Приложение № 2
к приказу от 01.08.18 № 253
ФГБОУ ВО Уральский ГАУ

Утверждаю:
Ректор ФГБОУ ВО Уральский ГАУ
_____ О.Г. Лоретц
«___»_____ 2018 г.

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите персональных данных (ПДн) в ФГБОУ ВО Уральский ГАУ.

1.2. Мероприятия по защите ПДн в ФГБОУ ВО Уральский ГАУ, являются составной частью управленческой и иной служебной деятельности его работников, и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Информационные системы и ресурсы, касающиеся обработки ПДн в ФГБОУ ВО Уральский ГАУ, подлежат обязательному учету и защите.

1.4. Режим защиты конфиденциальной информации устанавливается ФГБОУ ВО Уральский ГАУ как собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

ПДн должны обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и с использованием технических и программных средств технической защиты ПДн, сертифицируемых в установленном порядке.

1.5. Уровень технической защиты ПДн, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты ПДн и величины ущерба,

который может быть нанесен собственнику ПДн и субъекту ПДн при ее разглашении, утрате, уничтожении и искажении.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) ПДн должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.6. Объектами защиты в ФГБОУ ВО Уральский ГАУ являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи ПДн - далее основные технические средства и системы (ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается ПДн - далее вспомогательные технические средства и системы (ВТСС);
- помещения, специально предназначенные для обработки ПДн – защищаемые помещения (ЗП).

1.7. Ответственность за выполнение требований настоящего Положения возлагается на ответственное лицо по защите ПДн в ФГБОУ ВО Уральский ГАУ, на руководителей факультетов и института, на руководителей управлений и отделов, в которых обрабатываются ПДн, а также на специалистов допущенных к обработке, передаче и хранению в технических средствах информации, содержащей ПДн.

1.8. Непосредственное руководство работами по защите конфиденциальной информации осуществляет проректор по учебной работе ФГБОУ ВО Уральский ГАУ.

2. Охраняемые сведения в области ПДн.

2.1. Персональные данные (ПДн) работников, обучающихся и абитуриентов ФГБОУ ВО Уральский ГАУ, а также лиц, проживающих в общежитиях ФГБОУ ВО Уральский ГАУ на постоянной основе и не являющихся работниками университета.

Перечень сведений конфиденциального характера, касающихся субъектов ПДн, включает в себя:

- Сведения, касающиеся ПДн о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за

исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

- Сведения, составляющие тайну следствия и судопроизводства в отношении субъекта ПДн.
- Сведения, связанные с профессиональной деятельностью субъекта ПДн, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.).
- Сведения, связанные с коммерческой деятельностью субъекта ПДн, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна).

3. Технические каналы утечки ПДн, несанкционированного доступа и специальных воздействий на нее.

3.1. Доступ к ПДн граждан, нарушение ее целостности и доступности возможно реализовать за счет:

– несанкционированного доступа к ПДн при обработке в информационных системах и ресурсах;

- несанкционированного доступа к ПДн на бумажных носителях;

– утечки ПДн по техническим каналам;

- утечки ПДн без использования технических каналов.

3.2. Детальное описание возможных каналов утечки ПДн, несанкционированного доступа к информации и специальных воздействий на нее содержится в Концепции защиты ПДн, реализуемых в ФГБОУ ВО Уральский ГАУ.

4. Организационные и технические мероприятия по защите ПДн.

4.1. Разработка мер, и обеспечение защиты ПДн осуществляются работниками ФГБОУ ВО Уральский ГАУ, назначаемыми ректором соответствующим приказом.

4.2. Для защиты ПДн, обрабатываемых в информационных системах, используются сертифицированные по требованиям безопасности технические средства защиты.

4.3. Ответственность за обеспечение требований по защите ПДн возлагается на проректора по учебной работе ФГБОУ ВО Уральский ГАУ, в подчинении которого находятся подразделения университета, осуществляющие обработку ПДн.

4.4. Техническая защита ПДн:

4.4.1. Определение перечня помещений, в которых осуществляется обработка ПДн в

компьютерных системах.

4.4.2. Назначение сотрудников, осуществляющих обработку ПДн в конкретных помещениях, ответственных за выполнение требований по технической защите ПДн в этих помещениях.

4.4.3. Разработка Инструкций по обеспечению безопасности ПДн.

4.4.4. Разработка Правил допуска в помещения ФГБОУ ВО Уральский ГАУ, в которых осуществляется обработка ПДн.

4.4.5. Инструктирование работников, осуществляющих обработку ПДн на компьютерах и (или) бумажных носителях о мерах защиты ПДн (правилах эксплуатации ПЭВМ, других технических средств обработки информации, правилах работы с ПДн на бумажных носителях, правилах использования средств связи с соблюдением требований по технической защите ПДн).

4.4.6. Исключение неконтролируемого доступа в помещения, в которых обрабатываются ПДн, посторонних лиц и исключения их доступа к компьютерам с информацией ПДн.

Применение средств линейного электромагнитного зашумления (СЛЗ) линий электропитания, радиотрансляции, заземления, связи.

4.4.7. Техническая защита информации в автоматизированных информационных системах (ИС) от несанкционированного доступа в соответствии с требованиями законодательства РФ, соответствующих постановлений Правительства РФ, руководящих документов ФСБ России и ФСТЭК России, а также локальных актов ФГБОУ ВО Уральский ГАУ должна обеспечиваться путем:

- проведения классификации ИС, на которых осуществляется обработка ПДн;
- выполнения необходимых организационных мер защиты ПДн;
- установки сертифицированных программных и аппаратно-технических средств защиты информации от несанкционированного доступа к программам обработки ПДн..
- защиты ПДн в ИС от воздействия программ-закладок и компьютерных вирусов.

4.5. Организация и проведение работ по антивирусной защите ПДн при обработке ПДн техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

Организация и осуществление антивирусной защиты ПДн на электронных носителях достигается путём:

- установки и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- действий должностных лиц при обнаружении заражения информационно-

вычислительной техники, на которой осуществляется обработка ПДн, программными вирусами.

4.5.1. Осуществление работ по антивирусной защите ПДн возлагается на должностных лиц, осуществляющих контроль за антивирусной защитой.

4.5.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации ПДн, информационных массивов, программных средств общего и специального назначения;

- периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

4.5.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

4.5.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

- входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

- входной антивирусный контроль всей информации поступающей с электронной почтой;

- входной антивирусный контроль всей поступающей информации из сети Internet;

- выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

- периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

- обязательная антивирусная проверка используемых в работе внешних носителей информации;

- постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

- обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

- внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

- восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

4.5.5. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

4.5.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом в Центр компьютерных технологий ФГБОУ ВО Уральский ГАУ или проректору по учебной работе университета для принятия мер по восстановлению работоспособности программных средств и данных.

Также о факте обнаружения программных вирусов сообщается в организацию, от которой поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на компьютере, где осуществляется обработка ПДн, отключить ее от локальной сети и сети интернет и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными работниками Центра информационных технологий ФГБОУ ВО Уральский ГАУ.

4.5.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

4.5.8. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

4.6. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на системного администратора органа исполнительной власти.

4.6.1. Личный пароль пользователь не имеет права сообщать никому.

4.6.2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4.6.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

4.6.4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.6.4. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п. 4.6.4 настоящего Положения.

4.6.5. Хранение исполнителем значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором Touch Memory).

4.6.6. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях и периодический контроль возлагается на администратора безопасности ЦИТ университета.

5. Обязанности и права должностных лиц.

5.1. Ответственным по осуществлению мероприятий по защите ПДн в ФГБОУ ВО Уральский ГАУ назначен проректор по учебной работе университета.

5.2. Обеспечение технической защиты ПДн в ФГБОУ ВО Уральский ГАУ возлагается на ведущего инженера Центра информационных технологий университета.

5.3. Руководители подразделений ФГБОУ ВО Уральский ГАУ организуют и обеспечивают защиту ПДн, обрабатываемую в технических средствах и в помещениях подчиненных им подразделений.

5.4. Работники ФГБОУ ВО Уральский ГАУ, осуществляющие обработку ПДн на электронных и бумажных носителях в подразделениях университета, обеспечивают защиту информации в соответствии с требованиями (нормами), установленными в нормативных документах.

5.5. Руководители подразделений, в которых осуществляется обработка и хранение ПДн, обязаны дать указание прекратить обработку ПДн в случае обнаружения признаков нарушения

в работе компьютерной программы, вносить предложения о проверке программы ПДн и её криптографической защиты, а также в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Информация докладываются проректору по учебной работе немедленно.

5.6. Ректор ФГБОУ ВО Уральский ГАУ имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

6. Планирование работ по технической защите конфиденциальной информации и контролю.

6.1. В ФГБОУ ВО Уральский ГАУ составляются годовые планы работ по технической защите ПДн и проверочных мероприятий.

6.2. Проекты планов разрабатываются комиссией по организации защиты ПДн в университете и утверждаются ректором.

6.3. В планы по защите ПДн и контролю включаются:

- мероприятия по исполнению новых законодательных актов в сфере защиты ПДн в России и Свердловской области;
- подготовка проектов распорядительных документов по вопросам организации защиты ПДн в университете в соответствие новым законодательством;
- аттестация вновь вводимых в эксплуатацию компьютерных программ, а также периодическая переаттестация находящихся в эксплуатации средств технической защиты на соответствие требованиям законодательства;
- проведение периодического контроля состояния защиты ПДн в университете;
- мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;
- мероприятия по совершенствованию защиты ПДн в университете.

6.4. Контроль выполнения планов и отчетность по ним возлагается на проректора по учебной работе или работника Центра информационных технологий университета.

7. Контроль состояния защиты ПДн.

7.1. Основными задачами контроля состояния защиты ПДн в ФГБОУ ВО Уральский ГАУ являются оценка уровня существующих мер защиты, своевременное выявление и предотвращение утечки информации.

7.2. Контроль осуществляется:

- Внутренней комиссией ФГБОУ ВО Уральский ГАУ – не реже 1 раза в год;
- Работниками Центра информационных технологий ФГБОУ ВО Уральский ГАУ – постоянно.

- ФСТЭК России по Свердловской области – при организации проверки;
- Управлением ФСБ России по Свердловской области – при организации проверки.

7.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты ПДн, постановлений Правительства России, решений ФСТЭК России и ФСБ России, внутренних нормативных актов ФГБОУ ВО Уральский ГАУ в сфере защиты ПДн.

8. Мероприятия по режиму допуска в помещения, где размещены информационные системы ПДн.

Мероприятия по режиму допуска в помещения, где размещены информационные системы ПДн регламентируются «Правилами доступа сотрудников и иных лиц в рабочее и нерабочее время, а также в нештатных ситуациях в помещение с элементами информационной системы персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ «ФЦТ», в котором ведется обработка защищаемой информации».

9. Взаимодействие с предприятиями, учреждениями и организациями.

9.1. При проведении совместных работ ФГБОУ ВО Уральский ГАУ с предприятиями, учреждениями и организациями в сфере обработки и обмена информации ПДн должна быть обеспечена защита информации ПДн, независимо от места проведения работ.

9.2. В технических заданиях на выполнение совместных работ с использованием сведений ПДн, должны быть предусмотрены требования (или меры) по ее защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с проректором по учебной работе ФГБОУ ВО Уральский ГАУ и утверждаются ректором.

9.3. Организация защиты информации ПДн в подразделениях ФГБОУ ВО Уральский ГАУ, осуществляющих взаимодействие в данной области с предприятиями, учреждениями и организациями, а также ответственность за нарушения в области защиты ПДн при осуществлении указанного взаимодействия, возлагается на руководителей подразделений, а ответственность за обеспечение технической защиты информации в информационных системах - на исполнителей работ при использовании ими технических средств для обработки и передачи информации, подлежащей защите.