*Федеральное агентство по рыболовству*
*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования*
*«Астраханский государственный технический университет»*


# П Р И К А З

16.10 2014 г. Астрахань №286

об утверждении Регламента по обеспечению безопасности использования сотрудниками ФГБОУ ВПО «АГТУ» электронной подписи

В целях определения порядка работы с электронной подписью и обеспечения безопасности при работе с ней сотрудников Университета, включая обособленное структурное подразделение и филиалы, в соответствии с Федеральным законом № 63 «Об электронной подписи»

**П Р И К А З Ы В А Ю**:

1. Утвердить «Регламент по обеспечению безопасности использования сотрудниками ФГБОУ ВПО «АГТУ» электронной подписи», представленный в Приложении к приказу (далее - Регламент).

2. Начальнику отдела кадров Любиш Н.М. обеспечить заключение дополнительных соглашений (Приложение 8 Регламента) с лицами, допущенными к работе с электронной подписью, согласно приказу №604-Т от 07.10.2014г. «О наделении сотрудников правом владения электронной подписью для информационных систем финансового контура Университета».

3. Директорам филиалов и обособленного структурного подразделения АГТУ обеспечить заключение дополнительных соглашений (Приложение 8 Регламента) с лицами, допущенными к работе с электронной подписью, согласно приказу ректора №604-Т от 07.10.2014г. «О наделении сотрудников правом владения электронной подписью для информационных систем финансового контура Университета», а также в соответствии с приказами по филиалам и обособленному структурному подразделению о назначении ответственных лиц за осуществление обмена информацией.

4. Начальнику общего отдела Типаковой Н.Ю. довести содержание данного приказа в электронном виде до сведения заинтересованных лиц, а также лиц, указанных в приказе №604-Т от 07.10.2014г. «О наделении сотрудников правом владения электронной подписью для информационных систем финансового контура Университета».

5. Контроль за исполнением приказа возложить на начальника Управления информационных систем и технологий Кучина И.Ю.

Ректор, профессор А.Н. Неваленный

**Приложение к приказу №286 от «16» 10. 2014г.**

*Федеральное агентство по рыболовству*
*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования*
*«Астраханский государственный технический университет»*



**УТВЕРЖДАЮ**

Ректор ФГБОУ ВПО «АГТУ»

_____ А.Н. Неваленный

«10» _____ 2014г.

# РЕГЛАМЕНТ
## по обеспечению безопасности использования сотрудниками ФГБОУ ВПО «АГТУ» электронной подписи

**Астрахань, 2014**

## СОДЕРЖАНИЕ

## 1. Список сокращений

| | |
|---|---|
| **АРМ** | автоматизированное рабочее место |
| **ИБ** | информационная безопасность |
| **ОС** | операционная система |
| **ОСП** | обособленное структурное подразделение |
| **СКЗИ** | средство криптографической защиты информации |
| **УИСиТ** | Управление информационных систем и технологий |
| **Университет, ФГБОУ ВПО «АГТУ»** | Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный технический университет» |
| **ЭД** | электронный документооборот |
| **ЭП** | электронная подпись |

## 2. Термины и определения

**Автоматизированное рабочее место** – комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обработки данных.

**Администратор безопасности информации ОСП/филиала** – уполномоченное лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами в ОСП/филиале.

**Администратор безопасности информации Университета** – уполномоченное лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами в Университете, начальник отдела Информационной безопасности УИСиТ.

**Владелец сертификата ключа проверки ЭП** – лицо, которому в установленном Федеральным законом № 63 «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

**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 электронной подписи** – уникальная последовательность символов, предназначенная для создания электронной подписи.

**Компрометация** – факт доступа или подозрение на получение доступа постороннего лица к защищаемой информации (закрытого ключа, закрытого алгоритма, цифрового сертификата, учётных записей (паролей)).

**Криптоноситель** – съемный носитель, содержащий ключ электронной подписи.

**Пакет электронных документов** – совокупность одного или нескольких электронных документов, служащих для перемещения заключенной в нем информации.

**Сертификат ключа проверки электронной подписи** – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

**Средства криптографической защиты информации** – средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы.

**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.

**Удостоверяющий центр** – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом № 63 «Об электронной подписи».

**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.

**Электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

## 3. Общие положения

3.1. Настоящий Регламент по обеспечению безопасности использования сотрудниками ФГБОУ ВПО «АГТУ» электронной подписи (далее – Регламент) разработан в

соответствии с Федеральным законом № 63 «Об электронной подписи», нормативно-правовыми документами, регламентирующими отношения в сфере деятельности по защите информации с использованием криптографических (шифровальных) средств.

3.2. Цель разработки Регламента – определение порядка работы с электронной подписью и обеспечения безопасности при работе с ней, плановой и внеплановой смены сертификата электронной подписи работников ФГБОУ ВПО «АГТУ», включая ОСП и филиалы, и закрепление ответственности за сотрудниками, работающими с электронной подписью, за невыполнение требований норм, регулирующих электронное взаимодействие.

3.3. Применение электронных подписей в системах юридически значимого электронного документооборота и иных системах сопровождается рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием электронной подписи при несанкционированном получении злоумышленником ключа электронной подписи. В связи с этим необходимо выполнение приведенных в настоящем Регламенте организационно-технических и административных мер по обеспечению правильного функционирования средств обработки, передачи и защиты информации.

3.4. Регламент обязателен для исполнения всеми сотрудниками Университета, включая ОСП и филиалы, работающими с электронной подписью.

## 4. Порядок работы с электронной подписью

4.1. Перечень лиц, которые могут выступать в качестве участников электронного документооборота с использованием ЭП, определяется приказом ректора Университета или директора ОСП/филиала.

4.2. Администратор безопасности информации ОСП/филиала назначается приказом директора ОСП/филиала. Все действия по сопровождению систем электронной подписи администратор безопасности информации ОСП/филиала согласовывает с администратором безопасности информации Университета.

4.3. За техническое сопровождение АРМ с установленными средствами электронной подписи и средствами криптографической защиты в Университете отвечает УИСиТ.

4.4. С каждым сотрудником Университета и ОСП/филиала, являющимся участником электронного документооборота с использованием ЭП, заключается дополнительное соглашение к трудовому договору в двух экземплярах. Образец дополнительного соглашения приведен в Приложении 8. Один экземпляр дополнительного соглашения хранится в личном деле работника в отделе кадров, второй экземпляр – у сотрудника.

4.5. При использовании электронных подписей сотрудники Университета и ОСП/филиала, являющиеся участниками электронного документооборота с использованием ЭП, обязаны:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих ему ключей электронных подписей другим лицам без своего согласия (см. п.4.8);
- хранить криптоноситель в запираемом железном шкафу или сейфе;
- соблюдать «политику чистого стола»: при завершении работы с электронной подписью либо при необходимости покинуть помещение, криптоноситель должен быть убран в соответствующий железный шкаф или сейф;
- соблюдать парольную политику (см. п. 4.7);
- при вводе пароля исключать возможность его подсматривания посторонними лицами и/или техническими средствами (стационарными и/или встроенными в мобильные телефоны видеокамерами и т.п.);
- при необходимости покинуть рабочее место выполнять завершение или блокировку сеанса работы операционной системы;
- бережно относиться к криптоносителю, исключая механические повреждения;
- в случае повреждения криптоносителя либо при его некорректной работе сообщать об этом факте администратору безопасности информации Университета.

4.6. Сотрудникам Университета и ОСП/филиала, являющимся участниками электронного документооборота с использованием ЭП, запрещается:

- оставлять АРМ с установленными средствами электронной подписи и средствами криптографической защиты без контроля после ввода ключевой информации;
- вносить какие-либо изменения в программное обеспечение средств электронной подписи и средств криптографической защиты;
- осуществлять несанкционированное копирование криптоносителя;
- разглашать содержимое криптоносителя или передавать его посторонним, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- записывать на криптоноситель постороннюю информацию;
- хранить пароли в легкодоступных местах (на рабочем столе и т.п.), а также совместно с криптоносителем;

— сообщать другим лицам личный пароль и регистрировать их на АРМ под своим паролем;

— осуществлять несанкционированное вскрытие корпуса АРМ с установленными средствами электронной подписи и средствами криптографической защиты;

— использовать криптоноситель при компрометации ключа подписи (см. пп.4.12-4.13).

4.7. Парольная политика (пароль для входа в личные кабинеты систем электронного документооборота, пароль на криптоноситель) определяется следующими требованиями:

— длина пароля должна быть не менее 6 символов;

— в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.);

— при смене ЭП новое значение пароля на криптоноситель должно отличаться от предыдущего не менее чем в 4 позициях.

4.8. В случае необходимости передачи права использования ключа ЭП владельцем ключа ЭП:

1) приказом ректора Университета или директора ОСП/филиала назначается уполномоченное лицо, ответственное за использование ЭП и надлежащее хранение криптоносителя согласно настоящему Регламенту;
2) владельцем сертификата ключа проверки ЭП заполняется согласие на передачу прав использования ключа ЭП (Приложение 2). Один экземпляр согласия хранится в личном деле владельца сертификата ключа проверки ЭП в отделе кадров, второй экземпляр – у владельца, а третий экземпляр – у назначенного приказом ответственного лица.
3) назначенное приказом лицо заполняет обязательство уполномоченного лица (Приложение 3). Перечень выполняемых функций ответственным лицом при использовании ЭП определяется в согласии владельца сертификата ключа проверки ЭП и в обязательстве уполномоченного лица. Один экземпляр обязательства хранится в личном деле уполномоченного лица в отделе кадров, второй экземпляр – у уполномоченного лица, а третий экземпляр – у владельца.

Владелец сертификата ключа проверки ЭП имеет право отозвать согласие на передачу прав использования ключа ЭП до окончания срока действия согласия. В случае необходимости отзыва согласия до окончания срока действия согласия и/или

сертификата ключа проверки ЭП (например, по желанию владельца ключа ЭП или в случае увольнения уполномоченного лица) владельцу сертификата ключа проверки ЭП необходимо незамедлительно осуществить отзыв и получение нового сертификата ключа проверки электронной подписи в Удостоверяющем центре, выдавшим сертификат. Для этого необходимо выполнить действия, указанные в пункте 4.13.

4.9. Администратор безопасности информации Университета и ОСП/филиала обязан:

— производить установку сертификата ключа проверки ЭП, средств проверки электронной подписи и средств криптографической защиты;

— контролировать сроки окончания действия сертификата ключа проверки ЭП пользователей.

4.10. Администратор безопасности информации Университета и ОСП/филиала обязан вести следующие журналы:

— Журнал учета носителей ключевой информации ЭП (Приложение 4);

— Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение 5);

— Журнал регистрации сертификатов ключей проверки ЭП (Приложение 6);

— Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ (Приложение 7).

4.11. Порядок получения и плановой смены ЭП определяется регламентами, разработанными соответствующим удостоверяющим центром, производящим выдачу ЭП. Сотрудники Университета и ОСП/филиала, являющиеся участниками электронного документооборота с использованием ЭП, обязаны руководствоваться требованиями настоящего Регламента, а также требованиями инструкций по обеспечению безопасности информации соответствующего Удостоверяющего центра.

4.12. Сертификат ключа проверки ЭП должен быть отозван его владельцем в следующих случаях:

— компрометация ключа ЭП;

— прекращение или изменение полномочий владельца сертификата ключа проверки ЭП;

— отзыв согласия на передачу прав использования ключа ЭП уполномоченному лицу до окончания срока действия согласия и/или сертификата ключа проверки ЭП (например, по желанию владельца или в случае увольнения уполномоченного лица).

4.13. Порядок действий сотрудников Университета и ОСП/филиала, являющихся участниками электронного документооборота с использованием ЭП, при отзыве ключа ЭП:

— немедленно прекратить работу с ЭП;

— незамедлительно уведомить Удостоверяющий центр, выдавший сертификат ключа проверки электронных подписей.

## 5. Заключительные положения

5.1. Сотрудники Университета, являющиеся участниками электронного документооборота с использованием ЭП, не выполняющие требования настоящего Регламента, привлекаются к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

5.2. Ответственность за поддержание настоящего Регламента в актуальном состоянии несет отдел Информационной безопасности УИСиТ ФГБОУ ВПО «АГТУ».

5.3. В случае изменения действующего законодательства и иных нормативных актов настоящий Регламент и изменения к нему применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае отдел Информационной безопасности УИСиТ ФГБОУ ВПО «АГТУ» обязан инициировать внесение соответствующих изменений.

**Приложение 1**

к Регламенту по обеспечению безопасности
использования сотрудниками ФГБОУ ВПО «АГТУ»
электронной подписи
«16» 10 2014 г.

# Требования к обеспечению защиты от несанкционированного доступа АРМ с установленными средствами ЭП и средствами криптографической защиты

1. Настоящие требования обязательны для выполнения администраторами безопасности информации Университета и ОСП/филиала, а также структурными подразделениями УИСиТ, занимающимися техническим сопровождением АРМ с установленными средствами ЭП и средствами криптографической защиты.
2. Все действия по обеспечению защиты от несанкционированного доступа АРМ с установленными средствами ЭП, в том числе выбор средств защиты информации, администратор безопасности информации ОСП/филиала согласовывает с администратором безопасности информации Университета.
3. Правом установки и настройки средств ЭП и средств криптографической защиты должен обладать только администратор безопасности информации Университета и ОСП/филиала.
4. Системные блоки АРМ с установленными средствами ЭП и средствами криптографической защиты должны быть опечатаны. При опечатывании и вскрытии системных блоков АРМ соответствующие записи должны быть занесены в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ».
5. При использовании средств электронной подписи и средств криптографической защиты должны выполняться следующие меры по защите информации от несанкционированного доступа:
   5.1. Необходимо соблюдать парольную политику (для входа в операционную систему, BIOS и т.д.):
   — длина пароля должна быть не менее 6 символов;
   — в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также общепринятые и распространенные сочетания (USER, ADMIN, root, и т.д.);

— при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

— периодичность смены пароля не должна превышать 90 дней.

5.2. Сотрудники структурных подразделений, занимающихся техническим сопровождением АРМ с установленными средствами ЭП и средствами криптографической защиты, должны сконфигурировать операционную систему и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

— не использовать нестандартные, измененные или отладочные версии операционных систем;

— исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

— исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

— на АРМ с установленными средствами электронной подписи и средствами криптографической защиты должна быть установлена только одна операционная система;

— все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

— всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

— необходимо предусмотреть меры, максимально ограничивающие доступ к системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации (пароли и т.п.), отладочной информации;

— должно быть установлено лицензионное антивирусное программное обеспечение;

— необходимо регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы;

— необходимо настроить подсистему регистрации событий информационной безопасности и организовать регулярный анализ результатов аудита.

5.3. С целью контроля исходящего и входящего подозрительного трафика, АРМ с установленными средствами электронной подписи и средствами криптографической защиты должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в Интернет информации, инициированную программами, не имеющими соответствующих полномочий.