АСОУ
АКАДЕМИЯ СОЦИАЛЬНОГО УПРАВЛЕНИЯ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
«АКАДЕМИЯ СОЦИАЛЬНОГО УПРАВЛЕНИЯ»

ПРИКАЗ

07.06.2022 № 749-04

г. Мытищи

Об утверждении Положения о порядке организации и проведения работ по защите информации ограниченного доступа в АСОУ

В соответствии с Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09. 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и приказом ФСТЭК России 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»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Положение о порядке организации и проведения работ по защите информации ограниченного доступа в АСОУ (далее - Положение);

1.2. Структуру информационной безопасности АСОУ.

2. Руководителям структурных подразделений ознакомить работников, имеющих доступ к персональным данным, с настоящим Положением под их личную подпись.

3. Признать утратившим силу Приказ от 22.05.2017 № 154-07 «Об утверждении Положения о защите информации ограниченного доступа в ГБОУ ВО МО «Академия социального управления».

4. Контроль за исполнением настоящего приказа возложить на проректора по безопасности **Бородина В.Н.**

Ректор АСОУ **А.А. Лубский**

Утверждено
приказом АСОУ
от «07» 06 2022 года №749-04

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА в АСОУ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке организации и проведения работ по защите информации ограниченного доступа в АСОУ разработано на основании требований:

Федеральных законов:

- от 27.07.2006 г. № 152- ФЗ «О персональных данных»,
- от 27.07.2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации»,
- от 29.07.2004 г. № 98- ФЗ «О коммерческой тайне»,
-Трудового кодекса Российской Федерации;

Постановлений Правительства Российской Федерации:

- от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение определяет порядок организации и проведения работ в АСОУ для построения эффективной системы защиты информации (далее - СЗИ) от несанкционированного доступа и её последующей эксплуатации.

1.3. В настоящем Положении используются следующие основные термины и определения:

Информационная система (далее - ИС) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационная система персональных данных (далее - ИСПДн) является информационной системой, обрабатывающей иные категории персональных данных, так как в ней не обрабатываются персональные данные, относящиеся к специальным категориям ПДн, биометрические и общедоступные ПДн.

Информация ограниченного доступа (далее – информация) - сведения, доступ к которым ограничен Федеральными законами, в частности Указом Президента Российской Федерации от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», и отраженные в «Сводном перечне сведений конфиденциального характера», утвержденном постановлением Правительства Московской области от 27.11. 2002 № 573/46.

Обработка информации - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таковых средств.

Персональные данные (далее - ПДн) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). ПДн относятся к информации ограниченного доступа.

1.4. Требования настоящего Положения распространяется на все процессы обработки информации ограниченного доступа в АСОУ, как с использованием средств автоматизации, так и без использования таких средств, и являются обязательными для исполнения во всех структурных подразделениях, всеми должностными лицами АСОУ.

1.5. За общее состояние защиты информации в АСОУ ответственность несет ректор АСОУ.

Персональная ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях АСОУ возлагается на руководителей этих подразделений.

Ответственность за обеспечение защиты информации на рабочих местах, находящихся в структурном подразделении, возлагается непосредственно на пользователя информации.

Проведение работ по защите информации в ИС с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения возлагается на работника АСОУ выполняющего функции администратора ИСПДн.

Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту информации ограниченного доступа в АСОУ (далее – ответственный).

1.6. Все работники, допущенные к обработке информации, обязаны соблюдать конфиденциальность информации в течение срока действия трудового договора. Для этих работников предусмотрены в трудовом договоре обязательство о неразглашении информации.

1.7.Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения ПДн несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

1.8. Для оказания услуг в области аттестации информационных систем персональных данных АСОУ привлекает специализированные организации, имеющие лицензию на этот вид деятельности.

1.9. Положение может уточняться и корректироваться по мере необходимости. Все изменения в Положение вносятся приказом ректора АСОУ.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И АКТУАЛЬНЫЕ УГРОЗЫ

2.1. Охраняемые сведения - информация, обрабатываемая в ИСПДн АСОУ в соответствии с Перечнем процессов и сведений ограниченного доступа, обрабатываемых в государственном бюджетном образовательном учреждении высшего образования Московской области «Академия социального управления», а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2. Объекты защиты:

- ИСПДн различного назначения, участвующие в обработке информации и включенные в Перечень информационных систем персональных данных, используемых для обработки персональных данных в АСОУ утвержденный ректором;
- помещения, где установлены ИСПДн или хранится информация на бумажных носителях, включенные в Перечень мест хранения бумажных носителей персональных данных в АСОУ, утвержденный ректором.

2.3 . В соответствии с моделями угроз безопасности персональных данных в ИСПДн, актуальными являются только угрозы несанкционированного доступа к информационным ресурсам ИСПДн с целью получения, разрушения, искажения и блокирования информации.

Данный вид угроз в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» относится к угрозам 3-го типа.

2.4.Основное внимание должно быть уделено защите информации, в отношении которой, угрозы безопасности реализуются без применения сложных технических средств:

- обрабатываемой в ИСПДн от несанкционированного доступа (далее- НСД) нарушителей и непреднамеренных действий работников АСОУ;
- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в локальной вычислительной сети АСОУ при несанкционированном подключении к данной сети;
- при подключении ИСПДн к открытым телекоммуникационным сетям «Интернет».

3. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Целью защиты ИСПДн от НСД является обеспечение защиты информации путем выполнения требований нормативных правовых актов,

принятыми ФСТЭК России в исполнении части 4 статьи 19 Федерального закона от 27.07.2006 года № 152- ФЗ «О персональных данных» для соответствующего уровня защищённости ПДн, определенного актом.

3.2. Целью технических мероприятий по защите информации в АСОУ является предотвращение НСД к информации при её обработке в ИСПДн, связанное с действиями нарушителей, включая пользователей информационных систем, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступ к ИСПДн, реализующих угрозы из открытых телекоммуникационных сетей «Интернет», с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

3.3. Целями организационных мероприятий по защите информации в АСОУ являются:

- организация режима обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (установка замков, систем сигнализации, видеонаблюдения и т.п.);
- исключение непреднамеренных действий работников АСОУ, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации ИСПДн;
- сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием ИСПДн (физический вынос информации на электронных или бумажных носителях);
- исключение ознакомления сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями;
- обеспечение безопасного хранения материальных носителей ПДн (размещение сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.);
- использование средств гарантированного уничтожения материальных носителей ПДн (средства измельчения, сжигания, размагничивания и т.п.);
- использование систем пожарной сигнализации и пожаротушения.

3.4. Ректор АСОУ самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Положением.

К таким мерам могут, в частности, относиться:

- назначение ответственного за защиту информации ограниченного доступа;
- принятие локальных актов, определяющих политику в отношении обработки ПДн в АСОУ, а также устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;
- выбор в качестве основного средства защиты ИСПДн, не подключённых к сети Интернет, операционных систем «Windows 7 / 8 Professional, Windows 10» (далее - ОС), обладающих встроенными средствами защиты от НСД или других технических средств защиты от НСД (Secret Net и др.);
- настройка ОС на технических средствах из состава ИСПДн;

- сертификация вышеуказанных ОС технических средств по требованиям безопасности информации;

- определение режима разграничения прав доступа пользователей информационной системы. Разграничение доступа – это осуществление входа в систему по индивидуальному паролю;

- выбор дополнительных технических средств, сертифицированных по требованиям безопасности информации, в случае когда применение таких средств необходимо для нейтрализации актуальных угроз. В частности, для ИСПДн, подключенных к локальной сети АСОУ общего пользования;

- использование средств антивирусной защиты;

- предотвращение организационными мерами НСД к обрабатываемой информации;

- организация процесса резервного копирования и архивирования, как неотъемлемой части политики защиты информации;

- осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах;

- строгое соблюдение работниками АСОУ Инструкции по работе пользователей ИСПДн, утвержденной приказом ректора.

3.5. Документальное оформление мероприятий по защите объекта информатизации включает разработку и внедрение организационно - распорядительных документов:

- приказ об организации работ по обеспечению безопасности информации ограниченного доступа в АСОУ ;

- положение о защите информации ограниченного доступа в АСОУ;

- перечень процессов и сведений ограниченного доступа, обрабатываемых в АСОУ;

- список лиц, допущенных в соответствии с их должностными обязанностями к обработке информации;

- перечень информационных систем, используемых для обработки персональных данных в АСОУ;

- акты определения уровня защищенности ИСПДн;

- технические паспорта на ИС;

- модель угроз безопасности на ИС;

- список пользователей ИСПДн;

- перечень мест хранения бумажных носителей ПДн;

- инструкции ответственного за эксплуатацию и по работе пользователей ИС;

- должностные инструкции администратора безопасности и системного администратора ИС;

- журнал учёта паролей пользователей для работы в ИС;

- журнал учёта машинных носителей информации;

- документы на ИСПДн о соответствии требованиям безопасности информации (Аттестат соответствия требованиям безопасности или протокол оценки эффективности на информационную систему).

4. ВВОД В ЭКСПЛУАТАЦИЮ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Необходимым условием для ввода в эксплуатацию информационных систем персональных данных АСОУ является, их соответствие требованиям Федерального закона от 27.07.2006 года № 152- ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.2. Ректор АСОУ принимает решение об организации работ по построению систем защиты ИСПДн собственными силами АСОУ или с привлечением сторонней организации, имеющей лицензию ФСБ и ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

4.3. В случае привлечения сторонней организации она проводит аттестационные испытания либо оценку эффективности в соответствии с разработанным техническим заданием, а также программой и методикой испытаний согласованной с АСОУ, в соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Испытания завершаются выдачей документа о соответствии информационной системы требованиям безопасности информации (Аттестата соответствия требованиям безопасности или протокола оценки эффективности на информационную систему).

4.4. В случае проведения работ по построению системы защиты ИС силами АСОУ оценка полученного результата проводится в форме декларирования.

4.5. Для декларирования соответствия ИСПДн требованиям п.3.1 комиссией, утвержденной приказом ректора, подготавливаются и представляются на ИС:

- акт определения уровня защищенности ИСПДн;
- технический паспорт;
- организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам;
- модель угроз безопасности персональных данных;
- сертификаты средств защиты информации, используемые при построении системы защиты;
- инструкция по работе пользователей;
- инструкция ответственного за защиту информации ограниченного доступа.

4.6. При использовании для защиты ИСПДн от НСД технических средств защиты информации их настройка проводится силами АСОУ.

4.7. Контроль эффективности средств защиты информации (далее - СЗИ) осуществляется представителями соответствующих подразделений Министерства образования Московской области с оформлением акта на выполнение требований

федерального законодательства по защите информации по обеспечению безопасности ПДн субъектов ПДн при их обработке с использованием средств автоматизации.

4.8. В случае положительных результатов испытаний СЗИ ректор АСОУ декларирует соответствие ИС требованиям безопасности информации.

4.9. По результатам декларирования соответствия ответственным за защиту информации ограниченного доступа разрабатываются и доводятся до руководителей и работников АСОУ под роспись необходимые инструкции и рекомендации по порядку выполнения мероприятий по защите информации.

5. ОСОБЕННОСТИ ОБРАБОТКИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Обработка персональных данных работников АСОУ и сведений об их профессиональной служебной деятельности осуществляется в следующих целях:

- начисление и учет заработанной платы, пособий, вознаграждений;
- предоставление сведений в ИФНС, Пенсионный фонд, Фонд обязательного медицинского страхования, Фонд социального страхования, военкомат, Министерство образования Московской области;
- надлежащее исполнение условий трудового договора, обеспечение соблюдения трудового законодательства и иных нормативных правовых актов;
- организация учебно-воспитательного процесса;
- организация пропускного режима.

5.2. Обработка персональных данных обучающихся (абитуриентов), необходимых для оказания им услуг в области образования, осуществляется в следующих целях:

- начисление стипендий, пособий, вознаграждений;
- предоставление сведений в ИФНС, Пенсионный фонд, Фонд обязательного медицинского страхования, Фонд социального страхования, военкомат, Министерство образования Московской области;
- надлежащее исполнение образовательных услуг, обеспечение соблюдения трудового законодательства и иных нормативных правовых актов;
- организация учебно-воспитательного процесса;
- организация пропускного режима;
- обеспечение соблюдения законодательства при поступлении на обучение для реализации права на образование, предоставления льгот при поступлении в соответствии с законодательством Российской Федерации.

5.3. Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объем обрабатываемых ПДн в АСОУ соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

5.4. При обработке ПДн в АСОУ обеспечивается их точность, достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. АСОУ принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных ПДн.

5.5. Хранение ПДн в АСОУ осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок их хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Конкретные обязанности по хранению документов возлагаются на лиц, осуществляющих обработку ПДн, в соответствии с их трудовыми функциями и закрепляются в трудовых договорах, должностных инструкциях и иных регламентирующих документах Академии.

5.6. К ПДн относятся:

- документ, удостоверяющий личность (серия, номер, кем выдан, дата выдачи);
- дата и место рождения;
- биографические сведения;
- сведения об образовании;
- сведения о семейном положении;
- сведения о месте регистрации, проживании;
- сведения о наличии/отсутствии судимости;
- иное.

5.7. Все персональные данные субъекта ПДн следует получать у него самого.

Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Академии должно сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на их получение.

5.8. АСОУ не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.9. Субъект ПДн самостоятельно принимает решение о предоставлении своих ПДн и дает согласие на их обработку.

Обработка указанных данных возможна без его согласия в соответствии со ст. 6 Федерального закона от 27.07.2006 года № 152- ФЗ «О персональных данных»

5.10. Согласие на обработку ПДн оформляется в письменном виде.

Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта ПДн;

- цель обработки ПДн;

- перечень ПДн, на обработку которых дается согласие субъекта персональных данных;

- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

- срок, в течение которого действует согласие, а также порядок его отзыва.

5.11. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя ректора АСОУ.

5.12. Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту тайны.

5.13. Субъект ПДн имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;

- перечень обрабатываемых ПДн и источник их получения;

- сроки обработки ПДн, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

5.14. Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.15. Сведения о ПДн должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн.

5.16. Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю оператором при получении письменного запроса субъекта ПДн или его законного представителя. Письменный запрос должен быть адресован на имя ректора АСОУ или уполномоченное им лицо. Копии документов, содержащих ПДн, выдаются в срок не позднее тридцати дней со дня подачи письменного заявления об их выдаче. При выдаче документов для ознакомления, а также запрашиваемых копий и справок, работник, занимающийся обработкой ПДн, обязан удостовериться в личности запрашивающего (или его представителя) и потребовать предоставление документа, подтверждающего соответствующие полномочия.

5.17. Субъект вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных (Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Центральному федеральному округу) или в судебном порядке неправомерные действия или бездействия должностных лиц АСОУ при обработке и защите его ПДн.

5.18. Доступ к ПДн должен быть ограничен, в том числе путем определения перечня лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей. Доступ работников АСОУ к ИСПДн ограничен системой разграничения прав доступа, реализуемой в рамках системы защиты ПДн с использованием технических и организационных мероприятий.

5.19. Предоставление ПДн третьим сторонам осуществляется только с предварительного письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательством Российской Федерации, в частности Федеральными законами от 15.12.2001 №167- ФЗ «Об обязательном пенсионном страховании в Российской Федерации, от 16.07.1999 №165- ФЗ «Об основах обязательного социального страхования, от 29.11.2010 № 326- ФЗ «Об обязательном медицинском страховании в Российской Федерации».

5.20. Существенным условием договоров с третьими сторонами, в рамках, исполнения которых передаются ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

5.21. АСОУ с согласия субъекта может поручать обработку ПДн третьим сторонам, а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

В случае если АСОУ поручает обработку третьей стороне, в поручении на обработку ПДн должны быть в обязательном порядке определены:

- перечень действий (операций) с ПДн, которые будут совершаться третьей стороной;
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом – в договоре с оператором, в согласии и т. д.);
- обязанность третьей стороны соблюдать конфиденциальность ПДн и обеспечивать безопасность при их обработке;
- требования к защите ПДн.

6. ОБРАЩЕНИЕ С МАТЕРИАЛЬНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Персональные данные хранятся на материальных носителях двух видов:
- машинные носители информации (далее – МНИ);
- бумажные носители.

6.2. Бумажные носители ПДн должны храниться в условиях, исключающих несанкционированный доступ к ним посторонних лиц - в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6.3. Хранение бумажных носителей ПДн вместе с документами общего доступа запрещается, за исключением случаев, когда документы общего доступа являются приложениями к бумажным носителям ПДн.

6.4. Запрещается совместное хранение бумажных (документальных) носителей ПДн, обработка которых осуществляется в различных целях.

6.5. Все категории персональных данных должны быть указаны в едином Перечне мест хранения бумажных носителей персональных данных, утвержденном приказом ректора. В Перечне указывается:
- категории субъектов ПДн;

- категории ПДн;

- места хранения (номер или наименование помещения, в котором хранятся бумажные носители, номер шкафа (сейфа), где хранятся бумажные носители).

6.6. ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по истечении установленных сроков хранения информации, по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

6.7. Для предотвращения разрушения и утери информации, обрабатываемой на компьютере, пользователь ИСПДн должен осуществлять копирование необходимой информации по мере ее обновления на учтенные в установленном порядке МНИ (такие как: внешние жесткие диски, гибкие магнитные диски, USB флэш-накопители, карты флэш-памяти, оптические носители и др.). Носители должны быть учтены в Журнале учёта машинных носителей информации (далее – Журнал).

В Журнале указывают:

- номер машинного носителя;
- тип носителя;
- Ф.И.О. работника за кем закреплен;
- дата получения и подпись работника;
- дата возврата и подпись Администратора ИСПДн;
- отметка об уничтожении.

6.8. В Журнале также учитываются машинные носители информации с ЭЦП и носители, предназначенные для передачи ПДн третьей стороне.

Ответственность за ведение и хранение Журнала несёт ответственный за защиту информации, который один раз в год проверяет наличие МНИ у пользователей.

6.9. В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки МНИ такой носитель уничтожается или с него стираются ПДн (способом исключающим возможность восстановление данных).

6.10. Вынос резервных копий баз данных ИСПДн, содержащих информацию персонального характера, из АСОУ запрещен.

Передача и копирование их допустима только для прямого использования с целью технологической поддержки ИСПДн.

7. СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОСНОВНЫЕ ЦЕЛИ, ЗАДАЧИ, СТРУКТУРА

Подразделение информационной безопасности (группа защиты информации) (далее - ГЗИ) представляет собой самостоятельное структурное подразделение АСОУ.

ГЗИ формируется, реструктуризируется и ликвидируется приказом ректора АСОУ.

Работа подразделения ГЗИ выстраивается в соответствии с требованиями законодательства и иных нормативно-правовых актов в области защиты информации, в том числе уставной документации АСОУ.

Обязанности работников ГЗИ, их полномочия и степень ответственности за сохранность информационных ресурсов АСОУ, определяются положением и уставной документацией АСОУ, а также условиями трудового договора, должностными инструкциями.

ГЗИ взаимодействует с другими структурными подразделениями АСОУ в пределах своей компетенции.

7.1. Цели, задачи и функции подразделения ГЗИ

Цель работы подразделения ГЗИ - обеспечение защиты информационных ресурсов АСОУ от намеренного и ненамеренного разглашения, утери, искажения, похищения.

Задачи подразделения ГЗИ:

- разработка и внедрение системы безопасности и контроль за ее работой, анализ эффективности используемых средств защиты информации;
- разработка и внедрение организационных и технических мероприятий по комплексной защите информации в подразделениях АСОУ где происходит процесс обработки информации;
- проведение работ по организации защиты информации;
- контроль соблюдения нормативных требований по надежной защите информации;
- контроль за ведением делопроизводства с конфиденциальной информацией в соответствии с установленным порядком в АСОУ.

Функции подразделения ГЗИ:

- разработка и использование разнообразных методов и способов защиты конфиденциальной информации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
- внедрение режима конфиденциальности информации и контроль за его соблюдением;
- разработка документов, предписывающих соблюдение режима конфиденциальности информации работниками АСОУ, обучающимися, прикомандированными лицами;
- оценка эффективности внедренной системы защиты информационных ресурсов АСОУ от намеренного и ненамеренного разглашения, утери, искажения, похищения;
- проведение обучения и инструктажей работников АСОУ с последующим допуском к работе на АРМ, используемых в защищенных сетях АСОУ, и пользованию конфиденциальной информацией;
- составление необходимых актов проверки технических средств, оборудования ИС, помещений на предмет их соответствия требованиям безопасности;
- организация взаимодействия между структурными подразделениями АСОУ по вопросам защиты информации.

7.2. Взаимодействия подразделения ГЗИ с структурными подразделениями

Подразделение ГЗИ в пределах своей компетенции взаимодействует с:

- отделом кадров ОПУ для участия в вопросах предусматривающими допуск к конфиденциальной информации, отражения в личных делах сведений о выявленных нарушениях режима конфиденциальности;
- управлением финансово-экономической деятельности по вопросам оснащения и закупки необходимого оборудования, предназначенного для обеспечения информационной безопасности технических средств входящих в состав информационных систем;
- юридическим отделом ОПУ для своевременного изучения изменений законодательства в области защиты информации;
- структурными подразделениями АСОУ для координации их работы и обеспечения необходимого уровня защиты конфиденциальной информации.

7.3. Структура подразделения ГЗИ

ГЗИ находится в подчинении непосредственного начальника группы защиты информации, который назначается на данную должность ректором АСОУ.

Обязанности работников подразделения ГЗИ определяет непосредственный начальник подразделения ГЗИ.

Подразделение ГЗИ состоит из инженерно-технической группы в состав которой входят инженер и техник по защите информации, системные администраторы, специалисты, отвечающие за выполнение отдельных функций по защите информации.

Задачи инженерно-технической группы:

- обеспечение безопасности деятельности АСОУ с помощью технических средств защиты.
- определение границ контролируемой зоны с учетом возможностей;
- определение состава технических средств, используемых для передачи, приема и обработки конфиденциальной информации в пределах контролируемой зоны;
- обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования;
- выявление и оценка степени опасности технических каналов утечки информации;
- разработка мероприятий по ликвидации (локализации) установленных каналов утечки информации организационными, организационно-техническими или техническими мерами с применением аппаратных средств защиты.

8. ПРАВА И ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ АСОУ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Ректор АСОУ

Организует работу по построению системы защиты информации и организацию общего состояния информационной безопасности в АСОУ.

Наряду с установленными мерами по обеспечению безопасности персональных данных и разработанной организационно-распорядительной документацией, определяющей политику в отношении обработки ПДн в АСОУ, утверждает состав и перечень средств СЗИ, предложенных для обеспечения безопасности ПДн.

Оценивает соотношение вреда, который может быть причинен субъектам ПДн и принимаемых мер по защите ИСПДн.

8.2. Проректор по безопасности

Определяет порядок передачи информации внешним организациям, а также процесс обмена информацией между структурными подразделениями АСОУ.

Организует контроль за оценкой эффективности внедренной системы защиты информационных ресурсов АСОУ от намеренного и ненамеренного разглашения, утери, искажения, похищения;

Осуществляет контроль:

- за работой подразделения по обеспечению защиты информационных ресурсов АСОУ;
- за порядком подготовки, учета и хранения документов конфиденциального характера;
- исполнением приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- наличием в трудовых договорах с работниками, допущенными к информации ограниченного доступа, обязательств о не разглашении информации, содержащей персональные данные, которая стала им известна в связи с исполнением должностных обязанностей.

Проводит разбирательства об имеющихся недостатках и выявленных нарушениях требований руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования информации.

8.3. Проректор по цифровизации

Составляет Перечень процессов и сведений ограниченного доступа, обрабатываемых в АСОУ.

Обеспечивает выполнение организационных и технических мероприятий в АСОУ по инициализации работ по защите информации.

Вносит предложения о внесении изменений в процессы обработки информации, а также в ИСПДн, если это обусловлено необходимостью обеспечения соответствия законодательству в сфере персональных данных.

Определяет состав и перечень средств защиты информации, для обеспечения безопасности ПДн и предлагает их для применения в ИСПДн в процессе обработки информации.

Организует работу подразделения по обеспечению защиты информационных ресурсов АСОУ от намеренного и ненамеренного разглашения, утери, искажения, похищения.

Проводит мероприятия по аттестации и оценки эффективности автоматизированных информационных систем на соответствие нормативным требованиям безопасности.

Принимает участие в подготовки и разработки необходимой отчетной организационно-распорядительной документацией в АСОУ о состоянии работ по защите информации.

Участвует в поощрении или наложении взысканий на работников в связи с исполнением ими обязанностей, связанных с обработкой информации.

8.4. Ответственный за защиту информации:

- разрабатывает и своевременно обновляет организационно-распорядительные документы по вопросам защиты информации;
- своевременно направляет в Управление Роскомнадзора по ЦФО уведомление о намерении Оператора осуществлять обработку персональных данных и сообщает о происшедших изменениях в процессе обработки персональных данных;
- организует работу по получению согласия субъектов персональных данных на обработку персональных данных в случаях, предусмотренных законодательством в данной сфере;
- осуществляет проведение инструктажа пользователей АРМ (доведение под роспись требований инструкции «По работе пользователей с конфиденциальной информацией на АРМ»;
- знакомит работников АСОУ, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;
- осуществляет контроль за соответствием состава АС техническому паспорту (в т.ч. реальной конфигурации информационных связей);
- осуществляет контроль над действиями администратора безопасности и администратора ИС по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам АС, антивирусная защита, резервное копирование данных и т.д.), порядка учета, хранения и обращения с машинными носителями информации;
- обеспечивает защиту информации, циркулирующей на объектах информатизации, участвует в работе по аттестации ИС на соответствие

нормативным требованиям;

- проводит систематический контроль работы СЗИ, применяемых в ИС, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей ИС;
- контролирует порядок учёта и хранения машинных носителей информации;
- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИСПДн;
- принимает меры по оперативному изменению паролей при увольнении или перемещении работников, имевших допуск к ИСПДн;
- требует от руководителей проверяемых подразделений устранения выявленных нарушений и недостатков, дает обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает проректору по безопасности;
- вносит предложения проректору по цифровизации о поощрении или наложении взысканий на работников в связи с исполнением ими обязанностей, связанных с обработкой информации;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

8.5. Работник АСОУ, на которого возложены функции администратора безопасности, системного администратора автоматизированной информационной системы персональных данных:

- обеспечивает настройку и бесперебойную эксплуатацию программных и технических средств обработки ПДн, входящих в состав ИС;
- обеспечивает настройку, бесперебойную эксплуатацию и мониторинг средств защиты информации;
- настраивает права доступа работников к ПДн и средствам их обработки в соответствии с ролевой моделью доступа;
- проводит инструктаж пользователей ИС по правилам эксплуатации программных и технических средств обработки ПДн, а также СЗИ, входящих в состав ИСПДн;
- проводит смену паролей у пользователей ИС не реже одного раза в три месяца либо при компрометации паролей;

- хранит дистрибутивы программного обеспечения средств обработки информации ИС;

- обеспечивает контроль действий представителей сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты информации ИС;

- предоставляет необходимую информацию при проведении проверок регулирующими органами;

- оказывает содействие работникам, участвующим в процессах обработки и обеспечения безопасности ПДн, по вопросам использования средств обработки информации ИС, в рамках своей компетенции;

- незамедлительно уведомляет в случае обнаружения попыток или фактов несанкционированного доступа к ПДн о выявленных фактах ответственного за защиту информации ограниченного доступа.

8.6. Руководители структурных подразделений:

- лично отвечают за защиту информации в структурных подразделениях, сохранность машинных и иных носителей информации;

- организуют выполнение мероприятий по защите информации при использовании технических средств;

- участвуют в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих ИСПДн;

- участвуют в определении правил разграничения доступа к информации в ИСПДн, используемых в АСОУ.

8.7. Пользователи автоматизированной информационной системы персональных данных

Работа пользователей в ИСПДн осуществляться на базе общесистемного лицензионного программного обеспечения, зафиксированного в «Перечне разрешенного к использованию программного обеспечения, установленного в ИСПДн».

Допуск пользователей для работы осуществляется в соответствии со списком постоянных пользователей, предназначенных для обработки информации.

Учет работы пользователей в ИСПДн производится ответственным за защиту конфиденциальной информации (администратором безопасности).

Пользователи имеют право отрабатывать информацию в соответствии с полномочиями прав доступа «Пользователь» к ресурсам автоматизированного рабочего места, присвоенными системным администратором (администратор ИС) каждому пользователю.

Порядок работы:

Пароль на вход в АРМ пользователь получает от администратора ИС.

После включения компьютера пользователь должен ввести свои имя пользователя и пароль.

Для сохранности информации пользователь обязан корректно выключать (перезагружать) свой компьютер. **Обязательно** дождаться пока компьютер не выключиться самостоятельно!

При временном отсутствии пользователя на рабочем месте компьютер должен быть выключен или заблокирован.

В целях предотвращения разрушения и утери обрабатываемой информации на АРМ, пользователь должен осуществлять:

- копирование необходимой информации по мере ее обновления на учтенные в установленном порядке съемные носители;
- проверку магнитных носителей информации, поступивших из других отделов и сторонних организаций, программой - «антивирусом».

При любом сбое ИС, нестабильности в работе АРМ, сети, и т. д. пользователь должен сообщать администратору ИС.

При обнаружении компьютерного вируса пользователь обязан немедленно прекратить какие-либо действия на АРМ и поставить в известность администратора ИС.

Пользователь обязан ставить в известность администратора безопасности в случае появления сведений или подозрений о фактах несанкционированного доступа к информации.

Пользователю запрещается:

- Передавать кому-либо пароль, используемый на компьютере.
- Оставлять записанные пароли в доступных для других сотрудников местах.
- Изменять самостоятельно программное обеспечения (ПО) на компьютере или проводить обновление установленного ПО.
- Оставлять бесконтрольно включенный компьютер, на столе - магнитные носители и распечатанные листы с информацией.
- Выключать (приостанавливать защиту) антивирусный сканер на компьютере.
- Использовать для обработки информации компьютер, не предназначенный для этих целей.
- Использовать компьютер другого пользователя без разрешения администратора безопасности.

9. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

9.1.Планирование работ по защите информации проводится на основании:

- рекомендаций и указаний Роскомнадзора и ФСТЭК России;
- решений Московской областной комиссии по информационной безопасности и рекомендаций подразделения защиты информации Министерства образования Московской области;
- рекомендаций актов проверок контрольными органами;
- результатов анализа деятельности в области защиты информации.

9.2. Для подготовки и реализации организационных и технических мероприятий по защите информации ограниченного доступа, ответственным за

защиту информации ограниченного доступа, составляется годовой план работ по защите информации (далее - годовой план), утверждаемый ректором.

9.3. Контроль выполнения годового плана возлагается на проректора по безопасности АСОУ.

10. КОНТРОЛЬ СОСТОЯНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. С целью своевременного выявления и предотвращения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности СЗИ.

10.2. Контролю подлежат как принятые меры организации обработки информации, так и меры по обеспечению её безопасности.

10.3. В рамках проведения контроля проверяются:

- актуальность описания процессов обработки информации;
- актуальность перечня ИСПДн;
- актуальность перечня лиц, доступ которых к информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- актуальность сведений, указанных в Политике в отношении обработки персональных данных, проверка соблюдения ее положений и общедоступности;
- наличие письменных согласий субъектов ПДн и соответствия форм согласий требованиям законодательства;
- наличие договоров с организациями, которым поручается обработка ПДн ;
- соответствие организации в АСОУ обработки информации, осуществляемой без использования средств автоматизации, требованиям законодательства;
- проверка осведомленности работников АСОУ о положениях законодательства Российской Федерации о персональных данных, документов АСОУ, устанавливающих порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области;
- актуальность сведений, указанных в Уведомлении об обработке персональных данных АСОУ (при необходимости - отправка нового Уведомления в Роскомнадзор).

10.4. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений АСОУ.

10.5. Периодический контроль за эффективностью использования установленных СЗИ осуществляет ответственный за защиту информации ограниченного доступа. Он обязан присутствовать при всех проверках по вопросам защиты информации, результаты которых отражаются в Актах проверок.

10.6. По результатам проверок контролирующими органами, ответственный с привлечением заинтересованных должностных лиц, разрабатывает план устранения выявленных недостатков.

10.7. При обнаружении нарушений ректор АСОУ принимает необходимые меры по их устранению в сроки определенные действующим законодательством.

11. ОТВЕТСТВЕННОСТЬ

11.1. Лица, виновные в нарушении норм, регулирующих обработку информации, несут дисциплинарную, административную, гражданскую, уголовную и иную ответственность предусмотренную законодательством Российской Федерации.

11.2. Прекращение доступа к персональным данным и/или увольнение не освобождает работника АСОУ от принятых обязательств по неразглашению ПДн, ставших доступными при выполнении должностных обязанностей.

Утверждено
приказом АСОУ
от «07» 06 2022 года № 749-04

СТРУКТУРА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСОУ