МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УЛЬЯНОВСКИЙ ИНСТИТУТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ Б.П. БУГАЕВА»

УТВЕРЖДАЮ
Врио ректора
_____ О.В. Бабкин
«18» 07 2018 г.

ИНСТРУКЦИЯ
по обеспечению информационной безопасности
в ФГБОУ ВО УИ ГА
№ 01. 15. 1. 2018

ПРЕДИСЛОВИЕ

1. Инструкция вводится в действие с момента ее утверждения и действует до отмены.
2. Инструкция разработана в соответствии со следующими документами:
   2.1. Устав института, утвержденный приказом Росавиации от 25.12.2015 № 870.
   2.2. Руководство по СМК института.
3. Структура и содержание документа могут изменяться и дополняться с учетом влияния на деятельность института внутренних и внешних факторов, но не должны противоречить государственным и отраслевым стандартам, а также стандартам ВУЗа, действующим в ФГБОУ ВО УИ ГА.

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приказом ФСТЭК от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Настоящая Инструкция устанавливает в ФГБОУ ВО УИ ГА порядок работы с ЭВМ и документами – носителями информации, необходимой для нормального функционирования института, в том числе конфиденциальной информации.

1.3. Конфиденциальной считается информация, полученная в связи с выполнением служебных функций и содержащая в том числе, но не ограничиваясь этим: коммерческую тайну, персональные данные либо иную охраняемую законом информацию.

1.4. Цели настоящей инструкции:

– предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации, необходимой для нормального функционирования института, в том числе конфиденциальной информации;

– предотвращение неконтролируемого распространения конфиденциальной информации в результате её разглашения должностным лицом, имеющим доступ к информации или получение несанкционированного доступа к конфиденциальной информации.

1.5. Все операции по оформлению, формированию, ведению и хранению любой информации должны выполняться сотрудниками ФГБОУ ВО УИ ГА, осуществляющими данную работу в соответствии со своими трудовыми обязанностями.

1.6. Лицам, работающим с конфиденциальной информацией, запрещается разглашать данную информацию устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью.

1.7. Передача конфиденциальной информации допускается только в случаях, установленных законодательством Российской Федерации и действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению вышестоящих должностных лиц.

1.8. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах запроса или опубликованных в общедоступных источниках.

Все устные пояснения на запросы граждан и организаций могут производиться по поручению вышестоящих должностных лиц либо по согласованию с ними.

1.9. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность служебной информации и исключающие несанкционированный доступ к ним.

1.10. Материальные носители с конфиденциальной информацией должны храниться в запирающихся на ключ помещениях, металлических шкафах, иных шкафах, имеющих запираемые блок-секции. Должна быть исключена возможность неконтролируемого пребывания в соответствующих помещениях посторонних лиц.

1.11. В случае выявления инцидентов информационной безопасности (фактов или попыток несанкционированного доступа к информации, обрабатываемой в компьютере или без использования средств автоматизации) необходимо немедленно сообщить об этом, по требованию руководителя подразделения написать служебную записку на его имя и принять участие в служебной проверке по данному инциденту.

1.12. Запрещается самостоятельно устанавливать на служебные электронные вычислительные машины (далее - ЭВМ) какие-либо аппаратные или программные средства.

1.13. Пользователи ЭВМ должны знать личные пароли и персональные идентификаторы, хранить их в тайне.

1.14. При применении внешних носителей информации перед началом работы необходимо провести их проверку на предмет наличия компьютерных вирусов с помощью антивирусной программы.

1.15. Пользователи ЭВМ должны знать и строго выполнять правила работы с установленными на их компьютерах средствами защиты информации (антивирус, средства разграничения доступа, средства криптографической защиты и т.п.).

1.16. Необходимо передавать для хранения установленным порядком свое индивидуальное устройство идентификации (Touch Memory, Smart Card, Proximity и т.п.), другие реквизиты разграничения доступа и носители ключевой информации только руководителю подразделения или ответственному за информационную безопасность.

2. Обеспечение антивирусной безопасности

2.1. При возникновении подозрения на наличие компьютерного вируса (сообщение антивирусной программы, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль компьютера.

2.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь **ОБЯЗАН:**

- прекратить (приостановить) работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, ответственного за информационную безопасность, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

2.3. Пользователю **ЗАПРЕЩАЕТСЯ:**

- отключать средства антивирусной защиты информации;
- без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

3. Обеспечение информационной безопасности при использовании ресурсов сети Интернет

3.1. Ресурсы сети Интернет могут использоваться для осуществления выполнения требований законодательства Российской Федерации, дистанционного обслуживания, получения и распространения информации, связанной с деятельностью института (в том числе, путем создания информационного web-сайта), информационно-аналитической работы в интересах института, обмена почтовыми сообщениями, а также ведения собственной хозяйственной деятельности. Иное использование ресурсов сети Интернет, решение о котором не принято руководством института в установленном порядке, рассматривается как нарушение информационной безопасности.

3.2. С целью ограничения использования сети Интернет в неустановленных целях выделяется ограниченное число пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников института правами пользователя конкретного пакета выполняется в соответствии с его должностными обязанностями.

3.3.Особенности использования сети Интернет:

- сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом не предоставляются.

3.4. При осуществлении дистанционного обслуживания и электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет институт применяет соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства

криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

3.5. Почтовый обмен конфиденциальной информацией через сеть Интернет осуществляется с использованием защитных мер.

3.6. При пользовании ресурсами сети Интернет **ЗАПРЕЩАЕТСЯ:**

- использовать на рабочем месте иные каналы доступа компьютера к сети Интернет, кроме установленного;
- проводить самостоятельное изменение конфигурации технического и программного обеспечения компьютера, подключенной к сети Интернет;
- осуществлять отправку электронных почтовых сообщений, содержащих конфиденциальную информацию, по открытым каналам;
- использовать иные, кроме служебных, почтовые ящики для электронной переписки;
- открывать файлы, пришедшие вместе с почтовым сообщением, если не известен источник этого сообщения;
- осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее антивирусными программами;
- скачивать из сети Интернет, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т.п., без предварительного согласования с отделом телекоммуникаций института;
- использовать сеть Интернет вне служебных задач, посещать интернет – сайты, не связанные с выполнением должностных обязанностей.

4. Порядок работы с носителями ключевой информации

4.1. В некоторых подсистемах института для обеспечения контроля за целостностью передаваемых по технологическим каналам электронных документов (далее – ЭД), а также для подтверждения их подлинности и авторства могут использоваться средства электронной подписи (далее – ЭП).

4.2. Работнику института (владельцу ключа ЭП), которому в соответствии с его должностными обязанностями предоставлено право постановки на ЭД его ЭП, выдается персональный ключевой носитель информации, на который записана уникальная ключевая информация (ключ ЭП), относящаяся к категории сведений ограниченного распространения.

4.3. Персональные ключевые носители (эталон и рабочую копию) владелец ключа ЭП должен хранить в специальном месте, гарантирующем их сохранность.

4.4. Ключи проверки ЭП установленным порядком регистрируются в справочнике «открытых» ключей, используемом при проверке подлинности документов по установленным на них ЭП.

4.5. Владелец ключа ЭП **ОБЯЗАН:**

- под роспись в «Журнале учета ключевых носителей» получить ключевые носители, убедиться, что они правильно маркированы и на них установлена защита от записи;
- использовать для работы только рабочую копию своего ключевого носителя;
- сдавать свой персональный ключевой носитель на временное хранение руководителю подразделения или ответственному за информационную безопасность в период отсутствия на рабочем месте (например, на время отпуска или командировки);
- в случае порчи рабочей копии ключевого носителя (например, при ошибке чтения) владелец ЭП обязан передать его уполномоченному сотруднику, который должен в присутствии исполнителя сделать новую рабочую копию ключевого носителя с имеющегося эталона и выдать его взамен испорченного. Испорченная рабочая копия ключевого носителя должна быть уничтожена в установленном порядке.

4.6. Владельцу ключа ЭП **ЗАПРЕЩАЕТСЯ**:

- оставлять ключевой носитель без личного присмотра;
- передавать свой ключевой носитель (эталонную или рабочую копию) другим лицам (кроме как для хранения руководителю подразделения или ответственному за информационную безопасность);
- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск компьютера), снимать защиту от записи, вносить изменения в файлы, находящиеся на ключевом носителе;
- использовать ключевой носитель на заведомо неисправном дисководе и/или компьютере;
- подписывать своим персональным ключом ЭП любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;
- сообщать третьим лицам информацию о владении ключом ЭП для данного технологического процесса.

4.7. Действия при компрометации ключей

4.7.1. Если у владельца ключа ЭП появилось подозрение, что его ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сдать скомпрометированный ключевой носитель с пометкой в журнале учета ключевых носителей о причине компрометации, написать служебную записку о факте компрометации персонального ключевого носителя на имя руководителя подразделения.

4.7.2. Ответственный за информационную безопасность обязан немедленно оповестить о факте утраты или компрометации ключевого носителя руководство

института для принятия действий по блокированию ключей для ЭП указанного исполнителя.

4.7.3. По решению руководства института установленным порядком владелец ключа ЭП может получить новый комплект персональных ключевых носителей взамен скомпрометированных.

5. Организация парольной защиты

5.1. Пароль для своей учетной записи пользователь устанавливает самостоятельно.

5.2. Длина пароля должна быть не менее 7 символов. В числе символов пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

5.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (логины, имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

5.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.

6. Особенности обеспечения безопасности конфиденциальной информации, содержащей персональные данные

6.1. К персональным данным относится любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). К персональным данным, в частности, относятся сведения:

- о (об) анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимости;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании приказов, касающихся работников и обучающихся;
- содержании личных дел и трудовых книжек работников и обучающихся;
- содержании материалов, связанных с повышением квалификации и переподготовкой работников, их аттестацией, служебными расследованиями;
- содержании отчетов, направляемых в органы статистики.

6.2. Обработкой персональных данных является любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.3. Обработка персональных данных осуществляется с согласия субъекта персональных данных.

Субъекту персональных данных должно быть предложено заполнить форму письменного согласия на обработку персональных данных согласно Приложению № 1 к настоящей Инструкции.

Согласие субъекта на обработку его персональных данных не требуется в следующих случаях:

– если персональные данные являются общедоступными;

– когда персональные данные относятся к состоянию здоровья субъекта персональных данных, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия субъекта персональных данных невозможно;

– если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработки персональных данных по требованию уполномоченных на то государственных органов в случаях, предусмотренных федеральным законом;

– когда обработка персональных данных осуществляется в целях исполнения обращения, запроса самого субъекта персональных данных, договора с ним;

– обработки адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;

– обработки данных, включающих в себя только фамилии, имена и отчества.

6.4. Доступ к персональным данным работников, обучающихся и иных лиц разрешается только специально уполномоченным лицам, при этом данные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

6.5. Ответственный за организацию обработки персональных данных обязан:

- осуществлять внутренний контроль за соблюдением работниками ФГБОУ ВО УИ ГА законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведений работников ФГБОУ ВО УИ ГА положения законодательства о персональных данных;
- осуществлять контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей.

6.6. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна вестись таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных и установить Перечень лиц, осуществляющих обработку персональных данных.

6.7. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

6.8. Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи (телефон, телефакс, электронная почта и т.п.) без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

6.9. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры, журналы и др.) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых институтом способов обработки персональных данных;

б) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

в) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цель обработки которых заведомо несовместимы.

6.10. Допуск должностных лиц к обработке персональных данных в автоматизированной информационной системе осуществляется на основании соответствующих разрешительных документов и ключей доступа (паролей).

6.11. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа. Работа на компьютерах с персональными данными без паролей доступа или под чужими, а равно общими (одинаковыми) паролями, не допускается.

6.12. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, не допускается.

6.13. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям,

обеспечивающим защиту информации.

6.14. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

– использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

– недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

6.15. При обработке персональных данных в автоматизированной информационной системе разработчиками и администраторами систем должны обеспечиваться:

– обучение лиц, использующих средства защиты информации, применяемые в автоматизированных информационных системах, правилами работы с ними;

– учет лиц, допущенных к работе с персональными данными в автоматизированной информационной системе, прав и паролей доступа;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– описание системы защиты персональных данных;

– иные требования по защите персональных данных.

6.16. Особенности обеспечения безопасности информации и конфиденциальности о персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются локальными нормативными документами института, регламентирующими порядок использования указанных информационных систем, а также эксплуатационной и инструктивной документацией, касающейся технических средств обработки персональных данных в рамках конкретной автоматизированной информационной системы.

6.17. При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для систем высоких классов - также администратор системы безопасности. Техническое обслуживание оборудования должно осуществляться персоналом отдела телекоммуникаций института.

7. Ответственность работников института за нарушение настоящей инструкции

7.1. Работники института несут ответственность согласно действующему законодательству за разглашение сведений, составляющих служебную, коммерческую и иную охраняемую законом тайну (в том числе персональные данные) и сведений ограниченного распространения, ставших им известными по роду работы.

7.2. Нарушения установленных правил и требований по обеспечению информационной безопасности являются основанием для применения к работнику (пользователю) мер наказания, предусмотренных трудовым законодательством.

РАЗРАБОТАЛ:

Проректор по безопасности _____ С.А. Кузин

СОГЛАСОВАНО:

Проректор по ИИД-РК _____ А.А. Оленев

Начальник отдела телекоммуникаций _____ А.А. Костянов

Начальник отдела управления персоналом _____ С.А. Зинченко

Начальник юридического отдела _____ В.В. Зыбрякова

Приложение № 1

СОГЛАСИЕ
на обработку персональных данных

Я (далее - Субъект),

_____,
(фамилия, имя, отчество)

документ, удостоверяющий личность_____ №_____,
(вид документа)

выдан

_____,
(кем и когда)

зарегистрированный (ая) по адресу:

_____,

даю свое согласие ФГБОУ ВО УИ ГА (далее Оператор),
зарегистрированному по адресу: г. Ульяновск, ул. Можайского, д. 8/8,
на обработку своих персональных данных, на следующих условиях:

1. Оператор осуществляет обработку персональных данных Субъекта исключительно в целях

_____.

2. Перечень персональных данных, передаваемых Оператору на обработку:
   - фамилия, имя, отчество;
   - дата рождения;
   - паспортные данные;
   - контактный телефон (дом., сотовый, рабочий);
   - фактический адрес проживания;
   - прочие.
3. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий: обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ, а также на передачу такой информации третьим лицам, в случаях, установленных нормативными документами вышестоящих органов и законодательством.
4. Настоящее согласие действует бессрочно.
5. Настоящее согласие может быть отозвано Субъектом в любой момент по соглашению сторон. В случае неправомерного использования предоставленных данных соглашение отзывается письменным заявлением субъекта персональных данных.
6. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст.14 Федерального закона от 27.06.2006 № 152-ФЗ).

«____»_____ 20__г. _____ _____
Подпись *ФИО*

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«____»_____ 20__г. _____ _____
Подпись *ФИО*

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Ф.И.О.	Должность	Подпись	Дата	Примечание
1	2	3	4	5	6

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№	Номера страниц				Всего страниц в документе	№ документа	Входящий № сопроводит. о документа и дата	Подпись	Дата
	изме ненн ых	зам енё нн ых	нов ых	анну лиро ванн ых					
1	2	3	4	5	6	7	8	9	10