ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ КРАСНОДАРСКОГО КРАЯ

ПРИКАЗ

от 24 апреля 2012 года N 3325

ОБ УТВЕРЖДЕНИИ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ КРАСНОДАРСКОГО КРАЯ

В соответствии с Федеральным Законом от 27.07.2006 N 152-ФЗ "О защите персональных данных", с целью принятия мер по защите сведений, обрабатываемых с использованием средств автоматизации, так и без использования таких средств в образовательных учреждениях Краснодарского края приказываю:

1. Утвердить Концепцию информационной безопасности образовательных учреждений Краснодарского края (Приложение N 1).

2. Отделу информационно-технического обслуживания ГУ КК Центр укрепления материально-технической базы образования (Поляков) организовать проведение совещания-семинара с представителями муниципальных органов управления образования, государственных и муниципальных образовательных учреждений Краснодарского края по информационной безопасности.

3. Государственным и муниципальным образовательным учреждениям Краснодарского края принять меры по обеспечению требуемого уровня информационной безопасности.

4. Руководителям муниципальных органов управления образованием Краснодарского края назначить ответственных за информационную безопасность образовательных учреждений муниципального образования.

5. Контроль за исполнением настоящего приказа возложить на заместителя руководителя департамента Н.Е. Байрачного.

Руководитель департамента
Т.П.ХЛОПОВА

Приложение N 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ КРАСНОДАРСКОГО КРАЯ

Приложение N 1
к приказу
департамента образования и науки
Краснодарского края

Утверждаю:
Руководитель департамента
образования и науки
Краснодарского края
Т.П.ХЛОПОВА

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ КРАСНОДАРСКОГО КРАЯ

1. Общие положения

Концепция информационной безопасности образовательных учреждений Краснодарского края (далее - Концепция) разработана на основе Федеральных законов "О персональных данных", "Об образовании", "Об информации, информационных технологиях и о защите информации" с учетом рекомендации по проведению работ в подведомственных Рособразованию учреждениях по обеспечению защиты информационных систем персональных данных.

Под информационной безопасностью учреждений образования Краснодарского края понимается состояние защищенности персональных данных и иной информации ограниченного доступа от внутренних и внешних угроз.

Концепция определяет основные направления деятельности департамента образования и науки Краснодарского края (далее - Департамент) и учреждений образования Краснодарского края (далее - УО) по устранению потенциальных угроз в информационной сфере, содержит цели, задачи и принципы достижения требуемого уровня информационной безопасности, определяет виды угроз безопасности информации и информационные ресурсы, подлежащие защите.

Концепция служит основой для:

формирования организационной основы системы защиты информации;

принятия управленческих решений и разработки практических мер по реализации политики информационной безопасности, выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

формирования краевой отраслевой системы нормативных документов по защите персональных данных;

формирования и реализация единой технической политики в области обеспечения информационной безопасности;

координации деятельности Департамента и УО по обеспечению безопасности персональных данных и информации ограниченного доступа в распределенных информационных системах.

Мероприятия по обеспечению информационной безопасности являются составной частью деятельности Департамента и УО и должны осуществляться на постоянной основе во взаимосвязи с другими мерами по обеспечению установленного режима функционирования информационных систем.

Положения Концепции должны учитываться УО при разработке внутренних документов в области обеспечения информационной безопасности персональных данных и защиты информации ограниченного доступа.

1.1. Роль и место информационной безопасности персональных данных в системе образования Краснодарского края

Широкое внедрение информационных технологий в сферу образования повлекло за собой усиление роли автоматизированных систем в повседневной работе УО и системы образования Краснодарского края в целом.

Повсеместное создание баз данных учащихся и преподавателей, наполнение баз данных информацией об успеваемости, концентрация указанных баз на муниципальном и региональном уровне открыли потенциальные возможности для нарушителя по краже, модификации или уничтожению информации ограниченного доступа в значительных объемах.

Уже на данном этапе информатизации системы образования Краснодарского края дестабилизация информационных систем Департамента и УО может привести к нарушению и даже остановке образовательного процесса.

Необходимость усиления роли информационной безопасности в образовательном процессе также подчеркивается процедурой проведения Единого государственного экзамена, эффективность которого напрямую зависит от обеспечения информационной безопасности контрольных измерительных материалов до и во время проведения экзамена.

Одним из приоритетов развития информационной сферы Российской Федерации является защита прав и интересов детей в сети Интернет. Задачей Департамента и УО является не только обеспечение безопасного доступа несовершеннолетних к ресурсам всемирной сети в ходе образовательного процесса, но и обучение подрастающего поколения правилам безопасной работы и безопасного общения в сети Интернет.

При проведении государственного контроля за обработкой персональных данных ответственными федеральными службами (к таким относят Роскомнадзор, ФСТЭК и ФСБ) могут быть выявлены несоответствия процессов обработки и защиты персональных данных в УО, что может повлечь за собой административную ответственность вплоть до приостановки деятельности УО.

Обобщив все вышесказанное, можно сказать об усилении роли информационной безопасности в работе УО и необходимости адекватного увеличения внимания к этому вопросу со стороны руководства и сотрудников УО.

1.2. Объекты защиты

Объектами защиты в УО являются персональные данные и иная информация ограниченного доступа, материальные носители и средства обработки персональных данных и иной информации ограниченного доступа, а также пользователи информационных систем и обслуживающий персонал.

К информации ограниченного доступа относят:

любую информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) (далее - персональные данные);

контрольные измерительные материалы Единого государственного экзамена;

контрольные измерительные материалы экзаменов УО;

сведения о научной и научно-технической деятельности учащихся и преподавателей до официальной публикации их в открытых источниках;

иную информацию, доступ к которой ограничивается по решению руководства УО.

Объектами защиты являются персональные данные следующих категорий субъектов:

учащиеся УО и их родственники;

сотрудники Департамента и УО, а также члены их семей.

Ввиду того, что персональные данные обрабатываются и накапливаются с помощью ЭВМ, основным объектом защиты являются информационные системы персональных данных (далее - ИСПДн), в состав которых входят автоматизированные рабочие места (далее - АРМ) пользователей системы, сервера, коммутационное оборудование, базы данных, системы хранения информации, системное и прикладное программное обеспечение и другие средства вычислительной техники.

В соответствии с ч. 1 ст. 1 152-ФЗ "О персональных данных" персональные данные, обрабатываемые без использования средств автоматизации, являются объектом защиты, если характер работы с ними позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных (далее - картотеки персональных данных).

2. Основные цели и задачи обеспечения информационной безопасности персональных данных

2.1. Цели обеспечения информационной безопасности персональных данных

Основными целями деятельности по обеспечению информационной безопасности персональных данных являются:

защита прав граждан в сфере образования и обеспечение связанных с этими правами государственных гарантий;

защита персональных данных учащихся и сотрудников УО;

повышение эффективности использования современных информационных технологий - информационных систем персональных данных - в ходе образовательного процесса.

2.2. Задачи обеспечения информационной безопасности персональных данных

Задачами деятельности по обеспечению информационной безопасности персональных данных являются:

создание единой системы информационной безопасности, включающей в себя общий подход к построению систем информационной безопасности отдельных УО и Департамента образования и науки;

координация деятельности по обеспечению информационной безопасности Департамента и УО;

поддержание системы обеспечения информационной безопасности в состоянии, устойчивом к существующим и вновь выявляемым угрозам в информационной сфере;

разработка и внедрение в информационную инфраструктуру Департамента и УО современных методов и средств обеспечения информационной безопасности;

организация контроля состояния и оценки эффективности системы информационной безопасности и реализация мер по ее совершенствованию;

повышение осведомленности пользователей информационных систем персональных данных в вопросах обеспечения информационной безопасности персональных данных;

предупреждение, выявление и расследование инцидентов в области информационной безопасности.

3. Угрозы информационной безопасности персональных данных

Под угрозами информационной безопасности понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации путем несанкционированных и/или непреднамеренных воздействий на нее.

В соответствии с п. 8 Порядка проведения классификации информационных систем персональных данных <1>, угрозы информационной безопасности в УО по их функциональной направленности подразделяются на:

_____

<1> Утвержден Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года N 55/86/20

угрозы конфиденциальности персональных данных, выражающиеся в организации перехвата, хищения (открытого, тайного) персональных данных или средств обработки. Также данные угрозы могут быть сопряжены с утратой (неумышленной потерей) персональных данных, либо средств обработки;

угрозы целостности персональных данных, выражающиеся в организации несанкционированного уничтожения, искажения информации. Также данные угрозы сопряжены с нарушением установленных режимов работы аппаратно-программных средств обработки персональных данных;

угрозы доступности информации, выражающиеся в организации блокирования доступа к персональным данным или средствам обработки.

3.1. Виды угроз информационной безопасности персональных данных

Угрозы информационной безопасности УО по их предметной направленности подразделяются на:

угрозы информационным системам персональных данных;

угрозы информационной инфраструктуре Департамента и УО;

угрозы правам граждан в сфере образования (в том числе правам и интересам несовершеннолетних).

3.1.1. Угрозы информационным системам персональных данных

Угрозы информационным системам проявляются в виде:

осуществления несанкционированного доступа к ИСПДн с целью их противоправного использования;

хищения персональных данных из баз данных ИСПДн;

противозаконного сбора, накопления и использования персональных данных;

перехвата персональных данных техническими средствами;

внедрения электронных устройств съема информации в технические средства ИСПДн, системы связи и передачи данных, а также служебные помещения и кабинеты руководителей;

уничтожения, повреждения, нарушения или хищения электронных (машинных) и других носителей персональных данных;

навязывания ложной информации в сетях передачи данных и линиях связи Департамента и УО;

нарушения установленных ограничений на распространение и доступ к персональным данным.

3.1.2. Угрозы информационной инфраструктуре

Угрозы информационной инфраструктуре проявляются в виде:

нарушения технологии обработки персональных данных;

нарушения адресности и своевременности информационного обмена;

внедрения в технические и программные средства специальных компонентов, не предусмотренных функциональным назначением и документацией на эти изделия;

внедрения и распространения программ, нарушающих нормальное функционирование ИСПДн, систем связи и передачи данных, в том числе систем защиты персональных данных;

уничтожения, повреждения, блокирования, радиоэлектронного подавления или разрушения технических средств ИСПДн, систем связи и передачи данных;

хищения программных или аппаратных ключей, средств криптографической защиты информации;

воздействия на парольно-ключевые системы защиты персональных данных.

3.1.3. Угрозы правам граждан в сфере образования

Данные угрозы проявляются в виде:

несанкционированного доступа посторонних лиц к персональным данным с целью противоправного использования (например, изменения результатов контрольных мероприятий);

получения сведений о контрольных измерительных материалах;

навязывания подрастающему поколению ложных общечеловеческих ценностей, нравственного разложения, разжигания межнациональной розни и т.д.

3.2. Источники угроз информационной безопасности персональных данных

Источники угроз информационной безопасности персональных данных подразделяются на внешние и внутренние.

К числу внешних источников угроз относятся:

деятельность политических, экономических, общественных структур и отдельных лиц, направленная на противозаконное добывание персональных данных, нарушение принципов государственной политики в области образования;

информационный терроризм с целью дестабилизации системы образования Краснодарского края;

стихийные бедствия и катастрофы.

К внутренним источникам угроз информационной безопасности относятся:

непреднамеренные воздействия на порядок работы средств вычислительной техники ИСПДн, вызванные низкой квалификацией, невнимательностью или недисциплинированностью сотрудников УО;

несанкционированные действия сотрудников, направленные на получение персональных данных, изменение результатов экзаменов, получение контрольных измерительных материалов и т.д. против правил доступа информационных систем УО;

действие или бездействие сотрудников, повлекшее за собой несанкционированный доступ к персональным данным, нарушение прав и интересов несовершеннолетних и т.д.;

противоправные действия сотрудников сторонних организаций, осуществляющих поставку, установку и сервисное обслуживание средств вычислительной техники УО, программного обеспечения, оборудования связи и т.д.;

противоправные действия сотрудников сторонних организаций или посетителей, находящихся внутри периметра информационной инфраструктуры УО, пользующихся локальными информационными ресурсами УО и (или) имеющих доступ к средствам вычислительной техники УО;

несовершенство системы обеспечения информационной безопасности УО, отсутствие четкого механизма разграничения полномочий пользователей и доступа к персональным данным и иной информации ограниченного доступа;

использование импортных технических средств и программных продуктов, отсутствие регламентированной политики по унификации и стандартизации аппаратно-программных средств, внедряемых в УО;

недостаточная координация деятельности Департамента и УО по обеспечению информационной безопасности персональных данных;

отказы технических средств и сбои программного обеспечения в информационных системах УО, системах связи и передачи данных.

4. Основные принципы и меры по обеспечению информационной безопасности персональных данных

4.1. Основные принципы обеспечения информационной безопасности персональных данных

Информационная инфраструктура должна обеспечивать надежное взаимодействие между различными УО и Департаментом образования и науки в ходе повседневной образовательной деятельности, а также санкционированное взаимодействие с внешними абонентами: федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, юридическими лицами различных организационно-правовых форм.

Система обеспечения информационной безопасности должна строиться на следующих основных принципах:

соответствия реализуемых в ней организационно-технических решений требованиям законодательства Российской Федерации, нормативным документам федеральных органов исполнительной власти, уполномоченных на осуществление деятельности в сфере защиты информации, а также рекомендациям Рособразования;

единства руководства в вопросах определения и реализации общей стратегии противодействия информационным угрозам, научно-технической политики и методического обеспечения информационной безопасности;

непрерывности функционирования;

оценки эффективности и достаточности принимаемых мер защиты и корректировки их состава и содержания;

способности к масштабируемости и модернизации при появлении новых угроз и объектов защиты информации;

минимизации затрат на ее создание и поддержание в актуальном состоянии;

соответствия требований по обеспечению информационной безопасности, предъявляемых к создаваемым (модернизируемым) информационным системам, системам связи и передачи данных, реальным угрозам;

применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

4.2. Меры обеспечения информационной безопасности персональных данных

Меры обеспечения информационной безопасности должны носить упреждающий характер и быть направлены на предотвращение инцидентов, реализующих угрозы информационной безопасности.

В целях нейтрализации угроз информационной безопасности применяются правовые, организационные и организационно-технические меры защиты информации.

Правовые меры предусматривают разработку в УО внутренних нормативных документов, регламентирующих вопросы защиты персональных данных и иной информации ограниченного доступа.

С целью создания необходимого правового поля функционирования системы информационной безопасности сотрудники УО дают письменное обязательство о неразглашении персональных данных, контрольных измерительных материалов и иной информации ограниченного доступа и соблюдении принципов государственной политики в области образования, указанных в ст. 2 Федерального закона N 3266-1 "Об образовании".

Невыполнение сотрудниками УО требований по информационной безопасности приравнивается к невыполнению должностных обязанностей и может повлечь за собой, как минимум, дисциплинарную ответственность.

Организационные меры предусматривают:

назначение ответственных за организацию обработки персональных данных и иной информации ограниченного доступа, за техническое обслуживание средств защиты информации и технических средств информационных систем, за хранение материальных носителей персональных данных и контрольных измерительных материалов;

ознакомление работников с внутренними и внешними документами в области защиты персональных данных и информации ограниченного доступа под роспись;

повышение ответственности работников и руководителей всех уровней за выполнение установленных требований по защите информации;

проведение контроля за соблюдением работниками УО требований по обеспечению безопасности персональных данных и информации ограниченного доступа;

повышение осведомленности несовершеннолетних и их родителей в вопросах информационной безопасности и интернет-угроз;

прием и обработку обращений и запросов субъектов персональных данных или их представителей;

уведомление уполномоченного органа по защите прав субъектов персональных данных (РОСКОМНАДЗОР) о начале обработки персональных данных в случаях, предусмотренных ст. 22 152-ФЗ "О персональных данных".

Организационно-технические меры обеспечения информационной безопасности предусматривают:

установление правил доступа к ИСПДн в соответствии с должностными обязанностями сотрудников УО;

регистрацию всех действий пользователей ИСПДн;

обучение пользователей и персонала, обслуживающего системы защиты информации, правилам и способам работы с подсистемой информационной безопасности ИСПДн;

учет машинных носителей персональных данных;

проведение аттестации ИСПДн по требованиям безопасности информации;

унификацию и стандартизацию средств защиты информации;

использование сертифицированных средств защиты информации (в том числе средств шифрования);

проведение анализа эффективности и достаточности принятых мер по защите информации, разработку и реализацию предложений по совершенствованию систем защиты информации;

выявление незарегистрированных технических устройств и программного обеспечения, в том числе имеющего признаки контрафактности;

противодействие перехвату информации в каналах связи ИСПДн;

организацию безопасного доступа к ресурсам сети Интернет и контентную фильтрацию интернет-трафика;

резервирование информации и ее восстановление в случае возникновения инцидентов информационной безопасности;

использование пожарно-охранной сигнализации для физической

безопасности технических средств и персонала ИСПДн;

обеспечение гарантированной доступности информационных ресурсов ИСПДн с помощью:

резервирования оборудования и каналов связи;

балансировки нагрузки на сервера и каналы связи Департамента и УО;

обеспечения гарантированного электропитания.

контроль с использованием, в том числе, программных и технических средств за действиями пользователей ИСПДн и реакцию на нарушение установленных правил защиты информации.

Важное место среди перечисленных мер занимают мотивация, экономическое стимулирование и психологическая поддержка деятельности персонала, занятого обеспечением информационной безопасности.

4.3. Особенности обеспечения информационной безопасности персональных данных в сфере образования

Спецификой работы ИСПДн Департамента и УО является:

большой объем обрабатываемой информации;

территориальная распределенность УО по Краснодарскому краю;

использование каналов связи с низкой пропускной способностью;

отсутствие квалифицированных кадров в области обеспечения информационной безопасности;

устаревший парк компьютерной техники;

остаточное финансирование вопросов информационной безопасности;

низкий уровень информационной грамотности пользователей информационных систем.

Перечисленные факторы формируют дополнительные направления работ по обеспечению информационной безопасности:

планирование деятельности подразделений информационной безопасности с учетом ограниченных финансовых и людских ресурсов УО;

проведение мероприятий по обучению сотрудников УО правилам безопасной работы с информационными ресурсами (в т.ч. в сети Интернет).

5. Работа с инцидентами в области информационной безопасности персональных данных

Инциденты в области информационной безопасности возникают при нарушении правил и требований информационной безопасности.

В ходе инцидента реализуются (или создается возможность для реализации) угрозы информационной безопасности, что, как правило, приводит к нанесению вреда УО и (или) субъекту персональных данных.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы безопасности персональных данных и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов информационных систем персональных данных.

Работа с инцидентами включает в себя 3 направления:

выявление инцидентов в области информационной безопасности;

реакция на инциденты в области информационной безопасности;

предупреждение инцидентов в области информационной безопасности.

Работа по выявлению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

выявление инцидентов в области информационной безопасности с помощью технических средств;

выявление инцидентов в области информационной безопасности в ходе мероприятий по контролю за обработкой персональных данных и информации ограниченного доступа;

выявление инцидентов с помощью персонала Департамента и УО.

Реакция на инциденты в области информационной безопасности включает в себя:

фиксацию инцидента в области информационной безопасности;

определение границ инцидента и ущерба (в том числе потенциального) от реализации угроз информационной безопасности в ходе инцидента;

ликвидацию последствий инцидента и полное либо частичное возмещение ущерба;

наказание виновных в инциденте информационной безопасности.

Предупреждение инцидентов строится на:

планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками Департамента и УО;

проведении мероприятий по обучению сотрудников Департамента и УО правилам работы со средствами защиты информации в ИСПДн;

доведении до сотрудников норм законодательства и внутренних документов Департамента и УО, устанавливающих ответственность за нарушение требований информационной безопасности;

разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимающимися на работу;

своевременной модернизации системы обеспечения информационной безопасности ИСПДн с учетом возникновения новых угроз информационной безопасности;

своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

5.1. Причины инцидентов в области информационной безопасности

Причинами инцидентов в области информационной безопасности являются:

действие враждебных интересам Департамента и УО организаций и отдельных лиц;

отсутствие персональной ответственности за невыполнение требований защиты информации;

недостаточная работа с персоналом по соблюдению необходимого режима конфиденциальности персональных данных и иной информации ограниченного доступа;

отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;

недостаточная техническая оснащенность подразделений информационной безопасности;

совмещение должностных обязанностей по разработке и сопровождению или сопровождению и контролю за информационными системами;

наличие привилегированных бесконтрольных пользователей в информационной системе;

пренебрежение правилами и требованиями информационной безопасности сотрудниками Департамента и УО;

другие причины.

5.2. Расследование инцидентов в области информационной безопасности

Расследование инцидентов в области информационной безопасности должно включать в себя:

формирование комиссии по расследованию инцидента в области информационной безопасности;

определение границ инцидента - информационных ресурсов, технических средств и персонала, затронутых инцидентом;

определение причин инцидента, факторов, влияющих на возникновение инцидента;

определение участников инцидента;

определение последствий инцидента;

составление заключения по результатам расследования;

выработку рекомендаций по предотвращению возникновения подобных инцидентов в будущем.

5.3. Работа с персоналом по предупреждению инцидентов

Как правило, самым слабым звеном в любой системе безопасности является человек. Наличие современных доступных способов воздействия на персонал, таких как социальная инженерия, фишинг, подмена электронных идентификаторов, номеров телефонов и т.д., делает пользователя информационной системы частым объектом внимания злоумышленника. Поэтому направление работы с персоналом является основным направлением работы подразделений информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал Департамента и УО является также важным источником сведений об инцидентах информационной безопасности. Поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются поводом для смягчения либо отмены наказания за нарушение требований информационной безопасности.

6. Организационная основа системы обеспечения

информационной безопасности

Организационная основа системы обеспечения информационной безопасности должна решать следующие основные задачи:

формирование и совершенствование документальных и технических элементов системы обеспечения информационной безопасности;

обеспечение соответствия организации защиты персональных данных установленным требованиям;

реализация единой технической политики информационной безопасности в сфере образования Краснодарского края;

мониторинг внутренних и внешних условий функционирования объектов защиты, анализ эффективности управления защитой информации и подготовка решений по корректировке состава и содержания структурных элементов системы обеспечения информационной безопасности.

Основными участниками организационной основы системы обеспечения информационной безопасности сферы образования Краснодарского края являются:

руководитель Департамента образования и науки;

заместитель руководителя, курирующий вопросы защиты персональных данных, контрольных измерительных материалов и иной информации ограниченного доступа;

структурное подразделение Департамента, ответственное за организацию работ по защите персональных данных в УО Краснодарского края;

руководители УО;

ответственные за организацию обработки персональных данных в УО.

Ответственность за обеспечение информационной безопасности персональных данных и иной информации ограниченного доступа в УО возлагается на руководителей УО.

7. Документальная основа системы обеспечения информационной безопасности персональных данных

Для обеспечения деятельности по защите персональных данных в УО могут разрабатываться следующие внутренние документы:

документ, определяющий политику УО в отношении обработки персональных данных и содержащий сведения о реализуемых требованиях к защите персональных данных;

уведомление уполномоченного органа по защите прав субъектов персональных данных или справка о причинах неуведомления;

документы, подтверждающие законность обработки персональных данных (договора с субъектами, письменные согласия на обработку персональных данных, нормативные акты Российской Федерации), устанавливающие цели, условия, категории и сроки обработки персональных данных;

приказ о назначении ответственного за организацию обработки персональных данных в УО;

перечень сотрудников, имеющих право доступа к информационным системам персональных данных и картотекам;

приказ о назначении ответственных за техническое обслуживание средств вычислительной техники ИСПДн;

документ, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

документы по применению правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 152-ФЗ "О персональных данных";

документы по контролю за принимаемыми мерами по обеспечению безопасности персональных данных и оценке уровня защищенности ИСПДн;

документы по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований 152-ФЗ "О персональных данных", соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей по защите персональных данных;

документы по ознакомлению/обучению сотрудников с положениями законодательства Российской Федерации в области персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных

данных, локальными актами по вопросам обработки персональных данных;

документы, утверждающие места хранения материальных носителей персональных данных и ответственных лиц;

документ, определяющий угрозы безопасности персональных данных при их обработке в ИСПДн;

документы, подтверждающие уничтожение, обезличивание или блокирование персональных данных, цели обработки которых достигнуты;

обязательство о неразглашении персональных данных.

8. Техническая основа системы обеспечения информационной безопасности персональных данных

Техническая защита ИСПДн осуществляется на основе требований руководящих документов ФСТЭК и ФСБ, с учетом модели угроз.

Состав защитных подсистем ИСПДн может включать в себя:

подсистему управления доступом;

подсистему регистрации и учета;

подсистему обеспечения целостности;

подсистему антивирусной защиты;

подсистему обнаружения атак;

подсистему защиты от утечек защищаемой информации;

подсистему анализа защищенности;

подсистему резервирования и восстановления информации;

подсистему гарантированного электропитания;

подсистему управления средствами защиты информации;

подсистему межсетевого экранирования;

подсистему криптографической защиты каналов связи;

подсистему шифрования носителей информации;

подсистему корреляции событий информационной безопасности;

подсистему обеспечения инженерно-технической защиты;

подсистему обеспечения защиты информации от утечки по техническим каналам.

В зависимости от актуальности угроз информационной безопасности состав защитных подсистем может быть изменен.

ИСПДн должны проходить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию. Принятые в эксплуатацию ИСПДн должны проходить контроль эффективности защиты информации не реже 1 раза в год. Общепринятой практикой

становится периодическое проведение тестирования на проникновение с целью выявления брешей в системе обеспечения информационной безопасности УО.

К проведению работ по проектированию и внедрению средств защиты информации должны привлекаться организации, имеющие лицензии ФСТЭК и ФСБ на оказание услуг в области защиты конфиденциальной информации.

Средства защиты информации (в том числе средства шифрования) должны пройти в установленном порядке процедуру оценки соответствия, которой является добровольная сертификация в федеральном органе исполнительной власти, уполномоченном в области противодействия техническим разведкам и технической защиты информации (ФСТЭК) и (или) в федеральном органе исполнительной власти, уполномоченном в области обеспечения безопасности (ФСБ).