель считается скомпрометированным.
- В случае хранения персонального ключевого флеш-накопителя в сейфе пользователя НКИ, доставать ключевой флеш-накопитель из сейфа по необходимости и при первом вскрытии пенала убедиться в целостности и подлинности опечатывания. Если опечатывание нарушено, то флеш-накопитель считается скомпрометированным.

– По окончании рабочего дня убирать ключевой флеш-накопитель в пенал. Пенал должен быть опечатан и убран в сейф.

– В случае порчи рабочей копии ключевого флеш-накопителя (например, при ошибке чтения флеш-накопителя) передать его уполномоченному работнику ЦИДТ, который должен в присутствии пользователя НКИ или администратора информационной безопасности сделать новую копию ключевого флеш-накопителя.

7.3 Пользователю носителей ключевой информации запрещается:

7.3.1 оставлять ключевой флеш-накопитель в компьютере. После использования персональной ключевого флеш-накопителя для подписи или шифрования исполнитель должен убрать флеш-накопитель в сейф, а в случае хранения НКИ у администратора информационной безопасности, сдавать свой персональный ключевой флеш-накопитель на временное хранение администратору информационной безопасности.

7.3.2 оставлять персональный ключевой флеш-накопитель без личного присмотра где бы то ни было;

7.3.3 передавать свой персональный ключевой флеш-накопитель другим лицам (кроме как для хранения администратору информационной безопасности в опечатанном пенале);

7.3.4 делать неучтенные копии ключевого флеш-накопителя, распечатывать или переписывать с нее файлы на иной носитель информации, вносить изменения в файлы, находящиеся на ключевом флеш-накопителе;

7.3.5 использовать персональный ключевой флеш-накопитель на заведомо неисправном персональном компьютере;

7.3.6 подписывать своим персональным "секретным ключом ЭП" любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;

7.3.7 сообщать кому-либо вне работы, что он является владельцем "секретного ключа ЭП" для данного технологического процесса.

8 Порядок действий при компрометации носителей ключевой информации

8.1 К событиям, связанным с компрометацией ключевой информации, относится:

- утрата ключевого флеш-накопителя;
- утрата ключевого флеш-накопителя с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажения в системе связи;
- нерасшифровывание входящих или исходящих сообщений у абонентов;
- нарушение печати на сейфе или контейнере с ключевым флеш-накопителем.

8.2 Первые три события должны трактоваться как безусловная компрометация действующих ключей ЭП. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

8.2.1 При выявлении компрометации НКИ пользователь при обмене электронными документами немедленно:

- прекращает передачу информации с использованием скомпрометированных ключей ЭП или шифрования;
- сообщает о факте компрометации в ЦИДТ администратору информационной безопасности.

8.2.2 Администратор информационной безопасности ЦИДТ на основании извещения пользователя при обмене электронными документами исключает из электронной базы открытых ключей скомпрометированный

ключ ЭП или исключает криптографический номер Участника обмена электронными документами из списка абонентов.

8.2.3 В случае крайней необходимости пользователь при обмене электронными документами после компрометации может продолжить работу на резервных ключах. Информация о выдаче резервного ключа фиксируется в «Журнале учета выдачи электронной подписи на носителях ключевой информации в казначейство».

8.2.4 Пользователь при обмене Электронными документами подает заявку на изготовление нового ключа в ЦУКС и получает там новые ключи ЭП и шифрования с регистрацией в «Журнале учета выдачи электронной подписи на носителях ключевой информации в казначейство».

8.2.5 Работник ЦИДТ производит обмен тестовыми сообщениями на новых ключах ЭП и шифрования.

9 Обеспечение информационной безопасности при работе с носителями ключевой информации

9.1 Порядок размещения специального оборудования, охраны и режима в помещениях, в которых находятся средства криптографической защиты и носители ключевой информации:

- средства криптографической защиты для обслуживания носителей ключевой информации размещаются в помещениях Университета и ЦИДТ;
- размещение специального оборудования и режим в помещениях, в которых размещены средства криптографической защиты и носители ключевой информации обеспечивают: безопасность информации, средств криптографической защиты и ключевой информации, сведение к минимуму возможности неконтролируемого доступа к средствам криптографической защиты, просмотр процедур работы со средствами криптографической защиты посторонними лицами;
- порядок допуска в помещения определяется внутренним распоряжением ректора;
- для хранения ключевых флеш-накопителей, нормативной и эксплуатационной документации, инсталляционных флеш-накопителей помещения обеспечиваются сейфами;
- установленный порядок охраны помещений предусматривает периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны;
- размещение и установка средств криптографической защиты осуществляется в соответствии с требованиями документации на средства криптографической защиты;
- системные блоки ПК со средствами криптографической защиты оборудованы средствами контроля их вскрытия.

9.2 Порядок обеспечения безопасности хранения ключевых флеш-накопителей:

– учет и хранение носителей ключей шифрования и инсталляционных флеш-накопителей, непосредственная работа с ними поручается работникам ЦИДТ или ответственным работникам, назначенным приказом по Университету. На этих работников возлагается персональная ответственность за сохранность ключей шифрования;

– учет изготовленных для пользователей ключей шифрования, регистрация их выдачи для работы, возврата от пользователей и уничтожение ведется работниками ЦИДТ;

– хранение ключей шифрования, ключей ЭП, инсталляционных флеш-накопителей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, непредусмотренное правилами пользования систем криптозащиты, применение;

– безопасное раздельное хранение рабочих и резервных ключей, предназначенных для использования в случае компрометации рабочих ключей в соответствии с правилами пользования средств криптографической защиты;

– действующий закрытый ключ ЭП, записанный на флеш-накопитель, хранится в личном, опечатываемом сейфе (контейнере) пользователя НКИ, для исключения возможности копирования и несанкционированного использования ЭП посторонним лицом;

– резервный ключ ЭП должен хранится так же, как и действующий, но обязательно в отдельном опечатанном контейнере.

9.3 Требования к работникам, осуществляющим эксплуатацию и установку (инсталляцию) средств криптографической защиты и носителей ключевой информации:

– к работе со средствами криптографической защиты и носителям ключевой информации допускаются только работники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПК, изучившие правила пользования и эксплуатационную документацию ЦУКС по средствам криптографической защиты;

– работник должен знать о возможных угрозах информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

9.4 Ответственность работников, осуществляющих эксплуатацию и установку (инсталляцию) средств криптографической защиты и носителей ключевой информации:

– работники Университета, осуществляющие эксплуатацию и установку ЭП при работе с ключевыми документами руководствуются положениями соответствующего Регламента ЦУКС и настоящей инструкцией и несут персональную ответственность за невыполнение требований руководящих документов.

– работники ЦИДТ при установке ЭП проводят инструктаж по эксплуатации и хранению НКИ пользователям НКИ.

Приложение А
(обязательное)

Форма «Журнала учета выдачи электронной подписи на носителях ключевой информации в казначейство»

ФГБОУ ВО СПбГАУ

Журнал учета выдачи электронной подписи на носителях ключевой информации в казначейство

Журнал начат «____» _____ 201_ г.
Должность
_____/ _____ /
подпись *фамилия, имя, отчество*
Журнал завершен «____» _____ 201_ г.
Должность
_____/ _____ /
подпись *фамилия, имя, отчество*
Журнал составлен на _____ листах

№ п/п	Наименование электронного идентификатора	Серийный, учетный номер электронного идентификатора	Дата выдачи	ФИО, должность		Подпись		Дата возврата	Подпись		Примечание
				ответственного лица	получившего лица	ответственного лица	получившего лица		ответственного лица	получившего лица	
1	2	3	4	5	6	7	8	9	10	11	

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	*Фамилия И.О.*	*Должность*	*Дата*	*Подпись*