АДМИНИСТРАЦИЯ КУРСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

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.

Губернатор
Курской области А.Н.Михайлов

Управляющий делами Администрации Курской области
Отдел делопроизводства

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.

Приложение № 1
к Основным направлениям политики
информационной безопасности
органов исполнительной власти Курской области

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

информационной системы в органе исполнительной власти Курской области

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Область применения

Настоящая Инструкция администратора безопасности информационной системы (далее – ИС) определяет обязанности и порядок действий администратора безопасности по организации обеспечения безопасности информации, обрабатываемой в ИС органа исполнительной власти Курской области (далее – ОИВ).

Целью администрирования является достижение, контроль и совершенствование требуемого уровня защищённости информационной системы персональных данных (далее – ИСПДн) от несанкционированного доступа (далее – НСД).

Заданная цель достигается применением комплекса организационно-технических мероприятий по защите информации, установленных в ОИВ, а также обеспечением постоянного контроля над выполнением принятых мер.

Администратор безопасности ИС (далее - администратор безопасности) – лицо, осуществляющее контроль над обеспечением защиты информации в ИС, а также осуществляющее организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Администратор безопасности назначается распорядительным документом уполномоченного лица ОИВ из числа штатных сотрудников, имеющих необходимую квалификацию.

Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по разработке и осуществлению мероприятий по обеспечению защиты персональных данных (далее – ПДн) при их обработке в ИС.

Администратор безопасности руководствуется в своей практической деятельности положениями нормативно-правовых актов Российской Федерации и внутренними распорядительными документами ОИВ.

Требования администратора безопасности, связанные с выполнением возложенных на него функций, обязательны для исполнения всеми пользователями ИС.

Автоматизированное рабочее место администратора безопасности должно представлять собой выделенный персональный компьютер, размещенный в помещении, исключающем НСД к обрабатываемой в нем информации.

Настоящая Инструкция является неотъемлемой частью организационно-распорядительных документов ОИВ, регламентирующих защиту ПДн при их обработке в ИС.

1.2. Краткое описание возможностей системы защиты информации

Система защиты информации (далее – СЗИ) реализована комплексом организационных мер, а также набором программных и аппаратных решений, выполненных на базе технических и информационных средств, входящих в состав ИС.

Применение СЗИ позволяет обеспечить:

противодействие актуальным угрозам безопасности информации;

выполнение требований нормативно-правовых актов по защите информации.

1.3. Уровень подготовки администратора безопасности

Администратор безопасности должен обладать необходимыми знаниями и опытом работы в области защиты информации и системного администрирования.

Рекомендуемые требования к администратору СЗИ:

высшее инженерно-техническое образование;

знание технологий обеспечения информационной безопасности;

знание и умение использования законодательных, нормативно-распорядительных, специальных и иных требований к обеспечению безопасности информации (Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и т.д.);

знание применяемых операционных систем на уровне сетевого администратора, навыки установки операционных систем, опыт их конфигурирования;

знание сетевых технологий и протоколов на уровне сетевого администратора;

умение работать с пользователями (в том числе слабо компетентными в технических областях).

1.4. Перечень документации, с которой необходимо ознакомиться администратору

Для работы с СЗИ администратор безопасности должен ознакомиться со следующими документами на ИС ОИВ:

Модель угроз безопасности ИС;

Техническое задание на создание СЗИ.

2. ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ

В настоящей Инструкции использованы следующие термины:

доступ к информации – возможность получения информации и ее использования;

доступность информации – состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия;

информация – сведения (сообщения, данные) независимо от формы их представления;

информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

логин – имя учетной записи пользователя, позволяющее выполнить его аутентификацию при входе в систему;

межсетевой экран – локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы. Межсетевой экран обеспечивает защиту автоматизированной системы посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) автоматизированную систему на основе заданных правил, проводя таким образом разграничение доступа субъектов одной автоматизированной системы к объектам другой автоматизированной системы;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системы;

объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа;

пароль – секретное слово или набор символов, предназначенный для подтверждения прав доступа;

пользователь ИС – лицо, участвующее в функционировании ИС или использующее результаты ее функционирования;

правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

3. НАЗНАЧЕНИЕ И СОСТАВ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Назначение системы

СЗИ предназначена для обеспечения безопасности информации при ее обработке в ИС ОИВ.

Применение СЗИ осуществляется в течение всего жизненного цикла ИС в соответствии с проектными документами на ее создание, а также с эксплуатационной документацией на средства защиты, входящие в состав СЗИ. Не допускается обработка информации, к которой предъявляются требования по соблюдению ее конфиденциальности, без выполнения мер по ее защите.

3.2. Состав системы

ИС представляет собой совокупность информации, а также средства вычислительной техники и программного обеспечения, позволяющие производить обработку этой информации.

СЗИ включает в себя следующие программные и аппаратные средства, входящие в состав ИС:

операционные системы;

средства защиты информации от НСД;

антивирусное программное обеспечение;

средства анализа защищенности;

межсетевые экраны;

средства криптографической защиты информации.

Помимо технических и информационных мер СЗИ в ИС принят ряд организационных мер, направленных на достижение и поддержание на достигнутом уровне требуемых характеристик безопасности информации.

Детальное описание ИС, требования к СЗИ, а также методы и способы их достижения изложены в документах, приведенных в подразделе 1.4.

4. ОБЩИЕ ПРИНЦИПЫ РАБОТЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Структура системы

Меры по защите информации выполняются в соответствии с требованиями, определенными в Техническом задании на создание СЗИ ИС ОИВ.

СЗИ реализуется следующими группами мер (подсистемами)[1] и мероприятиями:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации;

регистрация событий безопасности;

антивирусная защита;

обнаружение вторжений;

контроль (анализ) защищённости информации;

обеспечение целостности ИС и информации;

обеспечение доступности информации;

защита среды виртуализации;

защита технических средств;

защита ИС, ее средств, систем связи и передачи данных;

выявление инцидентов и реагирование;

управление конфигурацией ИС и СЗИ;

меры по обеспечению безопасности информации при ее обработке в ИС с использованием средств криптографической защиты информации;

организационно-технические мероприятия.

4.2. Идентификация и аутентификация субъектов доступа и объектов доступа

Для однозначной идентификации пользователей и разграничения прав доступа к информации для каждого из работников ОИВ, имеющих доступ к ИС, администратором безопасности создаётся уникальная учётная запись.

Учётная запись включает в себя имя пользователя (логин) и пароль, являющиеся реквизитами доступа.

При регистрации пользователей администратором безопасности устанавливается соответствие всех используемых паролей доступа в ИС в соответствии с установленными требованиями.

Запрещается фиксировать учётные данные пользователя (пароли, логины, ключи и др.) на носителях информации при их использовании в местах, доступных другим лицам, а также сообщать их кому бы то ни было, кроме самого пользователя.

4.3. Управление доступом субъектов доступа к объектам доступа

Лица, доступ которых к информации, обрабатываемой в ИС, необходим для выполнения служебных обязанностей, допускаются к

---

[1] Здесь приведен общий список групп мер (подсистем), определенных для всех ИС ОИВ. Состав групп мер (подсистем) для каждой ИС определен в Техническом задании на создание СЗИ для каждой ИС ОИВ.

соответствующей информации на основании списка, утверждённого уполномоченным лицом ОИВ.

Каждому пользователю при его регистрации определяются права доступа на основании списка и в соответствии с разрешительной системой доступа к ИС.

При увольнении работника руководитель подразделения составляет заявку на удаление учётной записи пользователя из ИС, утверждает её и передаёт администратору безопасности. При получении заявки администратор безопасности удаляет учётную запись пользователя из ИС.

Разграничение доступа к защищаемой информации обеспечивается:

средствами операционных систем;

средствами защиты информации от НСД;

штатными средствами приложений обработки информации и систем управления базами данных;

иными применяемыми системами разграничения доступа приложений.

С целью существенного затруднения реализации угроз безопасности информации должны быть реализованы следующие мероприятия:

в Basic Input/Output System (далее – BIOS) серверов и рабочих станций устанавливается загрузка только с накопителя на жёстком магнитном диске;

опечатываются корпуса автоматизированных рабочих мест, обрабатывающих информацию с ограниченным доступом.

Ответственность за попытку нарушения прав доступа лежит на непосредственном начальнике пользователя, а в случае факта нарушения ответственность определяется после разбора причин и обстоятельств нарушения.

4.4. Ограничение программной среды

В ИС обеспечивается установка и (или) запуск только разрешенного к использованию в ИС программного обеспечения.

Администратор безопасности обеспечивает периодический контроль установленного (инсталлированного) в ИС программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в ИС.

4.5. Защита машинных носителей информации

Администратор безопасности является лицом, ответственным за учёт машинных носителей информации. Учёт носителей информации осуществляется в установленном порядке, принятом в ОИВ.

4.6. Регистрация событий безопасности

При работе пользователя в ИС должна осуществляться регистрация его входа (выхода) в систему (из системы). Механизм регистрации обеспечивается средствами «ActiveDirectory» операционной системы

(далее - ОС) WindowsServer, локальных ОС и средств защиты информации от НСД.

Запросы пользователей ИС на получение информации, а также факты предоставления информации по этим запросам должны регистрироваться средствами ИС в электронном журнале обращений.

Администратор безопасности осуществляет защиту сохраняемой информации о зарегистрированных событиях безопасности от НСД и уничтожения при помощи штатных средств используемых ОС и ИС обработки информации.

4.7. Обнаружение вторжений

Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе ИС (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов ИС (автоматизированных рабочих местах, серверах и иных узлах), определяемых администратором безопасности.

4.8. Антивирусная защита

Настройка средств антивирусной защиты должна обеспечивать надёжную защиту системы от воздействия вредоносных программ (программ-вирусов).

Обновление вирусных баз в ИС должно производиться на регулярной основе в соответствии с рекомендациями производителя антивирусного программного обеспечения.

4.9. Контроль (анализ) защищённости информации

Анализ защищённости реализуется специализированными программными средствами.

Данные результатов сканирования должны быть проанализированы и учтены для минимизации возможности реализации угроз удалённого доступа.

По расписанию, не реже 1 раза в квартал, администратор безопасности при помощи специализированных программных средств, а также средств управления программным обеспечением и СЗИ осуществляет контроль установки обновлений программного обеспечения, контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и СЗИ.

Контроль состава технических средств, программного обеспечения и СЗИ обеспечивается посредством формирования списка контролируемых узлов.

4.10. Обеспечение целостности ИС и информации

В ОИВ должна быть обеспечена возможность восстановления средств защиты информации от НСД, предусматривающая ведение двух копий установочного пакета средств защиты информации, копий настроек

средств защиты (подробного описания методики достижения данных настроек), а также периодическое обновление и контроль работоспособности данных копий.

4.11. Обеспечение доступности информации

Доступность информации обеспечивается за счёт применения системы резервирования данных.

Администратор безопасности должен обеспечить восстановление информации в течение установленного временного интервала с резервных машинных носителей информации.

4.12. Защита технических средств

Все технические средства ИС должны находиться в пределах контролируемой зоны ОИВ.

Администратор безопасности контролирует обеспечение управления физическим доступом к техническим средствам ИС, которое реализуется следующими мероприятиями:

утверждением списков помещений и лиц, допущенных в помещения, в которых обрабатываются информация и находятся технические средства ИС;

применением систем контроля и управления доступом;

применением средств охранной сигнализации и/или видеонаблюдения;

охраной помещений в нерабочее время.

Должно быть обеспечено размещение устройств вывода и отображения информации (мониторов) в помещениях, которое исключало бы её несанкционированный просмотр, за счёт следующих мероприятий:

установки на окна штор и/или жалюзи;

ограничения доступа в помещения посторонних лиц;

оптимизацией взаимного размещения технических средств.

4.13. Защита ИС, ее средств, систем связи и передачи данных

В ИС осуществляется разделение функций по управлению (администрированию) ИС, управлению (администрированию) СЗИ, функций по обработке информации и иных функций ИС.

Защита ИС, ее средств, систем связи и передачи данных реализуется посредством использования сертифицированных средств криптографической защиты информации.

4.14. Выявление инцидентов и реагирование на них

Администратор безопасности является лицом, ответственным за выявление инцидентов и реагирование на них.

4.15. Управление конфигурацией ИС и СЗИ

Администратору ИС (системному администратору) и администратору безопасности разрешены действия по внесению изменений в конфигурацию СЗИ.

Установка дополнительного системного и прикладного ПО выполняется при оформлении соответствующей заявки.

4.16. Организационно-технические мероприятия

Эксплуатация ИС должна осуществляться в полном соответствии с утвержденной организационно-технической и эксплуатационной документацией на СЗИ.

Все технические средства ИС должны быть заземлены и находиться в пределах офисных помещений ОИВ.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей информацию ограниченного доступа.

5. ОТВЕТСТВЕННОСТЬ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

5.1. Ответственность администратора безопасности

Администратор безопасности отвечает за организацию:

проведения мероприятий, направленных на предотвращение НСД к информации и (или) передачи их лицам, не имеющим права доступа к такой информации;

своевременного обнаружения фактов НСД к информации;

недопущения воздействия на технические средства ИС, в результате которого может быть нарушено их функционирование;

возможности восстановления информации, модифицированной или уничтоженной вследствие НСД к ней;

постоянного контроля за обеспечением уровня защищенности информации.

Администратор безопасности несет персональную ответственность за качество проводимых им работ по организации обеспечения защиты информации.

5.2. Обязанности администратора безопасности

Администратор безопасности обязан:

знать способы и методы защиты информации, применяемые в ИС;

обеспечить доступ пользователям к информации согласно их правам доступа;

постоянно проводить работу по выявлению возможных каналов утечки информации за счет НСД;

при обнаружении несанкционированного предоставления информации незамедлительно приостановить предоставление информации до выявления причин нарушений и устранения этих причин;

незамедлительно докладывать своему непосредственному руководству обо всех попытках нарушения системы защиты ИС;

анализировать данные электронных журналов обращений ИС с целью выявления возможных нарушений требований защиты;

осуществлять контроль за порядком учета, хранения и обращения с носителями информации;

организовывать и проводить проверки состояния средств защиты информации, проводить контроль за выполнением специальных требований по размещению средств вычислительной техники;

запрещать и немедленно блокировать попытки несанкционированного изменения программно-аппаратной среды ИС, ведущие к возможному инициированию фактов НСД;

производить контроль опечатывания системных блоков с целью предупреждения бесконтрольного доступа к рабочим местам и обрабатываемой информации;

участвовать в приемке вновь устанавливаемых средств защиты информации;

осуществлять постоянный контроль за работой средств защиты информации, применяемых в ИС, а также за выполнением установленного комплекса организационных мероприятий по защите информации;

контролировать правильность применения пользователями средств защиты информации и при необходимости оказывать им помощь;

уточнять в установленном порядке обязанности пользователей по поддержанию достигнутого класса защищенности ИС и вносить предложения по совершенствованию уровня защиты ИС;

участвовать в разработке документации ОИВ, регламентирующей защиту обрабатываемой информации в соответствии с требованиями руководящих документов.

Администратору безопасности запрещается оставлять свое рабочее место в состоянии, позволяющем осуществить НСД к обрабатываемой информации.

6. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Мероприятия по обеспечению безопасности информации по подсистемам защиты, которые должен выполнять администратор СЗИ, и их периодичность приведены в таблице.

Таблица. Мероприятия по обеспечению безопасности информации

№ п/п	Мероприятие	Периодичность
Идентификация и аутентификация субъектов доступа и объектов доступа		
1	Добавление, изменение, удаление пользователей ИС	По заявке руководителя подразделения
Управление доступом субъектов доступа к объектам доступа		
2	Назначение, активация, блокирование прав доступа к ресурсам ИС	По заявке руководителя подразделения
3	Контроль работоспособности средств межсетевого экранирования	Не реже одного раза в квартал
Ограничение программной среды		
4	Контроль используемого программного обеспечения в ИС	Не реже одного раза в месяц
Защита машинных носителей информации		
5	Обеспечение безопасности информации при использовании машинных носителей информации	Постоянно
Регистрация событий безопасности		
6	Просмотр и анализ результатов регистрации событий безопасности и реагирование на них	Не реже одного раза в месяц, а также в случае нарушения конфиденциальности информации
Обнаружение вторжений		
7	Контроль работоспособности средств обнаружения вторжений	Не реже одного раза в месяц
Антивирусная защита		
8	Контроль работоспособности средств антивирусной защиты	Не реже одного раза в месяц
Контроль (анализ) защищённости информации		
9	Анализ защищённости специализированными программными средствами	Не реже одного раза в квартал
10	Контроль обновлений программного обеспечения, состава технических и программных средств	Не реже одного раза в квартал
11	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Не реже одного раза в квартал

№ п/п	Мероприятие	Периодичность
Обеспечение целостности информационной системы и информации		
12	Контроль работоспособности средств восстановления СЗИ	Не реже одного раза в месяц
Обеспечение доступности информации		
13	Тестирование функций резервирования информации	Не реже одного раза в неделю
Защита технических средств		
14	Контроль выполнения требований к физической защите технических средств ИС	Не реже одного раза в месяц
Защита ИС, ее средств, систем связи и передачи данных		
15	Контроль распределения обязанностей по управлению (администрированию) ИС, управлению (администрированию) СЗИ, функций по обработке информации и иных функций ИС	Не реже одного раза в месяц
16	Контроль настроек средств криптографической защиты информации, применяемых для защиты информации при их передаче по каналам связи, имеющим выход за пределы контролируемой зоны	Не реже одного раза в месяц
Выявление инцидентов и реагирование		
17	Обнаружение, идентификация и регистрация инцидентов, а также принятие мер по устранению и предупреждению инцидентов	По мере возникновения
Управление конфигурацией ИС и СЗИ		
18	Управление изменениями конфигурации ИС и СЗИ, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений	По мере необходимости
Организационно-технические мероприятия		
19	Контроль выполнения требований к СЗИ, определенных в документации на нее	Постоянно

7. ИЗМЕНЕНИЕ СОСТАВА ИС

Состав и конфигурация технических и программных средств ИС определяется исходя из функций, выполняемых ИС, и функциональной необходимости.

При изменении состава ИС необходимо руководствоваться организационно-техническими требованиями, предъявляемыми к системе, приведенными в Модели угроз безопасности ИС.

8. ПРОБЛЕМЫ В РАБОТЕ СИСТЕМЫ И СПОСОБЫ ИХ РЕШЕНИЯ

При функционировании системы возможны сбои, вызванные нарушением штатного режима функционирования программных и аппаратных средств, входящих в состав системы защиты ИС. При возникновении таких сбоев администратор безопасности руководствуется эксплуатационной документацией на средство защиты.

В случае нарушения функционирования СЗИ обработка информации в ИС приостанавливается до устранения возникшей неисправности. Решение о приостановке обработки принимается уполномоченным лицом ОИВ по представлению администратора безопасности исходя из возможного ущерба и негативных последствий для информационной системы.

Приложение № 2
к Основным направлениям политики
информационной безопасности
органов исполнительной власти Курской области

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
информационной системы в органе исполнительной власти Курской области

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Область применения

Инструкция пользователя информационной системы (далее – ИС) органов исполнительной власти Курской области (далее – ОИВ) определяет обязанности и порядок действий пользователя по обеспечению безопасности информации, обрабатываемой в ИС ОИВ.

1.2. Краткое описание возможностей системы защиты информации

Система защиты информации (далее – СЗИ) реализована комплексом организационных мер, а также набором программных и аппаратных решений, выполненных на базе технических и информационных средств, входящих в состав ИС.

Применение системы защиты информации позволяет обеспечить:
противодействие актуальным угрозам безопасности информации;
выполнение требований нормативных актов по защите информации.

1.3. Уровень подготовки пользователя

Пользователь ИС должен обладать квалификацией, обеспечивающей базовые навыки работы на персональном компьютере.

1.4. Перечень документации, с которой необходимо ознакомиться пользователю

Для работы пользователь должен ознакомиться с настоящей Инструкцией и пройти инструктаж по обеспечению безопасности информации в ОИВ. Личной подписью в Журнале проведения инструктажа по информационной безопасности пользователь ИС принимает правила и требования по обеспечению безопасности информации, обрабатываемой в ИС ОИВ.

2. ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ

В настоящей Инструкции использованы следующие термины:

доступ к информации – возможность получения информации и ее использования;

доступность информации – состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия;

информация – сведения (сообщения, данные) независимо от формы их представления;

информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи;

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

логин – имя учетной записи пользователя, позволяющее выполнить его аутентификацию при входе в систему;

межсетевой экран – локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы. Межсетевой экран обеспечивает защиту автоматизированной системы посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) автоматизированную систему на основе заданных правил, проводя таким образом разграничение доступа субъектов одной автоматизированной системы к объектам другой автоматизированной системы;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системы;

объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа;

пароль – секретное слово или набор символов, предназначенный для подтверждения прав доступа;

пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования;

правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

3. НАЗНАЧЕНИЕ И СОСТАВ СИСТЕМЫ ИНФОРМАЦИИ

3.1. Назначение системы

СЗИ предназначена для обеспечения безопасности информации при ее обработке в ИС ОИВ.

3.2. Основные задачи, решаемые системой

Применение СЗИ позволяет решить следующие основные задачи:

противодействие угрозам безопасности информации;

исключение несанкционированного доступа к информации, обрабатываемой в ИС.

3.3. Состав системы

ИС представляет собой совокупность информации, а также средства вычислительной техники и программное обеспечение, позволяющие производить обработку этой информации.

СЗИ выполнена следующими программными и аппаратными средствами, входящими в состав ИС:

операционная система;

средства защиты информации от несанкционированного доступа;

антивирусное программное обеспечение;

средства анализа защищённости;

межсетевые экраны;

средства криптографической защиты информации.

4. ОТВЕТСТВЕННОСТЬ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

4.1. Ответственность пользователя

Пользователь отвечает за выполнение требований обеспечения безопасности информации при обработке в ИС в соответствии с действующими нормативно - правовыми актами Российской Федерации и внутренними распорядительными документами ОИВ.

Ответственность за попытку нарушения требований безопасности информации лежит на непосредственном руководителе пользователя, а в случае факта нарушения ответственность определяется после разбора причин и обстоятельств нарушения.

4.2. Обязанности пользователя

Пользователь обязан:

знать и соблюдать установленные правила обеспечения безопасности информации при обработке в ИС;

знать и соблюдать правила эксплуатации аппаратных средств, входящих в состав ИС;

знать и соблюдать правила обеспечения безопасности информации при доступе к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), доступ к таким сетям должен производиться только в случае возникновения служебной необходимости;

обеспечить сохранность используемых машинных носителей информации (далее – МНИ);

в случае возникновения нештатных ситуаций в работе ИС прекратить выполняемые работы и сообщить администратору безопасности ИС о сбое (неисправности).

Пользователю запрещается:

осуществлять запись информации на МНИ, не учтенные в установленном порядке в ОИВ;

выносить за пределы офисных помещений ОИВ учтенные МНИ, а также документы, содержащие информацию ограниченного доступа, без разрешения уполномоченных лиц;

передавать МНИ и документы, содержащие информацию ограниченного доступа, лицам, не участвующим в процессе ее обработки, без разрешения владельца информационного процесса (руководителя подразделения);

хранить МНИ вблизи источников электромагнитных излучений и прямых солнечных лучей;

вносить изменения в конфигурацию программно-аппаратных средств ИС (в том числе изменять расположение аппаратных модулей) без разрешения администратора безопасности ИС;

приносить и записывать игровые, обучающие и прочие программы и программные модули на МНИ, используемые для хранения и обработки информации;

допускать к решению задач (производству расчетов, формированию документов и т.п.) посторонних лиц;

оставлять свое рабочее место в состоянии, позволяющем осуществить несанкционированный доступ к обрабатываемой информации;

выполнять работы при обнаружении нарушенных пломб узлов и блоков ИС, самовольно срывать такие пломбы;

разглашать сведения о применяемых средствах защиты информации;

производить обработку информации с выключенными или нефункционирующими средствами защиты (в том числе при отключённой системе заземления);

использовать в работе МНИ, не проверенные на предмет отсутствия программ-вирусов.

5. ПРАВА ДОСТУПА К РЕСУРСАМ ИС

Каждому пользователю в зависимости от его должностных полномочий и выполняемых им служебных обязанностей назначаются права доступа к информационным ресурсам и техническим средствам ИС.

При необходимости изменения прав доступа пользователь обращается к своему непосредственному руководителю с обоснованием расширения (уменьшения) таких прав.

6. ПОРЯДОК РАБОТЫ С СИСТЕМОЙ

Для однозначной идентификации пользователей и разграничения прав доступа в целях исключения несанкционированного доступа к информации, для каждого сотрудника ОИВ, имеющего доступ к информации, администратором безопасности ИС создается уникальная учетная запись.

Учетная запись включает в себя имя пользователя (логин) и пароль, являющиеся реквизитами доступа.

После регистрации администратор безопасности ИС сообщает пользователю его учетные данные.

При первичном входе в систему, а также в сроки, установленные администратором безопасности ИС, пользователь производит смену пароля, при этом имя (логин) остается неизменным.

Выбор пароля пользователем, а также период его действия должны удовлетворять установленным требованиям.

Запрещается фиксировать учетные данные (логины, пароли, ключи и др.) на носителях информации при их использовании в местах, доступных другим лицам, а также сообщать их кому бы то ни было, кроме самого пользователя.

В случае утери или компрометации пароля пользователь должен немедленно сообщить о случившемся администратору безопасности ИС

7. ПОРЯДОК РЕАГИРОВАНИЯ ПРИ АВАРИЙНЫХ СИТАЦИЯХ

Пользователь ИС обязан незамедлительно поставить в известность администратора безопасности ИС при возникновении следующих ситуаций:

нарушены пломбы (наклейки) на корпусе системного блока, входящего в состав автоматизированного рабочего места ИС;

при входе в сеанс система не запрашивает данные аутентификации (логин и пароль);

антивирусное программное обеспечение сигнализирует о вирусной активности или выдает иное сообщение, не являющееся регламентным сообщением работы антивируса;

иные ситуации, вызывающие подозрения и влекущие за собой возможность осуществления несанкционированного доступа к информации.

Приложение № 3
к Основным направлениям политики
информационной безопасности
органов исполнительной власти Курской области

Рекомендации по проведению контроля обеспечения целостности, устойчивости функционирования и безопасности информационных систем, доступных в сети «Интернет»

1. Общие положения

1.1. Настоящие рекомендации определяют организацию и порядок проведения контроля защищенности информационных систем (далее - ИС), находящихся в эксплуатации.

1.2. Рекомендации распространяются на ИС Курской области, созданные или используемые в целях реализации полномочий органов исполнительной власти Курской области (далее - ОИВ), доступные в сети «Интернет».

1.3. Рекомендации разработаны на основе действующих в Российской Федерации правовых и нормативных документов по защите информации, в том числе приказа ФСБ России, ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования», приказа Минкомсвязи России от 25 августа 2009 г. № 104 «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования».

1.4. Контроль состояния защиты информации и оценка эффективности средств защиты информации являются неотъемлемой составной частью работ по защите информации при создании и эксплуатации ИС.

1.5. Обладателем информации/оператором ИС является ОИВ. В соответствии с п. 4 ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) обладатель информации, оператор ИС в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

своевременное обнаружение фактов несанкционированного доступа к информации;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением уровня защищенности информации.

1.6. В случае невыполнения данных рекомендаций оператор ИС несет ответственность в соответствии с законодательством Российской Федерации.

1.7. Для пресечения возможности взлома системы (общедоступного ресурса) необходимо обеспечить использование только лицензионного программного обеспечения и проведение его своевременного обновления.

2. Рекомендации по организации контроля защищенности ИС, доступных в сети «Интернет»

Контроль является одной из составляющих защиты ИС. Помимо контроля необходимо выполнить следующие мероприятия:

сбор информации и формирование перечня ИС, доступных в сети «Интернет», функционирующих (используемых) в ОИВ;

утверждение и подпись сформированного перечня ИС руководителем ОИВ;

проверка регистрации ИС в Реестре информационных систем Курской области, в случае отсутствия таковой, произвести соответствующие мероприятия по внесению ИС в Реестр ИС (в соответствии постановлением Губернатора Курской области от 05 августа 2009 г. № 252 «О Положении о реестре и паспортах информационных систем Курской области»);

размещение ИС на хостинге, у которого аппаратные мощности располагаются на территории Российской Федерации, в том числе обязательного заключения договора (соглашения) с хостинг-провайдером, в котором обязанности, установленные п. 4 ст. 16 Федерального закона №149-ФЗ должны быть возложены на хостинг-провайдера;

разработка инструкции пользователя ИС (в случае отсутствия) при работе с ИС посредством сети «Интернет».

Контроль состояния защиты информации ИС разделяется на внутренний и внешний аудит. ОИВ самостоятельно выбирает способ аудита.

Внутренний аудит. Осуществляется ответственным специалистом за защиту информации. ОИВ должен:

назначить ответственного специалиста за проведение мероприятий по обеспечению защиты информации ИС и контроль ее безопасного функционирования (специалист должен: иметь соответствующее профессиональное образование в сфере защиты информации или информационной безопасности и стаж по специальности не менее 1 года;

получить письменное заключение от уполномоченного органа о возможности работы в сфере защиты информации);

осуществить подбор сертифицированного программного обеспечения для проведения аудита информационной безопасности ИС.

Внешний аудит. Осуществляется организацией, имеющей лицензии на проведение мероприятий по обеспечению информационной безопасности. ОИВ должен назначить ответственного за:

составление плана-графика проведения аудита;

контроль выполнения организацией мероприятий данного плана-графика;

составление отчетов для уполномоченного органа.

3. Проведение контроля защищенности ИС, доступных в сети «Интернет»

3.1. Проведение контроля защищенности общедоступных ресурсов не реже 1 раза в квартал.

3.2. Контроль состояния защиты информации, заключается в оценке:

соблюдения требований правовых, организационно-распорядительных и нормативных документов по защите информации;

корректности использования и работоспособности применяемых мер и средств защиты информации в соответствии с их эксплуатационной документацией;

знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

3.3. По результатам контроля разрабатывается план по устранению недостатков в обеспечении информационной безопасности и по совершенствованию СЗИ ИС, в соответствии с которым в организации разрабатываются и проводятся необходимые мероприятия.

3.4. Устранение выявленных уязвимостей:

перечень выявленных уязвимостей направляется хостинг-провайдеру с указанием необходимости их устранения;

если выявленные уязвимости не были устранены, необходимо направить хостинг-провайдеру повторный запрос;

в случае отсутствия исполнения повторного запроса необходимо направить письмо о данной ситуации в комитет информатизации, государственных и муниципальных услуг Курской области с целью совместного решения сложившейся проблемы.

3.5. Информирование комитета информатизации, государственных и муниципальных услуг Курской области:

о проведении аудита, наличии выявленных уязвимостей, принятых мерах и результатах по их устранению;

в случае возникновения трудностей при проведении мероприятий по устранению выявленных уязвимостей;

два раза в год не позднее 1 апреля и 1 октября о внесенных изменениях в перечень ИС, доступных в сети «Интернет» и других изменениях или об отсутствии таких изменений.

Приложение № 4
к Основным направлениям политики
информационной безопасности
органов исполнительной власти Курской области

ПЛАН
проведения контроля состояния систем защиты информации в органах исполнительной власти Курской области

С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к ней и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности или доступности информации, в ОИВ проводится контроль состояния защиты информации комитетом информатизации, государственных и муниципальных услуг Курской области, который заключается в:

1) оценке полноты и соответствия требованиям основных руководящих документов в сфере обеспечения безопасности информации, разработанных в ОИВ;
2) оценке состояния технической защиты конфиденциальной информации (наличие и настройки необходимых средств защиты информации, установленных на представленных объектах информатизации) с указанием результатов регистрации событий;
3) проверке актуальности ведения журналов;
4) результате контроля, формировании протокола.

1. Изучение и оценка документации, разработанной в целях организации обеспечения безопасности информации в органах исполнительной власти Курской области

Перечень организационно-распорядительной документации, регламентирующей вопросы организации обработки ПДн и обеспечения безопасности ПДн:

1. Приказ (распоряжение) о назначении администратора безопасности информации в автоматизированной системе объекта информатизации ОИВ и возложении на него функциональных обязанностей.
2. Функциональные обязанности администратора безопасности информации в автоматизированной системе объектов информатизации ОИВ.
3. Расписка в ознакомлении лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими своих трудовых обязанностей, с перечнем и содержанием нормативно-правовых актов, в том числе локальных, устанавливающих требования по соблюдению конфиденциальности ПДн, а также требования по обеспечению безопасности ПДн и меры ответственности за их несоблюдение.

4. Приказ (распоряжение) об определении перечня помещений, предназначенных для обработки ПДн в ОИВ.

5. Перечень лиц, имеющих доступ в помещение, в котором обрабатываются ПДн.

6. Перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей.

7. Перечень защищаемых информационных ресурсов ИС.

8. Технический паспорт объекта информатизации.

9. Перечень параметров настройки ПО ИС.

10. Данные по уровню подготовки кадров, обеспечивающих защиту информации, в автоматизированной системе ИСПДн.

11. Приказ (распоряжение) о классификации ИС.

12. Акт классификации ИС.

13. Приказ (распоряжение) об обследовании и классификации помещений.

14. Акт обследования помещений на предмет соответствия требованиям к инженерно-технической укрепленности по защите объектов от преступных посягательств.

15. Акт классификации помещений на предмет соответствия требованиям к инженерно-технической укрепленности по защите объектов от преступных посягательств.

16. Комплект инструкций администраторам системы и пользователям по обеспечению безопасности информации в автоматизированной системе.

17. Инструкция о действиях сотрудников при возникновении чрезвычайных ситуаций в помещениях ОИВ.

18. Инструкция по приему под охрану помещений ОИВ.

19. Инструкция по резервированию и восстановлению работоспособности технических средств и ПО, баз данных и средств защиты информации в ИСПДн.

20. Приказ (распоряжение) о вводе в эксплуатацию объекта информатизации.

2. Оценка состояния технической защиты информации в органах исполнительной власти Курской области

Оценка состояния технической защиты информации представляет собой проверку соответствия наличия и настроек средств защиты информации и программного обеспечения, указанных в аттестационной документации.

При оценке состояния технической защиты конфиденциальной информации указываются:

1) наименование АРМ;
2) заводской (инвентарный) номер системного блока АРМ;
3) адрес размещения АРМ;
4) оценка состояния технической укрепленности помещений;

5) перечень установленных средств защиты информации;
6) контроль сетевых подключений;
7) настройки МЭ;
8) контроль подключения съемных носителей информации к ОИ;
9) контроль разграничения доступа в системе, НСД;
10) проверка целостности конфигурации оборудования и технических средств ОИ и проверка целостности программной среды ОИ;
11) своевременность обновления баз сигнатур антивирусного ПО;
12) просмотр журналов событий и безопасности ПО.

По каждому из пунктов формируется детальное описание.

3. Проверка актуальности ведения журналов учёта

1.Журнал приема (сдачи) под охрану кабинетов и ключей от них.
2.Журнал регистрации и учета машинных носителей ПДн.
3.Журнал регистрации конфиденциальных документов.
4.Журнал учета сейфов, металлических шкафов, спецхранилищ и ключей от них.

4. Формирование протокола контроля состояния систем защиты информации в органах исполнительной власти Курской области

Формирование протокола контроля состояния систем защиты информации представляет собой сборку и обработку результатов контроля:

1.Составление протокола контроля защищенности ОИ в ОИВ.
2.Представление протокола под роспись ответственному подразделения, в котором проводится контроль состояния систем защиты.