ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
Южное межрегиональное территориальное управление воздушного транспорта Федерального агентства воздушного транспорта
(Южное МТУ Росавиации)

УТВЕРЖДАЮ
И.о. начальника
Южного МТУ Росавиации
_____А.Е. Макоклюев

«25» 10 2018 г.

ПОЛОЖЕНИЕ
по обеспечению безопасности конфиденциальной информации

1. Основные положения

1.1. Настоящее Положение разработано в соответствии с частью 1 статьи 23, статьи 24 Конституции Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Целью настоящего «Положения по обеспечению безопасности конфиденциальной информации, не содержащей сведения, составляющие государственную тайну» (далее Положение) является регламентация технологического и организационного процесса защиты конфиденциальной информации, в том числе персональных данных в информационных системах Южного МТУ Росавиации (далее - ИС).

1.3. Действие настоящего Положения может быть отменено в связи с утратой актуальности, либо по иным причинам.

2. Принципы защиты информации

2.1. В целях защиты конфиденциальной информации, не содержащей сведения, составляющие государственную тайну, в том числе персональных данных (далее - ЗИ), создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение данной информацией. Целью и результатом несанкционированного доступа к ЗИ может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внедрение вредоносных программ, фальсификация содержания реквизитов документа и др.

2.2. Основным источником несанкционированного доступа к ЗИ является персонал, работающий с документами, содержащими защищаемую информацию.

2.3. Посторонние лица не должны знать информацию о распределении функций, рабочих процессах, технологии составления, оформления, ведения и хранения документов, дел и рабочих материалов в ИС. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к работе ИС, например, посетители, работники других организационных структур.

2.4. Для обеспечения защиты информации необходимо соблюдать следующие организационно-технические меры:

1) регламентация состава работников, функциональные обязанности которых требуют доступа к ЗИ, и процесса предоставления такого доступа;

2) регламентация порядка приёма, учёта и контроля деятельности посетителей;

3) поддержания порядка охраны зданий и помещений;

4) периодический контроль обеспечения защищённости ЗИ;

5) соблюдение требований к защите ЗИ субъектов при интервьюировании и собеседованиях.

В случаях обнаружения несоблюдения условий хранения носителей ЗИ и/или несоблюдения использования средств защиты информации (СЗИ), а также в случае обнаружения нарушения порядка предоставления ЗИ, должно производиться разбирательство и составляться заключение по выявленным фактам.

3. Перечень мер по защите информации, обрабатываемой без использования средств автоматизации

3.1. Для обеспечения защиты материальных носителей, содержащих ЗИ, обрабатываемых в ИС необходимо:

1) довести до сотрудников, осуществляющих обработку ЗИ на материальных носителях, информацию об особенностях и правилах осуществления такой обработки;

2) запретить вынос за пределы служебных помещений носителей, содержащих ЗИ, за исключением случаев, установленных законодательством;

3) хранить носители, содержащие ЗИ, только в сейфах (шкафах), с надёжными средствами защиты, предотвращающими неконтролируемый доступ к ним (места хранения носителей определяются приказом «Об утверждении мест хранения материальных носителей информации, не содержащей сведения, составляющие государственную тайну»);

4) обеспечить учёт материальных носителей, содержащих ЗИ (система учёта должна предоставлять возможность контроля над местонахождением каждого материального носителя);

5) организационно исключить необоснованное ознакомление с ЗИ лиц, не имеющих соответствующих полномочий.

6) обеспечить защиту от несанкционированного доступа и копирования ЗИ на материальных носителях, согласно организационным и распорядительным документам.

4. Контроль защищённости информации

4.1. Необходимо производить периодический контроль выполнения организационно-технических мер, а также контроль защищённости информационных ресурсов, содержащих ЗИ.

4.2. Виды контроля состояния защищённости, применяемые в ИС:

1) предварительный контроль (оценочная проверка обоснованности мер защиты до начала обработки ЗИ) — осуществляется с целью своевременного выявления и предотвращения предпосылок возможных нарушений требований или норм защиты конфиденциальной информации;

2) текущий контроль (проверка в процессе обработки ЗИ) - осуществляется с целью своевременного выявления возникающих трудностей и недостатков реализации, принятых мер защиты персональных данных и выработки мероприятий по их устранению. Текущий контроль может быть периодическим, повседневным или непрерывным;

3) контроль устранения недостатков (проверка, проводимая после устранения ранее допущенных нарушений норм и требований защиты информации, вследствие которых были приостановлены или ограничены работы с ЗИ) - осуществляется с целью выдачи разрешения на продолжение обработки персональных данных субъектов;

4) внутренний контроль - проводится силами уполномоченных работников;

5) организационный контроль - подразумевает проверку состояния полноты и обоснованности мероприятий, по защите защищаемых информационных ресурсов требованиям соответствующих руководящих и нормативных документов;

6) контроль эффективности - проводится с целью проверки соответствия количественных или качественных показателей эффективности мероприятий по защите ЗИ установленным требованиям или нормам эффективности защиты;

7) технический контроль - обеспечивает проверку эффективности защиты с использованием технических и (или) программных средств контроля и в дальнейшем получение наиболее объективной и достоверной информации о состоянии объектов контроля.

5. Организационная структура и обязанности ответственных лиц

5.1. Приказом назначается лицо, ответственное за организацию обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в том числе персональных данных (ответственное лицо) и администратор безопасности информационной системы (администратор безопасности), которые проводят мероприятия по защите ЗИ. При необходимости дополнительно назначаются ответственные лица в структурных подразделениях.

5.2. Ответственное лицо:

1) осуществляет внутренний контроль над соблюдением законодательства Российской Федерации в сфере защиты информации;

2) доводит до сведения работников положения законодательства Российской Федерации, локальных актов по вопросам обработки ЗИ, требований к защите информации;

3) организует приём и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приёмом и обработкой таких обращений и запросов.

5.3. Администратор безопасности отвечает за обеспечение работоспособности элементов ИС и средств защиты информации, обеспечение необходимого уровня состояния защиты ЗИ, правильность настройки средств защиты, организацию выдачи, хранения и уничтожения материальных носителей ЗИ.

6. Обязанности оператора

6.1. Сотрудники, работающие с ИС обязаны использовать ЗИ только в соответствии с целями обработки, определившими ее получение.

6.2. Сотрудники обязаны не отвечать на запросы, связанные с ЗИ, по телефону или факсу.

6.3. Для защиты ЗИ необходимо:

1) в порядке, установленном законодательством РФ, обеспечить защиту ЗИ от неправомерного ее использования или утраты;

2) ознакомить сотрудника с настоящим Положением;

3) осуществлять передачу ЗИ только в соответствии с настоящим Положением и законодательством Российской Федерации;

4) предоставлять ЗИ только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;

5) по запросу ознакомить субъекта персональных данных (ПДн), не являющегося сотрудником, или в случае недееспособности либо несовершеннолетия субъекта, его законного представителя с настоящим Положением;

6) по требованию субъекта ПДн или его законного представителя предоставить ему полную информацию о его персональных данных и порядке обработки этих данных.

При обнаружении нарушений порядка предоставления ЗИ ответственные сотрудники обязаны незамедлительно приостановить предоставление информации пользователям ИС до выявления причин нарушений и устранения этих причин.

7. Права субъектов персональных данных

7.1. Субъекты персональных данных имеют право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему

субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществлённой или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

7.2. Субъекты персональных данных имеют право получать доступ к своим персональным данным, включая право получать копии любой записи, содержащей собственные персональные данные, за исключением случаев, предусмотренных федеральным законом.

7.3. Субъекты персональных данных имеют право требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства.

7.4. При отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта он имеет право заявить в письменной форме о своём несогласии, представив соответствующее обоснование.

7.5. Субъекты персональных данных имеют право требовать от оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях.

7.6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным

нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

8. Ответственность за нарушение норм, регулирующих получение, обработку и защиту информации

8.1. Руководитель, разрешающий доступ сотрудника к документу, содержащему ЗИ, несёт персональную ответственность за данное разрешение.

8.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ЗИ, несут дисциплинарную, материальную, административную, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

8.3. Каждый сотрудник несёт единоличную ответственность за сохранность и конфиденциальность полученной в процессе работы ЗИ.

8.4. За неисполнение или ненадлежащее исполнение сотрудником возложенных на него обязанностей по соблюдению установленного порядка работы с ЗИ руководство оператора вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

8.5. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечёт наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

Начальник ОАХО П.В. Подтележников