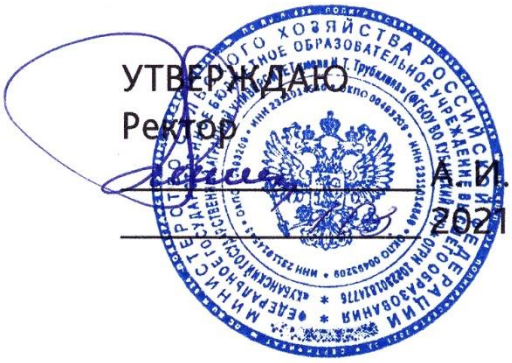
Quality Management System

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
ИМЕНИ И. Т. ТРУБИЛИНА»



СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Политика информационной безопасности при работе с персональными данными

Положение университета

Пл КубГАУ 3.2.6 — 2021
версия 1.1

Краснодар
2021

Лист согласования

РАЗРАБОТАНО

Начальник управления кадрового обеспечения и делопроизводства — А. А. Коровин

ЭКСПЕРТИЗА ПРОВЕДЕНА

Начальник центра менеджмента качества — В. М. Смоленцев

СОГЛАСОВАНО

Первый проректор — С. М. Резниченко

Проректор по учебной работе — А. В. Петух

Проректор по научной работе — А. Г. Кощаев

Начальник центра информационных технологий — А. С. Креймер

Начальник отдела кадров — М. И. Удовицкая

Начальник юридического отдела — С. В. Новикова

Содержание

1 Назначение и область применения

Настоящее положение Федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный аграрный университет имени И. Т. Трубилина» (далее – университет) является официальным документом, определяющим требования к персоналу информационной системы персональных данных, степень ответственности персонала, структуру и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в информационной системе персональных данных университета.

Требования настоящей политики распространяются на всех сотрудников университета (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

2 Нормативные ссылки

Настоящее положение разработано в соответствии с:

— Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Федеральный закон от 30 декабря 2020 г. № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»;

— Постановление Правительства РФ от 01.11.2012 г. № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;

— Постановление Правительства РФ от 15.09.2008 г. № 687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

— Постановление Правительства РФ от 06.07.2008 г. № 512 «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

— Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных;

— Пл КубГАУ 3.2.5 «Организация и обеспечение безопасности персональных данных».

3 Общие положения

Целью настоящей Политики, является обеспечение безопасности объектов защиты университета от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в «Перечне персональных данных, подлежащих защите».

Состав информационной системы персональных данных подлежащих защите, представлен в «Перечне информационной системе персональных данных».

4 Цели сбора персональных данных

4.1 Оператор обрабатывает персональные данные в целях:

— оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества;

— заключения, исполнения и прекращения гражданско-правовых договоров;

— предоставления сведений страховым компаниям, предоставления установленной законодательством отчетности;

— выполнения требований действующего законодательства;

— в иных случаях, установленных в законе, уставе Оператора.

4.2 Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.3 Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.4 Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.5 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.6 Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

5 Правовые основания обработки персональных данных

Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных:

— федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью оператора;

— Устав оператора;

— договоры, заключаемые между оператором и субъектом персональных данных;

— согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор информационной системы персональных данных и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками университета – пользователей информационной системы персональных данных правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в положениях о структурных подразделениях университета, осуществляющих обработку персональных данных в информационной системе персональных данных и должностных инструкциях сотрудников университета.

Необходимо внести в положения о структурных подразделениях университета, осуществляющих обработку персональных данных в информационной системе персональных данных, сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) персональных данных, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

6 Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

6.1 Категории субъектов персональных данных, чьи данные обрабатываются.

6.1.1 Работники Оператора, бывшие работники, кандидаты на трудоустройство, а также члены семьи работников.

6.1.2 Обучающиеся, абитуриенты университета.

6.1.3 Прочие клиенты Оператора (физические лица).

6.2 В отношении категории, указанной в пункте 6.1.1 (за исключением членов семьи работников), обрабатываются:

— фамилия, имя, отчество;

— дата и место рождения;

— адреса места жительства и регистрации;

— контактный телефон;
— гражданство;
— образование;
— профессия, должность;
— стаж работы;
— семейное положение, наличие детей;
— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
— данные страхового свидетельства государственного пенсионного страхования;
— идентификационный номер налогоплательщика;
— табельный номер;
— сведения о доходах;
— сведения о воинском учете;
— сведения о судимостях;
— сведения о повышении квалификации, о профессиональной переподготовке;
— сведения о наградах (поощрениях), почетных званиях;
— сведения о социальных гарантиях.

6.3 Персональные данные родственников работников обрабатываются в объеме, переданном работником и необходимом для предоставления гарантий и компенсаций работнику, предусмотренных трудовым законодательством:
— фамилия, имя, отчество;
— дата рождения.

6.4. В отношении обучающихся и абитуриентов обрабатываются:
— фамилия, имя, отчество;
— пол;
— возраст;
— дата и место рождения;
— адреса места жительства и регистрации;
— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
— данные страхового свидетельства государственного пенсионного страхования;
— гражданство;
— контактный телефон.

7 Порядок и условия обработки персональных данных

7.1 Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

7.2 Оператор не вправе обрабатывать и распространять персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

7.3 Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

7.4 Письменное согласие субъекта персональных данных должно включать:

— фамилию, имя, отчество;

— адрес субъекта персональных данных;

— номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

— наименование и адрес Оператора;

— цель обработки персональных данных;

— перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

— перечень действий с персональными данными, на совершение которых дается согласие

— способ его отзыва;

— подпись субъекта персональных данных.

7.5 Обработка персональных данных осуществляется Оператором следующими способами:

— неавтоматизированная обработка персональных данных;

— автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

— смешанная обработка персональных данных.

7.6 Оператор организует обработку персональных данных в следующем порядке:

1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;

2) издает настоящую Политику, локальные акты по вопросам обработки персональных данных;

3) применяет правовые, организационные и технические мер по обеспечению безопасности персональных данных;

4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;

5) осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;

6) знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

7.7 При обработке персональных данных Оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.8 В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

7.9 Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.

7.10 При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

8 Система защиты персональных данных

Система защиты персональных данных строится на основании:

— итогового отчета об обследовании информационной системы персональных данных;

— отчета о результатах проведения внутренней проверки защиты персональных данных на бумажных носителях.

— перечня персональных данных, подлежащих защите;

— акта классификации информационной системы персональных данных;

— модели угроз безопасности персональных данных;

— матрицы доступа пользователей к защищаемым информационным ресурсам информационной системы персональных данных;

— руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности персональных данных каждой информационной системой персональных данных университета. На основании анализа актуальных угроз безопасности персональных данных описанного в модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности персональных данных. Выбранные необходимые мероприятия отражаются в «Плане мероприятий по обеспечению защиты персональных данных».

Для информационной системы персональных данных должен быть составлен список используемых технических средств защиты (далее – Список), а также программного обеспечения, участвующего в обработке персональных данных, на всех элементах информационной системы персональных данных:

— автоматизированное рабочее место пользователей;

— сервера приложений;

— система управления базы данных;

— граница локальной вычислительной сети;

— каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются персональные данные.

В зависимости от уровня защищенности информационной системы персональных данных и актуальных угроз, система защиты персональных данных может включать следующие технические средства:

— антивирусные средства для рабочих станций пользователей и серверов;

— средства межсетевого экранирования;

— средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки персональных данных операционными системами (ОС), прикладным программными обеспечениями (ПО) и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать:

— управление и разграничение доступа пользователей;

— регистрацию и учет действий с информацией;

— обеспечивать целостность данных;

— производить обнаружений вторжений.

Список используемых технических средств отражается в «Плане мероприятий по обеспечению защиты персональных данных». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов информационной системы персональных данных, соответствующие изменения должны быть внесены в список, который утверждается ректором университета или лицом, ответственным за обеспечение защиты персональных данных.

9 Требования к подсистемам системы защиты персональных данных

Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от класса информационной системы персональных данных, определенного в «Акте классификации информационной системы персональных данных». Список соответствия функций подсистем системы защиты персональных данных классу защищенности представлен в техническом задании по созданию системы защиты информации информационной системы персональных данных.

Система защиты персональных данных включает в себя следующие подсистемы:

9.1 Подсистемы управления доступом, регистрации и учета.

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

— идентификации и проверка подлинности субъектов доступа при входе в информационную систему персональных данных;

— идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

— идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

— регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

— регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

— регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки персональных данных (операционных систем, приложений и систем управления баз данных). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

9.2 Подсистема обеспечения целостности и доступности.

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационной системы персональных данных ФГБОУ ВО Кубанский ГАУ, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов информационной системы баз данных.

9.3 Подсистема антивирусной защиты.

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и автоматизированного рабочего места пользователей информационной системы персональных данных ФГБОУ ВО Кубанский ГАУ.

Средства антивирусной защиты предназначены для реализации следующих функций:

— резидентный антивирусный мониторинг;

— антивирусное сканирование;

— скрипт-блокирование;

— централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

— автоматизированное обновление антивирусных баз;

— ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

— автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы информационной системы персональных данных.

9.4 Подсистема межсетевого экранирования.

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

— фильтрации открытого и зашифрованного (закрытого) IP-трафика;

— фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

— идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

— регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

— контроля целостности своей программной и информационной части;

— фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

— фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

— регистрации и учета запрашиваемых сервисов прикладного уровня;

— блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

— контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

9.5 Подсистема анализа защищенности.

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО информационной системы персональных данных, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

9.6 Подсистема обнаружения вторжений.

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы информационной системы персональных данных, подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

9.7 Подсистема криптографической защиты.

Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в информационной системе персональных данных университета, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

10 Пользователи информационной системы персональных данных

В информационной системе университета можно выделить следующие группы пользователей, участвующих в обработке и хранении персональных данных:

- администратора информационных систем;
- администратора безопасности;
- оператора автоматизированного рабочего места (АРМ).

Данные о группах пользователях, уровне их доступа и информированности должны быть отражены в матрице доступа пользователей к защищаемым информационным ресурсам.

Типизация пользователей информационной системы персональных данных, их уровень доступа и возможности установлена в Пл КубГАУ 3.2.5 «Организация и обеспечение безопасности персональных данных».

11 Требования к персоналу по обеспечению защиты персональных данных

Все сотрудники университета, являющиеся пользователями информационной системой персональных данных, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым

объектам и соблюдению принятого режима безопасности персональных данных.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационной системой персональных данных.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами информационной системы персональных данных и системы защиты персональных данных.

Сотрудники университета, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники университета должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники университета должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами университета, третьим лицам.

При работе с персональными данными в информационной системе персональных данных сотрудники университета обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов АРМ или терминалов.

При завершении работы с информационной системой персональных данных сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники университета должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятую политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системы персональных данных, могущих повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

Должностные обязанности пользователей информационной системы персональных данных описаны в следующих документах:

— инструкция администратора информационной системы персональных данных;

— инструкция администратора безопасности информационной системы персональных данных;

— инструкция пользователя информационной системы персональных данных;

— инструкция пользователя при возникновении внештатных ситуаций.

3.1 Лист регистрации изменений

Содержание изменения	Дата и номер приказа	Дата введения изменения
Введение в действие, версия 1.0	26.09.2016 г. № 330а	26.09.2016 г.
Актуализация положения, версия 1.1	01.03.2021 г. № 88	01.03.2021 г.