Приложение №1
к приказу №360 от «20» 10. 2015г.

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

УТВЕРЖДАЮ
Ректор ФГБОУ ВПО «АГТУ»,
профессор
_____ А.Н.Неваленный
«20» 10 2015г.

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите конфиденциальной информации в ФГБОУ ВПО «Астраханский государственный технический университет»

Астрахань, 2015

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по защите конфиденциальной информации (далее - Положение) в ФГБОУ ВПО «Астраханский государственный технический университет» (далее - Университет) определяет основные принципы, организацию, порядок осуществления работ по защите информации, основные требования и рекомендации, способы и средства защиты циркулирующей в Университете конфиденциальной информации, не содержащей сведения, составляющие государственную тайну (далее - конфиденциальная информация).

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера», Гражданским кодексом Российской Федерации (в частности ст. 771) и другими нормативно-методическими документами по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

1.3. Целью настоящего Положения является:

— укрепление механизмов правового регулирования отношений в области защиты конфиденциальной информации;

— создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

— защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых.

1.4. Настоящее Положение содержит основные требования по защите конфиденциальной информации. Требования остальных документов, касающихся вопросов обработки и защиты конфиденциальной информации, в том числе персональных данных, не должны противоречить требованиям настоящего Положения.

1.5. Порядок организации и проведения работ по защите персональных данных определен Положением об обработке и защите персональных данных работника ФГБОУ ВПО «АГТУ», а также Положением об обработке и защите персональных данных абитуриентов и обучающихся в ФГБОУ ВПО «АГТУ».

2. Термины и определения

Для целей настоящего Положения используются следующие основные понятия:

2.1. **Автоматизированная обработка конфиденциальной информации** – обработка конфиденциальной информации с помощью средств вычислительной техники.

2.2. **Автоматизированная система (АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.3. **Аттестация объекта информатизации по требованиям безопасности информации** – комплекс организационно-технических мероприятий, в результате которых посредством выдачи специального документа «Аттестата соответствия» подтверждается, что на аттестационном объекте выполнены требования по безопасности информации, заданные в нормативно-технической документации, утвержденные государственными органами обеспечения безопасности информации и контролируемые при аттестации.

2.4. **Доступ к конфиденциальной информации Университета** – процедура ознакомления полномочным должностным лицом Университета определенных лиц со сведениями, составляющими конфиденциальную информацию Университета.

2.5. **Защищаемые помещения (ЗП)** – помещения, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

2.6. **Информационный ресурс** – различная информация Университета на всех этапах ее жизненного цикла, обеспечивающая основную деятельность Университета и представляющая ценность с точки зрения поставленных целей.

2.7. **Контролируемая зона (КЗ)** – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

2.8. **Конфиденциальная информация** – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

2.9. **Неавтоматизированная обработка конфиденциальной информации** – обработка конфиденциальной информации без помощи средств вычислительной техники.

2.10. **Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

2.11. **Разглашение сведений, составляющих конфиденциальную информацию,** – передача в устной, письменной, электронной или иной форме, раскрытие и подобные действия, совершенные пользователем умышленно или по неосторожности, включая халатное отношение к своим должностным обязанностям, повлекшие ознакомление со сведениями, относящихся к конфиденциальной информации Университета, любых лиц, не имеющих права доступа на законном основании к указанным сведениям.

2.12. **Служебная информация ограниченного распространения** – конфиденциальная информация, образующаяся в процессе управленческой деятельности Университета, распространение которых препятствует реализации Университетом предоставленных ему полномочий, либо иным образом отрицательно сказывается на их реализации.

2.13. **Средство вычислительной техники (СВТ)** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

2.14. **Техническая защита информации** – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

3. Сведения конфиденциального характера Университета

3.1. Отнесение информации к конфиденциальной осуществляется в соответствии с Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера».

3.2. Перечень сведений конфиденциального характера утверждается приказом Университета.

4. Организационные и технические мероприятия по защите информации

4.1. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения, в Университете определен Инструкцией о порядке обращения со служебной информацией ограниченного распространения.

4.2. Защита конфиденциальной информации осуществляется путем выполнения комплекса мероприятий (правовых, организационных, технических) по предотвращению утечки информации по техническим каналам, от несанкционированного доступа (далее – НСД), предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, а также путем выполнения специальных работ, порядок организации и выполнения которых определяется Правительством РФ и федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности.

4.3. Лица, осуществляющие обработку информации конфиденциального характера на средствах вычислительной техники (далее - СВТ), обязаны соблюдать требования законодательства Российской Федерации, а также локальных нормативных документов Университета в части обработки конфиденциальной информации и вопросов обеспечения безопасности информации.

4.4. Для обработки конфиденциальной информации необходимо использовать СВТ с применением сертифицированных программных, технических и программно-технических средств защиты информации. Применяемое на СВТ программное обеспечение должно быть лицензионным.

4.5. Для передачи конфиденциальной информации по линиям связи за пределы Университета необходимо использовать защищенные каналы связи с применением сертифицированных по требованиям безопасности информации криптографических средств защиты информации.

4.6. Межсетевое взаимодействие с другими локально-вычислительными сетями с выходом в сеть общего пользования типа «Интернет» осуществляется только после установки на СВТ или АС средств защиты информации от НСД, межсетевого экрана и проведения аттестационных испытаний СВТ (АС) с целью официального подтверждения эффективности применяемых мер и средств защиты информации, отвечающих требованиям «СТР-К» и другим нормативным документам.

4.7. Для обеспечения физической безопасности конфиденциальной информации, циркулирующей в ЛВС, осуществляются следующие мероприятия:

— ограничение доступа посторонних лиц к серверам и прочим компонентам инфраструктуры автоматизированной системы;
— резервное копирование конфиденциальной информации;
— периодический контроль ресурсов;
— обеспечение компонентов инфраструктуры автоматизированной системы источниками бесперебойного питания.

5. Порядок аттестации и ввода в эксплуатацию объектов информатизации

5.1. Аттестация по требованиям безопасности информации является необходимым условием для ввода в эксплуатацию объектов информатизации, предназначенных для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров, а также государственных информационных систем.

5.2. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе владельца объекта информатизации.

5.3. Аттестация объектов информатизации осуществляется организациями, имеющими лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации или сотрудниками Университета при условии наличия соответствующей лицензии.

5.4. Для проведения аттестационных испытаний подготавливаются документы:

— Технический паспорт, включающий состав технических и программных средств, планы размещения основных и вспомогательных технических средств и систем, состав и схемы размещения средств защиты информации, план контролируемой зоны;
— Акт классификации автоматизированной системы;
— Перечень защищаемых ресурсов;
— Организационно-распорядительная документация;
— Разрешительная система доступа к защищаемым ресурсам;
— Инструкции пользователям и администратору безопасности информации;
— Инструкции по эксплуатации средств защиты информации;
— Сертификаты соответствия требованиям по безопасности информации и формуляры на используемые средства защиты информации.

5.5. Аттестационные испытания объекта информатизации проводятся в соответствии с программой и методиками испытаний.

5.6. На основании выданного специализированной организацией аттестата соответствия издается приказ о разрешении обработки конфиденциальной информации на объекте информатизации и назначении лиц, ответственных за обеспечение защиты информации при его эксплуатации.

5.7. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации, указывается в Аттестате соответствия.

6. Контроль состояния защищенности информации

6.1. С целью обеспечения единой дисциплины в организации работ по защите конфиденциальной информации, своевременного выявления предпосылок и предотвращения утечки информации по техническим каналам, НСД и непреднамеренных воздействий на информацию и средства ее обработки проводится периодический контроль состояния защиты информации. Контроль защиты информации осуществляется сотрудниками отдела информационной безопасности Управления информационных систем и технологий и заключается в оценке:
— соблюдения нормативных и методических документов ФСТЭК России;
— работоспособности применяемых средств защиты информации в соответствии с их эксплутационной документацией;
— знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

6.2. Повседневный контроль организационных и технических мероприятий, направленных на обеспечение защиты информации, осуществляется руководителями соответствующих структурных подразделений.

6.3. К контролю эффективности мероприятий могут привлекаться сотрудники проверяемых отделов.

6.4. Результаты проверок отражаются в техническом паспорте объектов информатизации.

6.5. По результатам проверок руководители заинтересованных структурных подразделений и должностные лица, ответственные за организацию работ по защите информации, разрабатывают план выработки недостатков.

7. Планирование работ по защите информации и контролю защиты информации

7.1. Планирование мероприятий по защите информации проводится на основании:
— Рекомендаций актов проверок контрольными органами ФСТЭК России, ФСБ России, Роскомнадзора России;
— Результатов контроля состояния защищенности конфиденциальной информации.

7.2. Для подготовки и реализации организационных и технических мероприятий по защите информации составляется годовой план работ отдела информационной безопасности, в котором указываются:
- Планируемые работы по защите информации и контролю ее эффективности;
- Подразделения и должностные лица, отвечающие за выполнение указанных работ, исполнители этих работ и отвечающие за контроль;
- Материально-техническое обеспечение;
- Сроки выполнения работ, отметка о выполнении.

8. Обязанности и права должностных лиц

8.1. Должностные лица, ответственные за организацию работ по защите информации, имеют право:
- контролировать исполнение приказов и распоряжений ректора Университета по вопросам обеспечения безопасности информации;
- требовать от руководителей проверяемых структурных подразделений устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения информационной безопасности;
- требовать от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- запрещать эксплуатацию систем обработки и передачи информации при несоблюдении требований по защите информации.

8.2. Сотрудникам, имеющим доступ к конфиденциальной информации, запрещается:
- обрабатывать конфиденциальную информацию на СВТ, не оснащенных средствами защиты информации, при отключении или некорректно работающих средствах защиты информации;
- использовать конфиденциальную информацию в личных целях;
- использовать для передачи конфиденциальной информации незащищенные каналы связи;
- передавать конфиденциальную информацию лицам, не имеющим права доступа к указанным сведениям;
- выносить носители конфиденциальной информации за пределы контролируемой зоны, без согласования с руководством Университета;
- делать записи, расчеты, заметки, содержащие конфиденциальную информацию, в личных тетрадях, блокнотах и иных неучтенных носителях.

8.3. Сотрудники, имеющие доступ к конфиденциальной информации, обязаны:
- строго соблюдать требования по защите информации и правила эксплуатации СВТ;
- обеспечивать сохранность машинных носителей информации и целостность установленного программного обеспечения;
- знать и соблюдать установленные требования по учету, хранению и пересылке машинных, бумажных и иных носителей информации;
- при начале обработки конфиденциальной информации убедиться в работоспособности средств защиты информации;
- применять антивирусные средства при использовании съемных носителей информации.

8.4. Руководители структурных подразделений:
- отвечают за защиту информации в структурном подразделении, сохранность машинных и иных носителей информации;
- организует выполнение мероприятий по защите конфиденциальной информации при использовании технических средств;

— участвует в определении правил разграничения доступа к информации в используемых объектах информатизации;
— согласовывает с начальником отдела информационной безопасности установку, замену и перемещение технических средств на аттестованных объектах информатизации.

8.5. Обо всех фактах и попытках нарушения безопасности конфиденциальной информации сотрудники Университета обязаны ставить в известность непосредственного руководителя или отдел информационной безопасности.

9. Ответственность за нарушение режима конфиденциальности

9.1. При приеме на работу каждый работник предупреждается об ответственности за разглашение сведений конфиденциального характера, ставших ему известными в связи с выполнением им своих трудовых обязанностей.

9.2. Допуск к конфиденциальной информации осуществляется только после ознакомления и подписания работником Обязательства о соблюдении требований при обработке конфиденциальной информации, представленного в Приложении 1 к настоящему Положению.

9.3. Работники Университета, имеющие доступ к конфиденциальной информации, несут персональную ответственность в соответствие с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования конфиденциальной информации.

9.4. Работники Университета, виновные в нарушении норм, регулирующих получение, обработку и защиту конфиденциальной информации, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствие с законодательством Российской Федерации.

9.5. Если действиями (бездействием) работника, связанными с нарушением правил обращения с конфиденциальной информацией, причинен материальный ущерб, возмещение ущерба производится в порядке, предусмотренном законодательством Российской Федерации и трудовым договором.

9.6. Контроль над выполнением норм, регулирующих получение, обработку и защиту конфиденциальной информации, возлагается на руководство Университета, должностных лиц, ответственных за организацию работ по защите информации, руководителей структурных подразделений, в которых осуществляется обработка конфиденциальной информации.

9.7. По фактам разглашения конфиденциальной информации руководителем структурного подразделения назначается служебное расследование.

Приложение 1
к Положению о порядке организации и проведения работ по защите конфиденциальной информации в ФГБОУ ВПО «Астраханский государственный технический университет»
«____» _____ 2015г.

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации, в том числе персональных данных

Я, _____
(фамилия, имя, отчество)

занимающий (ая) должность _____
(полное наименование должности и структурного подразделения)

_____

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией и Положением о порядке организации и проведения работ по защите конфиденциальной информации в ФГБОУ ВПО «АГТУ», Положением об обработке и защите персональных данных работника ФГБОУ ВПО «АГТУ», об обработке и защите персональных данных абитуриентов и обучающихся в ФГБОУ ВПО «АГТУ» (далее – Положения) мне может быть предоставлен допуск к информации, содержащей сведения конфиденциального характера, в том числе персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. принимать меры в пределах своих полномочий по сохранности сведений конфиденциального характера, ставших мне известными в связи с выполнением своих трудовых обязанностей;
2. во время работы в Университете и в течение 3-х лет после увольнения не раскрывать (не передавать) третьим лицам, в том числе другим работникам структурных подразделений, ставшие мне известными конфиденциальные сведения, за исключением случаев, когда это вызвано служебной необходимостью, при соблюдении установленных требований и правил;
3. не использовать ставшие мне известными конфиденциальные сведения с целью получения выгоды;
4. соблюдать указанные в указанных выше Положениях требования и правила обеспечения безопасности информации;
5. в случае попытки третьих лиц получить от меня информацию, содержащую сведения конфиденциального характера, в том числе персональные данные, сообщать об этом непосредственному руководителю, а также в отдел информационной безопасности Управления информационных систем и технологий;
6. в случае прекращения работы в Университете возвратить все документы и другие материалы, содержание которых отнесено к сведениям конфиденциального характера, полученные в ходе выполнения служебных обязанностей;
7. выполнять требования нормативных правовых актов, а также локальных организационно-распорядительных документов, регламентирующих вопросы защиты конфиденциальной информации, в том числе персональных данных.

Я ознакомлен(а) с Положением о порядке организации и проведения работ по защите конфиденциальной информации в ФГБОУ ВПО «АГТУ», Положением об обработке и защите персональных данных работника ФГБОУ ВПО «АГТУ», об обработке и защите персональных данных абитуриентов и обучающихся в ФГБОУ ВПО «АГТУ».
Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен к дисциплинарной, уголовной, гражданской ответственности, и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____

Дата Личная подпись Расшифровка подписи

Приложение №2
к приказу №360 от «20» 10 2015г.

Лист ознакомления с Положением о порядке организации и проведения работ по защите конфиденциальной информации в ФГБОУ ВПО «Астраханский государственный технический университет»

ФИО	Должность	Подпись	Дата ознакомления