АДМИНИСТРАЦИЯ КУРСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 30.08.2018 Курск № 347-ра

Об утверждении Основных направлений политики информационной безопасности органов исполнительной власти Курской области

В соответствии с Концепцией защиты информации в Курской области, утвержденной постановлением Губернатора Курской области от 02.03.2015 №85-пг, и в целях развития и использования информационных технологий на территории Курской области (региональной информатизации) и обеспечения защиты информации:

1. Утвердить прилагаемые Основные направления политики информационной безопасности органов исполнительной власти Курской области.

2. Руководителям органов исполнительной власти Курской области, являющихся юридическими лицами, определить администраторов безопасности государственных информационных систем.

3. Возложить на областное казенное учреждение «Центр электронного взаимодействия» обязанности администратора безопасности государственных информационных систем органов исполнительной власти Курской области, не являющихся юридическими лицами.

4. Рекомендовать органам местного самоуправления Курской области разработать основные направления политики информационной безопасности органов местного самоуправления на основе Основных направлений политики информационной безопасности органов исполнительной власти Курской области.

5. Контроль за исполнением настоящего распоряжения возложить на Управляющего делами Администрации Курской области А.Т.Стрелкова.

6. Распоряжение вступает в силу со дня его подписания.

Управляющий делами Администрации Курской области
Отдел делопроизводства

Губернатор
Курской области А.Н.Михайлов

305264 596109

УТВЕРЖДЕНЫ
распоряжением Администрации
Курской области
от 30.08.2018 № 347 -ра

Основные направления политики информационной безопасности органов исполнительной власти Курской области

1. Термины, определения и сокращения

1.1. **Обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

1.2. **Безопасность информации** – состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

1.3. **Доступность информации** – свойство информации, при котором имеется возможность получения информации и ее использования.

1.4. **Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя, при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право.

1.5. **Целостность информации** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

1.6. **Единая информационная коммуникационная среда Курской области** - региональная система обмена информацией, построенная с использованием технико-технологических решений.

1.7. **Защита информации от несанкционированного доступа** – комплекс мер, направленный на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

1.8. **Информация ограниченного доступа** – информация, доступ к которой ограничен федеральным или региональным законодательством.

1.9. **Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

1.12. **Биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные).

1.13. **Система защиты информации органа власти** – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

1.14. **Средство защиты информации от несанкционированного доступа** – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

1.15. **Угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

1.16. ПДн - персональные данные.

1.17. ИС - информационные системы.

1.18. ИСПДн – информационная система персональных данных.

1.19. ЕИКС - единая информационная коммуникационная среда Курской области.

1.20. НСД - несанкционированный доступ.

1.21. ОИВ - орган исполнительной власти.

1.22. Инструкция - Инструкция администратора безопасности информационной системы.

1.23. СЗИ - система защиты информации.

1.24. МНИ - машинный носитель информации.

1.25. АРМ – автоматизированное рабочее место.

1.26. МЭ – межсетевое экранирование.

1.27. ОИ – объект информатизации.

1.28. ПО – программное обеспечение.

1.29. Федеральным законом № 152-ФЗ - Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».

2. Общие положения

2.1. Цели и задачи Основных направлений политики информационной безопасности.

Основные направления политики информационной безопасности ОИВ Курской области определяют систему приоритетов, принципов и методов достижения информационной безопасности конфиденциальной информации и электронных информационных ресурсов ОИВ Курской области. Меры защиты информации, определенные Основными направлениями политики информационной безопасности (далее – Политика), направлены на нейтрализацию актуальных угроз информационной безопасности, потенциально опасных для конфиденциальной информации, обрабатываемой в ОИВ Курской области.

Область действия Политики распространяется на ПДн, иную конфиденциальную информацию, а также ИС, входящие в состав ЕИКС ОИВ Курской области (далее при совместном упоминании – «объекты защиты»). Область действия Политики не распространяется на процессы, в рамках которых производится обработка информации, отнесенной в соответствии с законодательством Российской Федерации к сведениям, составляющим государственную тайну.

Политика направлена на обеспечение интересов Курской области и Российской Федерации в целом путем обеспечения надежного бесперебойного и безопасного использования ПДн, прочей конфиденциальной информации, а также ИС, входящих в состав ЕИКС ОИВ Курской области.

Политика структурирует цели и задачи ОИВ Курской области в сфере обеспечения защиты информации, уточняет приоритеты защиты информации исходя из требований законодательства Российской Федерации, нормативных документов Курской области и локальных нормативных актов ОИВ Курской области.

Политика основывается на том, что процесс обеспечения защиты информации является комплексной, многоуровневой и системной задачей, включающей различные объекты и цели защиты, учитывающей характер угроз, способы противодействия им и критерии оценки эффективности систем обеспечения информационной безопасности.

Документ разработан для реализации основных методологических подходов, формирования принципов и направлений работ по обеспечению информационной безопасности сотрудниками ОИВ Курской области.

2.2. Принципы обеспечения информационной безопасности ОИВ Курской области.

Обеспечение защиты информации в ОИВ Курской области осуществляется в соответствии с законодательством Российской Федерации, государственными нормативно-методическими документами в области защиты информации, нормативно-методическими документами, утвержденными ОИВ Курской области и приказами комитета

информатизации, государственных и муниципальных услуг Курской области.

Целями обеспечения защиты информации являются:

обеспечение конфиденциальности, доступности и целостности ПДн и иной информации ограниченного доступа;

обеспечение непрерывности функционирования ЕИКС Курской области;

создание системы обеспечения защиты информации, направленной на нейтрализацию актуальных угроз информационной безопасности;

снижение уязвимости информационных активов, входящих в состав ЕИКС Курской области.

Требования к СЗИ ИС, входящих в состав ЕИКС ОИВ Курской области, определяются на основании класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

Обеспечение защиты информации осуществляется посредством реализации следующих мер:

формирование требований к защите информации, содержащейся в ИС;

разработка СЗИ ИС;

внедрение СЗИ ИС;

аттестация ИС по требованиям защиты информации (далее - Аттестация) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной ИС;

обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации;

контроль реализации мер информационной безопасности с целью поддержания должного уровня информационной безопасности.

Таким образом, цель обеспечения защиты информации заключается в создании, эксплуатации и поддержании должного уровня защиты информации в отношении объектов защиты и информации, обрабатываемой в них.

В основе обеспечения защиты информации ОИВ Курской области лежит комплексный подход, включающий в себя следующие меры:

определение юридических норм взаимоотношения с внешними организациями;

определение организационной структуры и подчинения органов, задействованных в процессе обеспечения защиты информации;

определение административных норм и регламентов, устанавливающих обязанности и ответственность сотрудников;

определение организационно-технических норм и регламентов, определяющих порядок обеспечения защиты информации в ИС, входящих в состав ЕИКС;

использование программных и аппаратных средств защиты информации;

мониторинг и контроль реализации мер защиты информации.

Методическое руководство, разработку региональной нормативной базы в сфере защиты информации и контроль по вопросам обеспечения защиты информации в ОИВ Курской области и (в случае необходимости) в их подведомственных учреждениях осуществляет комитет информатизации, государственных и муниципальных услуг Курской области.

Комитет информатизации, государственных и муниципальных услуг Курской области совместно с областным казенным учреждением «Центр электронного взаимодействия» организует работу по созданию и обеспечению защиты информации объектов защиты от угроз информационной безопасности в органах исполнительной власти Курской области, которые не являются юридическими лицами.

2.3. Организационная структура СЗИ ОИВ Курской области.

Организационная структура СЗИ ОИВ Курской области определяется в соответствии с Концепцией защиты информации в Курской области, утвержденной постановлением Губернатора Курской области от 02.03.2015 №85-пг.

Организационная структура СЗИ ОИВ:

Губернатор Курской области – возглавляет СЗИ в Курской области;

комиссия по информационной безопасности при Губернаторе Курской области – координирует деятельность по защите информации государственных и муниципальных органов власти и организаций;

комитет информатизации, государственных и муниципальных услуг Курской области - организует деятельность по защите информации в ОИВ Курской области;

функции по защите информации в органах исполнительной власти Курской области, которые не являются юридическими лицами, исполняются областным казенным учреждением «Центр электронного взаимодействия»;

ОИВ Курской области, которые являются юридическими лицами, создают структурные подразделения или назначают ответственных сотрудников, на которых возлагаются функции по защите информации в данных ОИВ Курской области, также в ОИВ определяются лица в должности не ниже заместителя руководителя, которые осуществляют организующие и контрольные функции за соблюдением требований по защите информации. Данные ОИВ самостоятельно организуют деятельность по обеспечению защиты информации в своих подведомственных учреждениях.

Основным контролирующим органом по защите информации в ОИВ Курской области является комитет по информатизации, государственных и муниципальных услуг Курской области. Подведомственные учреждения контролируются ОИВ Курской области, в чьей сфере ведения они находятся.

2.4. Управление системой защиты информации ОИВ Курской области.

В целях управления защитой информации ОИВ Курской области проводятся мероприятия по анализу и улучшению системы защиты ИС, входящих в состав ЕИКС, и тестированию работоспособности системы защиты ПДн, и сведений конфиденциального характера. В рамках проводимых мероприятий осуществляются:

контроль за событиями безопасности и действиями пользователей в ИС;

контроль (анализ) защищенности информации, содержащейся в ИС;

анализ и оценка функционирования СЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании СЗИ ИС;

периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

принятие решений по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ, повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

Контрольные мероприятия могут осуществляться ОИВ Курской области самостоятельно либо с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Периодичность проведения контрольных мероприятий определяется исходя из требований, предъявляемых к информации, обрабатываемой в ИС, но не реже 1 раза в квартал.

2.5. Правила обеспечения защиты информации в ИС ОИВ Курской области.

Для нейтрализации угроз информационной безопасности, актуальных для ИС, входящих в состав ЕИКС (обрабатывающих ПДн и иную конфиденциальную информацию) ОИВ Курской области, реализуются группы мер обеспечения защиты информации в соответствии с определёнными требованиями к СЗИ, в том числе:

идентификация и аутентификация субъектов и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

применение мер ограничения программной среды;

защита МНИ, на которых хранятся и (или) обрабатываются ПДн и иная конфиденциальная информация;

регистрация событий безопасности;

обеспечение антивирусной защиты;

реализация мер по обнаружению (предотвращению) вторжений;

контроль (анализ) защищенности ПДн и иной конфиденциальной информации;

обеспечение целостности информационных систем, ПДн и иной защищаемой информации;

обеспечение доступности ПДн и иной защищаемой информации;

реализация мер защиты среды виртуализации;

реализация мер по защите технических средств;

осуществление защиты ИС, их средств, систем связи и передачи данных;

реализация мер по выявлению инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ПДн и иной конфиденциальной информации, реагирование на них;

осуществление мер по управлению конфигурацией ИС и систем защиты ПДн.

Обязанности и порядок действий администратора безопасности и пользователей ИС определенны в соответствующих инструкциях, которые приведены в приложениях № 1 и № 2 к настоящей Политике.

Обладатель информации в случаях, установленных законодательством Российской Федерации, обязан обеспечить постоянный контроль за обеспечением уровня защищенности информации.

Рекомендации по проведению контроля обеспечения целостности, устойчивости функционирования и безопасности ИС, доступных в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), приведены в приложении № 3 к настоящей Политике.

3. Обработка ПДн в ОИВ Курской области

3.1. Принципы обработки ПДн.

При организации обработки ПДн в ОИВ Курской области соблюдаются следующие принципы:

законности;

ограничения обработки ПДн достижением конкретных, заранее определенных и законных целей;

недопущения обработки ПДн, несовместимой с целями сбора ПДн;

недопущения объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

обработки только тех ПДн, которые отвечают целям их обработки;

соответствия содержания и объема обрабатываемых ПДн заявленным целям обработки;

недопущения обработки ПДн, избыточных по отношению к заявленным целям их обработки;

обеспечения точности, достаточности и актуальности ПДн по отношению к целям обработки ПДн;

уничтожения либо обезличивания ПДн по достижении целей их обработки или, в случае утраты необходимости, в достижении этих целей, при невозможности устранения допущенных нарушений при обработке ПДн, если иное не предусмотрено федеральным законодательством.

3.2. Условия обработки персональных данных.

Обработка ПДн ОИВ Курской области осуществляется при соблюдении одного из перечисленных ниже условий:

обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ОИВ Курской области функций, полномочий и обязанностей;

обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

обработка ПДн необходима для осуществления прав и законных интересов ОИВ Курской области или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее – Общедоступные ПДн);

осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Получение и обработка ПДн (предоставление ОИВ Курской области доступа к обработке ПДн) в случаях, предусмотренных Федеральным законом № 152-ФЗ, осуществляется ОИВ Курской области с письменного согласия субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного квалифицированной электронной подписью.

Согласие на обработку ПДн дается субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом № 152-ФЗ.

ОИВ Курской области вправе обрабатывать ПДн без согласия субъекта ПДн (или при отзыве субъектом ПДн согласия на обработку ПДн) при наличии законных оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федеральным законом №152-ФЗ.

Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, органами исполнительной власти Курской области осуществляется в соответствии с основаниями, указанными в части 2 статьи 10 Федеральным законом № 152-ФЗ.

Обработка биометрических ПДн в ОИВ Курской области допускается только при наличии согласия субъекта ПДн. Обработка биометрических ПДн допускается в случаях реализации международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

ПДн субъекта ПДн могут быть получены ОИВ Курской области от лица, не являющегося субъектом ПДн, при условии предоставления подтверждения наличия оснований, указанных в п.п. 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федеральным законом № 152-ФЗ или иных оснований, предусмотренных законодательством Российской Федерации.

Для организации обработки ПДн во всех ОИВ Курской области приказом руководителя назначаются ответственные лица в должности не ниже заместителя руководителя.

В органах, обеспечивающих деятельность Администрации Курской области, назначаются специалисты со следующими функциональными обязанностями:

взаимодействие с сотрудниками областного казенного учреждения «Центр электронного взаимодействия», назначенными администраторами безопасности;

подготовка предложений по внесению изменений в информационную систему ПДн.

Право доступа к ПДн субъектов ПДн на бумажных и электронных носителях имеют работники ОИВ Курской области в соответствии с их должностными обязанностями и в порядке, регламентируемом внутренними нормативными документами. Передача ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только

между работниками ОИВ Курской области, имеющими доступ к ПДн, осуществляется в рабочем порядке с учетом технологии работы с соответствующим ресурсом ПДн.

Передача ПДн субъектов ПДн третьим лицам осуществляется в соответствии с требованиями действующего законодательства.

ОИВ Курской области вправе осуществить передачу (поручить обработку) ПДн третьей стороне с согласия субъекта ПДн и в иных случаях, предусмотренных действующим законодательством Российской Федерации, на основании заключаемого с этой стороной договора (далее – Поручение). В указанном Поручении определяется перечень действий (операций) с ПДн, которые будут совершаться обработчиком, цели обработки, обязанности обработчика по обеспечению безопасности ПДн и требования по безопасности ПДн. Обработчик обязан соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом № 152-ФЗ, обеспечивая конфиденциальность и безопасность ПДн при их обработке.

Внесение изменений в ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе в отношении целей обработки ПДн, осуществляется в рабочем порядке в объеме полученного от субъекта ПДн согласия.

ОИВ Курской области уведомляет Уполномоченный орган по защите прав субъектов ПДн об обработке ПДн. С этой целью направляется уведомление об обработке ПДн по форме Уполномоченного органа и в сроки, установленные Федеральным законом №152-ФЗ.

3.3. Категории субъектов ПДн, которые подлежат обработке в ОИВ Курской области:

государственные гражданские служащие ОИВ Курской области; родственники государственных гражданских служащих ОИВ Курской области; служащие ОИВ Курской области; соискатели/кандидаты на замещение вакантных должностей государственной гражданской службы ОИВ Курской области, для зачисления в кадровый резерв ОИВ Курской области; уволенные с государственной гражданской службы ОИВ Курской области; жители Курской области, обратившиеся в ОИВ Курской области; ПДн иных категорий, обработка которых ведется в соответствии с требованиями федерального и регионального законодательства.

В целях, указанных в пункте 3.2 настоящей Политики, обрабатываются ПДн государственных гражданских служащих ОИВ Курской области, родственников государственных гражданских служащих ОИВ Курской области, служащих ОИВ Курской области, соискателей/кандидатов на замещение вакантных должностей государственной гражданской службы ОИВ Курской области, для зачисления в кадровый резерв ОИВ Курской области, уволенных с государственной гражданской службы ОИВ Курской области, жителей Курской области, обратившихся в ОИВ Курской области; ПДн иных

категорий, обработка которых ведется в соответствии с требованиями федерального и регионального законодательства:

фамилия, имя, отчество; число, месяц, год рождения; место рождения; гражданство; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации, фактического проживания); номер контактного телефона; реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; реквизиты страхового медицинского полиса обязательного медицинского страхования; реквизиты свидетельства государственной регистрации актов гражданского состояния; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о трудовой деятельности; сведения о воинском учете и реквизиты документов воинского учета; сведения об образовании; сведения об ученой степени; информация о владении иностранными языками, степень владения; медицинское заключение об отсутствии у гражданина заболевания; фотография; сведения о пребывании за границей; информация о классном чине государственной гражданской службы; информация о наличии или отсутствии судимости; государственные награды, иные награды и знаки отличия; сведения о профессиональной переподготовке и (или) повышении квалификации; сведения о доходах, об имуществе и обязательствах имущественного характера; номер расчетного счета; номер банковской карты; адрес электронной почты; пол; иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 3.2 настоящей Политики.

3.4. Конфиденциальность ПДн.

ОИВ Курской области, получившие доступ к ПДн, обязуются не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

3.5.Сроки обработки и хранения ПДн.

Сроки обработки и хранения ПДн государственных гражданских служащих ОИВ Курской области, соискателей/кандидатов на замещение вакантных должностей государственной гражданской службы ОИВ Курской области, для зачисления в кадровый резерв ОИВ Курской области, уволенных с государственной гражданской службы ОИВ Курской области и иных субъектов ПДн, определяются в соответствии с номенклатурой дел органов ОИВ и законодательством Российской Федерации.

3.6. Порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований.

Ответственным за документооборот и архивирование в ОИВ Курской области осуществляется систематический контроль и выделение документов, содержащих ПДн, с истекшими сроками хранения, подлежащих уничтожению.

Вопрос об уничтожении выделенных документов, содержащих ПДн, рассматривается на заседании Экспертной комиссии ОИВ Курской области (далее - ЭК), состав которой утверждается приказом ОИВ Курской области.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами ЭК и утверждается руководителем ОИВ Курской области.

По окончании процедуры уничтожения документов (сжигание, химическое уничтожение) должностным лицом ОИВ Курской области, ответственным за архивную деятельность, составляется соответствующий Акт об уничтожении документов, содержащих ПДн.

Уничтожение по окончании срока обработки ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4. Обеспечение безопасности критической информационной инфраструктуры

В соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» должна быть обеспечена безопасность критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В ОИВ Курской области должны быть определены и прокатегорированны объекты критической информационной инфраструктуры. Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

В соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивается одна из категорий значимости объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий

В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом

исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создается система безопасности такого объекта и обеспечивается ее функционирование.

Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры.

В ОИВ Курской области должны быть назначены сотрудники, ответственные за ведение реестра объектов критической информационной инфраструктуры и обеспечение на них безопасности информации.

5. Обеспечение юридической значимости электронных документов

В ОИВ Курской области должны выполняться предусмотренные законодательными и нормативными документами уполномоченных органов организационно-технические мероприятия по обеспечению контроля целостности и подтверждения авторства электронных документов посредством применения электронной подписи.

6. Реализация требований информационной безопасности в ЕИКС ОИВ Курской области

В целях реализации собственных полномочий и обеспечения обмена информацией (и в иных установленных федеральными законами целях)

ОИВ Курской области используются ИС. ИС создаются на основании соответствующего решения, которое, в том числе, определяет оператора ИС.

В зависимости от правомочий обладателя информации и полномочий по созданию ИС Курской области ИС разделяются на внутренние и внешнеориентированные ИС.

ЕИКС Курской области создана в целях:

обеспечения ОИВ Курской области доступа заинтересованных лиц к информации об их деятельности;

эффективного и качественного информационного обеспечения решения задач социального и экономического развития Курской области;

обеспечения эффективного информационного взаимодействия органов государственной власти Курской области с федеральными органами государственной власти, органами местного самоуправления, гражданами и организациями.

Организационные и технические меры защиты информации, применяемые к ИС, входящим в состав ЕИКС Курской области, определяются в зависимости от типа доступа к информации, обрабатываемой в них. Не допускается эксплуатация ИС Курской области без использования в целях обеспечения защиты информации комплекса организационных и технических мер, установленных нормативными правовыми актами Российской Федерации, определяющих порядок и меры обеспечения защиты информации. Технические средства, предназначенные для обработки информации, содержащейся в ИС Курской области, в том числе программно-технические средства и СЗИ, должны соответствовать требованиям федерального законодательства и иметь соответствующие сертификаты соответствия.

В зависимости от типа обрабатываемой информации ИС разделяются на ИС с общедоступной информацией и ИС с информацией ограниченного доступа.

Обработка информации в ИС с общедоступной информацией осуществляется с обеспечением следующих приоритетов:

целостность информации;

доступность информации.

Информация, относящаяся к ПДн и иной конфиденциальной информации, предназначенная для использования исключительно сотрудниками ОИВ Курской области при выполнении ими своих служебных обязанностей обрабатывается в соответствии со следующими приоритетами:

конфиденциальность;

целостность;

доступность.

Объектами защиты в ИС являются:

информация (данные) ОИВ Курской области, доступная с помощью ИС;

управляющая информация ИС и их подсистем информационной безопасности.

7. Подключение к российскому государственному сегменту сети «Интернет» RSNet

В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации ОИВ Курской области должны осуществить подключение находящихся в их ведении государственных ИС и информационно-телекоммуникационных сетей к российскому государственному сегменту сети «Интернет» (далее – RSNet) и обеспечить размещение (публикацию) информации в сети «Интернет» в соответствии с порядком, утвержденным Указом Президента Российской Федерации от 22 мая 2015 г. №260 «О некоторых вопросах информационной безопасности Российской Федерации».

Подключение ИС и информационно-телекоммуникационных сетей к сети «Интернет» через сегмент RSNet осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств. Защита информации в ИС и информационно-телекоммуникационных сетях, подключаемых к сети «Интернет» через российский сегмент RSNet, обеспечивается в соответствии с законодательством Российской Федерации.

Поддержание, эксплуатацию и развитие российского государственного сегмента RSNet обеспечивает Федеральная служба охраны Российской Федерации.

Процедура и технические условия подключения ИС и информационно-телекоммуникационных сетей к сегменту RSNet определяются в соответствии с приказом Федеральной службы охраны Российской Федерации от 7 сентября 2016 г. №443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет».

Технические условия подключения к сети «Интернет» и размещения (публикации) в ней информации через сеть RSNet определяются Соглашением о подключении к информационно-телекоммуникационной сети «Интернет» и размещении (публикации) в ней информации через российский государственный сегмент сети «Интернет» (сеть RSNet) и включают в себя следующие технические параметры подключения:

технологическая площадка, через которую осуществляется подключение;

тип канала связи;

скорость передачи данных;

логические характеристики подключения;

требования по обеспечению информационной безопасности.

Процедура подключения ИС и информационно-телекоммуникационных сетей к сети RSNet включает в себя следующие этапы:

обращение ОИВ в адрес оператора сети RSNet;

заключение Соглашения;

организация подключения ИС и информационно-телекоммуникационных сетей к сети «Интернет» через сеть RSNet в соответствии с Техническими условиями.

8. Ответственность за реализацию и поддержку Политики

8.1. Ответственность за обеспечение требований по защите информации возлагается на руководителей ОИВ Курской области, эксплуатирующих ИС.

8.2. Ответственность должностных лиц ОИВ Курской области, имеющих доступ и осуществляющих обработку к ПДн (с использованием ИС и без их использования) и иной конфиденциальной информации, за невыполнение положений данной Политики и норм нормативных правовых актов, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними нормативными документами ОИВ Курской области

9. Финансирование мероприятий по информационной безопасности

9.1. Финансирование мероприятий по информационной безопасности в ОИВ Курской области, их подведомственных учреждениях осуществляется за счёт средств соответствующей государственной программы и средств ОИВ Курской области и их подведомственных учреждений, выделяемых на защиту ИС из бюджета Курской области.

9.2. При планировании проведения мероприятий по развитию ИС ОИВ, учреждений и организаций Курской области объем финансирования на проведение указанных мероприятий рассчитывается с учетом расходов на проведение мероприятий по информационной безопасности в соответствии с требованиями действующего законодательства.

9.3. При планировании мероприятий по защите информации ОИВ Курской области их подведомственные учреждения должны согласовывать их объемы и состав с комитетом информатизации, государственных и муниципальных услуг Курской области и ежегодно до 1 ноября предоставлять в комитет информатизации, государственных и муниципальных услуг Курской области перечень запланированных мероприятий по защите информации в ОИВ и их подведомственных учреждениях и объемы финансовых средств, необходимые для реализации указанных мероприятий, в том числе предусмотренные в бюджете Курской области на следующий год.

10. Осуществление контроля информационной безопасности

10.1.Внешний контроль за реализацией мероприятий по информационной безопасности ОИВ Курской области и их подведомственных учреждений осуществляет комитет информатизации, государственных и муниципальных услуг Курской области.

10.2.Внутренний контроль за реализацией мероприятий по информационной безопасности ОИВ Курской области, которые не являются юридическими лицами, осуществляет областное казенное учреждение «Центр электронного взаимодействия».

10.3. Внутренний контроль за реализацией мероприятий по информационной безопасности ОИВ Курской области, которые являются юридическими лицами, осуществляется самостоятельно данными органами. Результаты проведения внутреннего контроля направляются в адрес комитета информатизации, государственных и муниципальных услуг Курской области не позднее 5 рабочих дней с даты их утверждения.

10.4. Внутренний контроль за реализацией мероприятий по информационной безопасности учреждений, подведомственных ОИВ Курской области, осуществляется самостоятельно данными органами.

10.5. Типовой план проведения контроля состояния систем информационной безопасности в ОИВ Курской области представлен в приложении № 4 к настоящей Политике.