

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени И.С. ТУРГЕНЕВА»
(ОГУ им. И.С.Тургенева)

07.11.2016

П Р И К А З

№ 629

**Об утверждении обязанностей ответственных
по информационной безопасности**

В целях выполнения требований Федерального закона Российской Федерации от 27.07.2006 года № 152-ФЗ «О персональных данных», «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 20.08.2002 года № 282, приказов ФСТЭК России от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», других законодательно - нормативных документов Российской Федерации, Орловской области и документов федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева) в области безопасности информации,

п р и к а з ы в а ю:

1. Утвердить инструкцию ответственного за защиту информации в ОГУ имени И.С. Тургенева (Приложение 1).
2. Утвердить инструкцию Администратору безопасности информации ОГУ имени И.С. Тургенева (Приложение 2).
3. Утвердить инструкцию Администратору системному ОГУ имени И.С. Тургенева (Приложение 3)
4. Контроль за исполнением настоящего приказа возложить на директора Департамента информатизации и перспективного развития Коськина А.В.

И.о. ректора



О.В. Пилипенко

СОГЛАСОВАНО

Директор департамента информатизации и
перспективного развития



А.В. Коськин

Начальник ПУ

Т.И. Ератова

ИНСТРУКЦИЯ

ответственного за защиту информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева»

1. Общие положения

Инструкция лица, ответственного за защиту информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - Инструкция), разработана в соответствии с требованиями существующих законодательно - нормативных документов Российской Федерации, Орловской области и документов федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева) в области безопасности информации.

Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева.

Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами Российской Федерации, Орловской области, настоящей Инструкцией, а также иными локальными нормативными актами ОГУ имени И.С. Тургенева, регламентирующими вопросы обработки конфиденциальной информации (персональных данных).

2 Обязанности лица, ответственного за защиту информации (организацию обработки персональных данных)

2.1 Лицо, ответственное за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева обязано:

- осуществлять внутренний контроль за соблюдением всеми сотрудниками ОГУ имени И.С. Тургенева законодательства Российской Федерации о защите информации (персональных данных), в том числе требований к защите информации (персональных данных);

- доводить до сведения сотрудников ОГУ имени И.С. Тургенева положения законодательства Российской Федерации о защите информации (персональных данных), локальных актов по вопросам обработки конфиденциальной информации (персональных данных), требований к защите информации (персональных данных);

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

3. Права лица, ответственного за организацию обработки персональных данных

3.1. Лицо, ответственное за защиту информации (персональных данных), имеет право:

- принимать решения в пределах своей компетенции; требовать от сотрудников ОГУ имени И.С. Тургенева соблюдения действующего законодательства Российской Федерации по защите информации, а также локальных нормативных актов ОГУ имени И.С. Тургенева по защите информации (персональных данных);

- контролировать в ОГУ имени И.С. Тургенева осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», другими нормативными правовыми актами Российской Федерации, Орловской области по защите информации (персональных данных) и принятыми в соответствии с ними нормативными правовыми актами;

- взаимодействовать с руководством и иными структурными подразделениями ОГУ имени И.С. Тургенева по вопросам обработки конфиденциальной информации (персональных данных).

4. Ответственность лица, ответственного за защиту информации (организацию обработки персональных данных)

4.1. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о защите информации (персональных данных) лицо, ответственное за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева, несет предусмотренную законодательством Российской Федерации ответственность.

ИНСТРУКЦИЯ

Администратора безопасности информации (БИ)

Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

1. Общие положения

1.1. Инструкция администратора безопасности информации автоматизированных информационных систем, в том числе информационных систем персональных данных (далее – АИС и ИСПДн соответственно), Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева), обрабатывающих конфиденциальную информацию, в том числе персональные данные (далее – Администратор БИ), определяет задачи, обязанности, права и ответственность Администратора БИ по вопросам обеспечения информационной безопасности при обработке конфиденциальной (в том числе персональных данных) информации в АИС и ИСПДн ОГУ имени И.С. Тургенева.

1.2. Обязанности Администратора БИ возлагаются на сотрудника ОГУ имени И.С. Тургенева приказом ректора.

1.3. По вопросам обеспечения безопасности информации (персональных данных) Администратор БИ подчиняется ректору, ответственному по защите информации (по безопасности персональных данных) ОГУ имени И.С. Тургенева.

1.4. Администратор БИ руководствуется положениями настоящей Инструкции, «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации», утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282, приказами ФСТЭК России 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других руководящих документов ФСТЭК и ФСБ России по защите информации (персональных данных), а также требованиями эксплуатационных документов на систему защиты информации от несанкционированного доступа.

2. Основная задача и обязанности Администратора БИ

2.1. Основными задачами Администратора БИ являются:

2.1.1. Организация эксплуатации технических и программных средств защиты информации АИС и ИСПДн в соответствии с установленными требованиями по защите информации.

2.1.2. Текущий контроль работы средств и систем защиты информации АИС и ИСПДн.

2.1.3. Контроль за работой пользователей АИС и ИСПДн, выявление и регистрация попыток несанкционированного доступа к защищаемым информационным ресурсам.

2.2. В соответствии с возложенными задачами Администратор БИ осуществляет следующие функции:

2.2.1. Выполняет работу по внедрению и эксплуатации в АИС и ИСПДн общесистемных программных средств, сертифицированных по требованиям безопасности информации:

- выполняет контроль за установкой на серверном оборудовании и рабочих станциях АИС и ИСПДн общесистемных программных средств;
- выполняет настройку общесистемных программных средств в соответствии с сертифицированными шаблонами безопасности;
- выполняет установку и настройку специального программного обеспечения для контроля и настройки общесистемных программных средств, сертифицированных по требованиям безопасности информации.

2.2.2. Организует работу по внедрению и эксплуатации СЗИ в соответствии с установленными требованиями по защите информации:

- выполняет работу по установке и настройке технических и программных средств защиты информации АИС и ИСПДн от несанкционированного доступа к ней;
- обеспечивает эксплуатацию технических и программных средств защиты информации АИС и ИСПДн, контролирует работоспособность и эффективность функционирования этих средств;
- осуществляет систематический контроль работы средств защиты информации АИС и ИСПДн;
- распределяет между пользователями АИС и ИСПДн необходимые реквизиты криптографической защиты (пароли, ключи защиты и т.п.), формирует и распределяет между пользователями необходимые реквизиты защиты от НСД;
- выполняет ввод описаний пользователей АИС и ИСПДн в информационную базу СЗИ от НСД;
- выполняет своевременное удаление описаний пользователей АИС и ИСПДн из базы данных СЗИ от НСД при изменении списка сотрудников ОГУ имени И.С. Тургенева, допущенных к обработке конфиденциальной информации (далее - КИ) и персональных данных (далее - ПДн).
- проводит обучение пользователей АИС и ИСПДн правилам работы со средствами защиты информации;
- организует работу по эксплуатации СЗИ в АИС и ИСПДн.
- проводит контроль целостности СЗИ с целью выявления несанкционированных изменений в ней;
- выполняет восстановление программной среды, программных средств и настроек СЗИ от НСД при сбоях.

2.2.3. Организует работу по защите информации, циркулирующей в АИС и ИСПДн:

- осуществляет контроль разграничения прав доступа к защищаемой информации на несъемных носителях информации рабочих мест пользователей АИС и ИСПДн;
- принимает участие в разработке документов по обеспечению безопасности информации при эксплуатации АИС и ИСПДн;
- осуществляет контроль за проведением смены паролей пользователей АИС и ИСПДн;

- осуществляет настройку и сопровождение подсистемы регистрации и учета действий пользователей АИС и ИСПДн;
- принимает меры по предупреждению угроз безопасности информации, возникающих в результате случайных ошибок пользователей АИС и ИСПДн при обработке электронных документов;
- проводит периодический контроль средств вычислительной техники, подключенных к АИС и ИСПДн, на предмет исключения несанкционированного изменения в составе, конструкции, конфигурации, размещении средств вычислительной техники, а также в составе программного обеспечения;
- регулярно анализирует содержимое системных журналов, проводит работы по выявлению возможных каналов утечки КИ и персональных данных за счет несанкционированных доступов к информации и техническим средствам АИС и ИСПДн, ведет их учет;
- обобщает и анализирует сведения о противоправных устремлениях к информации, попытках преодоления СЗИ, используемых при этом методах и средствах;
- анализирует состояние защищенности информационных ресурсов АИС и ИСПДн, готовит предложения по совершенствованию СЗИ;
- принимает участие в оценке реальной опасности утечки информации, подлежащей защите при использовании технических средств, в разработке эффективных и экономически обоснованных мер по ее защите;
- осуществляет контроль за выводом документов пользователей АИС и ИСПДн на принтерах и за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;
- осуществляет контроль соблюдения требований по безопасности информации при использовании машинных носителей информации;
- разрабатывает и вводит установленным порядком необходимую учетную и объектовую документацию (журнал учета идентификаторов, инструкции пользователям и т.д.);
- выполняет установку и настройку антивирусной системы защиты информации в АИС и ИСПДн, контроль за периодическим обновлением антивирусных баз (средств), осуществляет контроль за соблюдением пользователями АИС и ИСПДн порядка и правил проведения антивирусного тестирования;
- осуществляет контроль доступа лиц в помещение, где установлены рабочие станции и серверное оборудование АИС и ИСПДн, в соответствии с утвержденными списками сотрудников ОГУ имени И.С. Тургенева, допущенных к обработке КИ и ПДн;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток неправомерного доступа к охраняемым сведениям или попыток хищения, копирования, изменения сообщает ответственному за защиту информации (обработку ПДн) и ректору ОГУ имени И.С. Тургенева.

3. Обязанности Администратора БИ

Администратор БИ обязан:

- 3.1. Знать состав АИС и ИСПДн (серверное оборудование, рабочие станции, используемое программное обеспечение).
- 3.2. Знать состав пользователей АИС и ИСПДн и их производственную деятельность (выполняемые операции, права, привилегии).

3.3. Знать порядок и технологию включения и удаления пользователей в СЗИ от НСД.

3.4. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в соответствии с требованиями руководящих и нормативно-методических документов по защите информации.

3.5. Докладывать о выявленных нарушениях и НСД пользователей АИС и ИСПДн к защищаемой информации, принимать необходимые меры по устранению выявленных нарушений.

3.6. Проводить инструктаж пользователей АИС и ИСПДн по правилам работы с используемыми средствами и системами защиты информации.

3.7. Осуществлять контроль соответствия уровня конфиденциальности выводимой информации на внешние носители информации и грифа конфиденциальности этих носителей, а также правильности их учета.

3.8. Осуществлять контроль соответствия уровня конфиденциальности информации, выводимой на печать, и грифа конфиденциальности бумажных машинных носителей информации – листов бумаги, а также правильности их учета.

3.9. Осуществляет контроль за уничтожением конфиденциальной информации и ее носителей, гарантированного уничтожения информации средствами СЗИ от НСД.

4. Права Администратора БИ

Администратор БИ имеет право:

4.1. Иметь доступ к средствам обработки и передачи информации АИС и ИСПДн, постоянно осуществлять проверки состояния СЗИ, контролировать состояние защищенности АИС.

4.2. Требовать от пользователей АИС и ИСПДн соблюдения установленных правил обработки КИ и ПДн и выполнения требований руководящих и нормативно-методических документов по защите информации.

4.3. Обращаться к ответственному за защиту информации (за безопасность ПДн) ОГУ имени И.С. Тургенева, а в случае их отсутствия к ректору и с требованием о прекращении доступа пользователя к работам в АИС и ИСПДн в случае грубых нарушений требований руководящих и нормативно-методических документов по защите информации, порядка и правил обработки конфиденциальной информации или нарушения функционирования средств и систем защиты информации.

4.4. Требовать назначения служебного расследования в отношении пользователя АИС и ИСПДн по фактам нарушения безопасности информации и НСД к защищаемой информации.

5. Ответственность Администратора БИ

5.1. Администратор БИ ОГУ имени И.С. Тургенева несет ответственность в полном объеме по действующему законодательству Российской Федерации за разглашение сведений, составляющих КИ, ПДн и другой информации ограниченного доступа ставших известными ему в соответствии с родом работы.

ИНСТРУКЦИЯ

Администратора системного автоматизированной информационной системы (информационной системы персональных данных) федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность Администратора системного автоматизированной информационной системы (далее - АИС), в том числе информационной системы персональных данных (далее – ИСПДн), федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева).

1.2. Администратор системный АИС, ИСПДн (далее – Администратор) в пределах своих функциональных обязанностей, обеспечивает работоспособность технических средств АИС (ИСПДн) и установленного программного обеспечения.

1.3. Администратор назначается в установленном порядке приказом ОГУ имени И.С. Тургенева.

1.4. Администратор в своей работе должен руководствоваться настоящей Инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

- Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказы ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- локальные акты ОГУ имени И.С. Тургенева;

- иные нормативные акты Российской Федерации, Орловской области в области безопасности информации (персональных данных)

1.5. Основные понятия и термины, используемые в настоящей Инструкции, применяются в значениях, определенных статьей 3 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Обязанности:

а) знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также локальных актов ОГУ имени И.С. Тургенева, регламентирующих деятельность по защите конфиденциальной информации

(персональных данных);

б) устанавливать, настраивать и сопровождать необходимое для работы АИС (ИСПДн) программное обеспечение;

в) обеспечивать функционирование и поддержание в рабочем состоянии программных средств и средств вычислительной техники в пределах возложенных на него обязанностей;

г) выполнять резервирование и восстановление программных средств;

д) контролировать физическую сохранность оборудования АИС (ИСПДн);

е) не допускать установку, использование, хранение и распространение в АИС (ИСПДн) программных средств, не связанных с выполнением функциональных задач;

ж) взаимодействовать с ответственным за защиту информации (организацию обработки персональных данных) и Администратором безопасности информации АИС (ИСПДн) при проведении работ, связанных с анализом и оценкой защищенности информации в АИС (ИСПДн);

з) докладывать ответственному за защиту информации (организацию обработки персональных данных), Администратору безопасности информации АИС (ИСПДн) об обнаруженных недекларированных возможностях программных средств, нарушениях и несанкционированных действиях пользователей;

и) взаимодействовать с ответственным за защиту информации (организацию обработки персональных данных), Администратором безопасности информации АИС (ИСПДн) по вопросам обеспечения правильной эксплуатации средств вычислительной техники АИС (ИСПДн);

к) проводить инструктаж и консультации пользователей АИС (ИСПДн) по правилам работы и эксплуатации используемых средств вычислительной техники.

3. Права

а) требовать от пользователей АИС (ИСПДн) точного соблюдения установленной технологии обработки информации и выполнения инструкций по работе с техническими и программными средствами АИС (ИСПДн);

б) обращаться к ответственному за защиту информации (организацию обработки персональных данных) и Администратору безопасности информации АИС (ИСПДн) с предложением о приостановке обработки конфиденциальной информации (персональных данных) в случаях грубых нарушений установленной технологии их обработки и/или функционирования программных и/или технических средств;

в) докладывать непосредственному руководителю о нарушениях или невыполнении пользователями инструкций по работе с техническими и программными средствами АИС (ИСПДн).

4. Ответственность

Системный администратор АИС (ИСПДн) несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.