УТВЕРЖДЕНА

постановлением Губернатора

Курской области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_\_\_

ИНСТРУКЦИЯ

по защите конфиденциальной информации в информационных системах органов исполнительной власти Курской области

**ОГЛАВЛЕНИЕ**

[1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 4](#_Toc48899400)

[1.1. Термины и определения 4](#_Toc48899401)

[1.2. Принятые сокращения 5](#_Toc48899402)

[2. ОБЩЕЕ ПОЛОЖЕНИЕ 7](#_Toc48899403)

[2.1. Назначение инструкции по защите информации в органах исполнительной власти Курской области 7](#_Toc48899404)

[2.2. Цель и задачи защиты информации в информационных системах органов исполнительной власти Курской области 8](#_Toc48899405)

[2.3. Нормативно-методическое обеспечение 8](#_Toc48899406)

[3. ПОРЯДОК СОЗДАНИЯ, ВВОДА В ЭКСПЛУАТАЦИЮ, ЭКСПЛУАТАЦИИ И ВЫВОДА ИЗ ЭКСПЛУАТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ 11](#_Toc48899407)

[3.1. Формирование требований к защите информации в информационных системах 11](#_Toc48899408)

[3.2. Разработка системы защиты информации 12](#_Toc48899409)

[3.3. Внедрение системы защиты информации 14](#_Toc48899410)

[3.4. Аттестация информационной системы 16](#_Toc48899411)

[3.5. Обеспечение защиты информации в ходе эксплуатации 16](#_Toc48899412)

[3.6. Обеспечение защиты информации при выводе из эксплуатации информационной системы 19](#_Toc48899413)

[4. МЕРОПРИЯТИЯ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ в органах исполнительной власти Курской области 21](#_Toc48899414)

[4.1. Мероприятия по защите конфиденциальной информации 21](#_Toc48899415)

[4.2. Рекомендованный перечень организационно-распорядительной документации 22](#_Toc48899416)

[5. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И КОНТРОЛЮ 24](#_Toc48899417)

[6. ОРГАНИЗАЦИЯ КОНТРОЛЯ НАД СОСТОЯНИЕМ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ 26](#_Toc48899418)

[Приложение № 1](#_Toc48899419) 29

[Приложение № 2](#_Toc48899420) 32

[Приложение № 3](#_Toc48899421) 38

[Приложение № 4](#_Toc48899422) 43

[Приложение № 5](#_Toc48899423) 46

# 1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

## 1.1. Термины и определения

В настоящей Инструкции по защите конфиденциальной информации в информационных системах органов исполнительной власти Курской области используются следующие основные термины и определения:

1. Автоматизированное рабочее место – комплекс средств вычислительной техники и программного обеспечения, располагающийся, непосредственно на рабочем месте сотрудника и предназначенный для автоматизации его работы.
2. Государственная информационная система Курской области – это внешнеориентированная информационная система Курской области, предполагающая участие в сборе и обработке информации, доступа к ней органов исполнительной власти Курской области, органов местного самоуправления, граждан, организаций в соответствии с федеральным законодательством и законодательством Курской области, созданная на основании правового акта государственного органа, в том числе органа государственной власти Курской области, в целях реализации полномочий региональных государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.
3. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
4. Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
5. Конфиденциальная информация – документированная информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и распоряжением Губернатора Курской области от 17.05.2012 № 360-рг «Об утверждении Перечня сведений конфиденциального характера».
6. Оператор информационной системы – орган исполнительной власти Курской области и его подведомственные организации, орган местного самоуправления Курской области и его подведомственные организации, сторонняя организация, заключившая соответствующий договор, сотрудники которого осуществляют деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
7. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу (субъекту персональных данных).
8. Система защиты информации – 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.
9. Средства защиты информации – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.
10. Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

## 1.2. Принятые сокращения

1.2.1. ИС – информационная система.

1.2.2. ПДн – персональные данные.

1.2.3. ИСПДн – информационная система персональных данных.

1.2.4. ГИС – государственная информационная система.

1.2.5. ОИВ – органы исполнительной власти Курской области.

1.2.6. МНИ – машинный носитель информации.

1.2.7. АРМ – автоматизированное рабочее место.

1.2.8. ПО – программное обеспечение.

1.2.9. СЗИ – система защиты информации.

1.2.10. УБИ – угрозы безопасности информации.

1.2.11. ОРД – организационно-распорядительная документация.

1.2.12. ТЗ – техническое задание.

1.2.13. НСД – несанкционированный доступ.

1.2.14. Инструкция – Инструкция по защите конфиденциальной информации в информационных системах органов исполнительной власти Курской области.

1.2.15. Комитет – комитет цифрового развития и связи Курской области.

1.2.16. ОКУ «ЦЭВ» - Областное казенное учреждение «Центр электронного взаимодействия.

# 2. ОБЩЕЕ ПОЛОЖЕНИЕ

## 2.1. Назначение инструкции по защите информации в органах исполнительной власти Курской области

Настоящая Инструкция предназначена для организации и проведения работ по обеспечению безопасности защищаемой информации в ИС (ГИС, ИСПДн и ИС, содержащие сведения для служебного пользования). К защищаемой информации относятся ПДн и конфиденциальная информация.

Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», [постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных](garantF1://70152506.0)», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказом Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

## 2.2. Цель и задачи защиты информации в информационных системах органов исполнительной власти Курской области

Целью защиты конфиденциальной информации является предотвращение утечки, хищения, утраты и искажения информации, ее уничтожения, блокирования, модификации и копирования лицами, не имеющими на это права и других форм вмешательства в ИС, а также установление порядка организации и проведения работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну в ИС на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

Задачами защиты конфиденциальной информации являются:

выявление возможных каналов утечки информации;

предотвращение или существенное затруднение несанкционированного доступа к конфиденциальной информации;

оценка возможностей технических средств разведки и реальной опасности утечки конфиденциальной информации;

предотвращение утечки информации по техническим каналам;

разработка и осуществление экономически обоснованных технических и организационных мероприятий по защите информации;

соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности и достоверности информации в системах ее обработки;

сохранение возможности управления процессом обработки и пользования конфиденциальной информацией;

организация контроля над состоянием защиты информации.

## 2.3. Нормативно-методическое обеспечение

1. Федеральный Закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».
2. Федеральный Закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
4. Постановление Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - приказ ФСТЭК России от 11.02.2013 № 17).
6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» (далее - постановление Правительства Российской Федерации от 06.07.2015 № 676).
8. Постановление Губернатора Курской области от 05.08.2009 № 252 «О Положении о реестре и паспортах информационных систем Курской области».
9. Распоряжение Администрации Курской области от 30.08.2018 № 347-ра «Об утверждении Основных направлений политики информационной безопасности органов исполнительной власти Курской области».
10. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» Федеральной службы по техническому и экспортному контролю от 14.02.2008.
11. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК России от 15.02.2008.
12. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости».
13. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
14. ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения» (далее - ГОСТ 51583).
15. ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования» (далее - ГОСТ 51624).
16. ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее – ГОСТ 34.601).
17. ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».
18. ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем».
19. ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

# 3. ПОРЯДОК СОЗДАНИЯ, ВВОДА В ЭКСПЛУАТАЦИЮ, ЭКСПЛУАТАЦИИ И ВЫВОДА ИЗ ЭКСПЛУАТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

## 3.1. Формирование требований к защите информации в информационных системах

Определение требований к СЗИ, содержащейся в ИС, осуществляется руководителем или ответственными лицами, назначенные руководителем ОИВ и включает:

принятие решения о необходимости защиты информации, содержащейся в ИС;

классификацию ИС по требованиям защиты информации, определение уровня защищенности ПДн, при их обработке в ИС;

определение УБИ, реализация которых может привести к нарушению безопасности информации в ИС, и разработку на их основе модели угроз безопасности информации;

определение требований к СЗИ.

При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

анализ целей создания ИС и задач, решаемых этой ИС;

определение информации, подлежащей обработке в ИС;

анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

принятие решения о необходимости создания СЗИ, а также определение целей и задач защиты информации в ИС, основных этапов создания СЗИ и функций по обеспечению защиты информации, содержащейся в ИС.

При классификации ИС, результат оформляется актом классификации ИС.

Результаты определения уровня защищенности ПДн при их обработке в ИС оформляются актом определения уровня защищенности.

УБИ определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации УБИ и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения УБИ, используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

По результатам определения УБИ при необходимости разрабатываются рекомендации по корректировке характеристик ИС, направленные на блокирование (нейтрализацию) отдельных УБИ.

В модель угроз безопасности информации входит описание ИС и ее характеристики, а также описание УБИ, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИС, способов реализации УБИ и последствий от нарушения свойств безопасности информации.

Требования к СЗИ определяются в зависимости от класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС и УБИ, включенных в модель угроз безопасности информации.

## 3.2. Разработка системы защиты информации

Разработка СЗИ ИС осуществляется в соответствии с ТЗ на создание ИС и (или) ТЗ на создание СЗИ ИС с учетом модели угроз безопасности информации, предусмотренной подпунктом "г" пункта 1 (2) постановления Правительства Российской Федерации от 06.07.2015 № 676, ГОСТ 34.601, ГОСТ 51583 и ГОСТ 51624 и в том числе, включает:

проектирование СЗИ;

разработку эксплуатационной документации на СЗИ;

макетирование (при необходимости) и тестирование СЗИ.

Разработка СЗИ может осуществляться как собственным подразделением (специалистом) по защите информации при взаимодействии и под методическим руководством Комитета так и специализированными организациями, имеющими лицензии на этот вид деятельности, на договорной основе.

СЗИ не должна препятствовать достижению целей создания ИС и ее функционированию. При разработке СЗИ учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

При проектировании СЗИ осуществляются следующие мероприятия:

1. определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным ПО, иные объекты доступа);
2. определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в ИС;
3. выбираются меры защиты информации, подлежащие реализации в СЗИ;
4. определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
5. определяется структура СЗИ, включая состав (количество) и места размещения ее элементов;
6. осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС;
7. определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению УБИ;
8. определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

ТЗ формируется в соответствии с подпунктами "а" и "в" пункта 1(1) постановления Правительства Российской Федерации от 06.07.2015 № 676, выполняя требования к защите информации, содержащейся в ИС.

Перед отправкой в Управление ФСТЭК по Центральному федеральному округу, модель угроз безопасности информации ГИС и (или) ТЗ на создание ГИС согласуется с комитетом цифрового развития и связи Курской области, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации.

Для разработки модели угроз безопасности информации, ОИВ могут использовать Типовую модель угроз безопасности информационных систем персональных данных органов государственной власти Курской области, утвержденную Комиссией по информационной безопасности при Губернаторе Курской области.

Макетирование (при необходимости) и тестирование СЗИ производится для проверки работоспособности и совместимости средств защиты информации, выполнение соответствующих требований к СЗИ и (или) корректировка проектных решений по созданию СЗИ ИС.

ТЗ на создание СЗИ ИС и модель угроз безопасности информации утверждаются руководителем ОИВ или заместителем руководителя ОИВ, ответственным за организацию по созданию СЗИ ИС.

## 3.3. Внедрение системы защиты информации

Внедрение СЗИ организуется в соответствии с проектной и эксплуатационной документацией на СЗИ и, в том числе, включает:

1. установку и настройку СЗИ в ИС;
2. разработку ОРД, определяющих правила и процедуры, реализуемые ОИВ для обеспечения защиты информации в ИС в ходе ее эксплуатации;
3. внедрение организационных мер защиты информации;
4. предварительные испытания СЗИ (при необходимости);
5. опытную эксплуатацию СЗИ (при необходимости);
6. анализ уязвимостей ИС и принятие мер защиты информации по их устранению;
7. приемочные испытания СЗИ (при необходимости).

Установка и настройка средств защиты информации в ИС проводится в соответствии с эксплуатационной документацией на СЗИ и документацией на средства защиты информации.

Разрабатываемые ОРД по защите информации определяют правила и процедуры:

1. планирования мероприятий по защите информации в ИС;
2. выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению УБИ, и реагирования на них;
3. управления конфигурацией аттестованной ИС и СЗИ;
4. контроля за обеспечением уровня защищенности информации, содержащейся в ИС;
5. информирования и обучения персонала ИС;
6. защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

При внедрении организационных мер защиты информации осуществляются:

1. реализация правил разграничения доступа (матрица доступа), регламентирующих права доступа субъектов доступа к объектам доступа, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения и введение ограничений на действия пользователей;
2. проверка полноты и детальности описания в ОРД по защите информации действий пользователей и администраторов ИС по реализации организационных мер защиты информации;
3. отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

Предварительные испытания СЗИ включают проверку работоспособности СЗИ, а также принятие решения о возможности опытной эксплуатации СЗИ.

Опытная эксплуатация СЗИ включает проверку функционирования СЗИ, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации СЗИ.

Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации УБИ. Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и ПО ИС. При анализе уязвимостей ИС проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и ПО, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и ПО, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и ПО. В случае выявления уязвимостей ИС, приводящих к возникновению дополнительных УБИ, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей. По результатам анализа уязвимостей должно быть подтверждено, что в ИС отсутствуют уязвимости, содержащиеся в банке данных УБИ ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

Приемочные испытания СЗИ ИС включают проверку выполнения требований к СЗИ ИС в соответствии с ТЗ на создание СЗИ ИС.

## 3.4. Аттестация информационной системы

Аттестация ИС организуется руководителем ОИВ или, по решению руководителя ОИВ, администратором безопасности ИС и (или) ответственным за организацию обработки ПДн в ИС, и включает проведение комплекса аттестационных испытаний, в результате которых подтверждается соответствие СЗИ ИС с ТЗ на создание СЗИ ИС и модели угроз безопасности информации ИС.

Аттестат соответствия выдается на весь срок эксплуатации СЗИ ИС, в соответствии с приказом ФСТЭК России от 11.02.2013 № 17. Администратор безопасности информации ИС в ходе эксплуатации ИС обеспечивает поддержку соответствия СЗИ аттестату соответствия в рамках реализации мероприятий, предусмотренных настоящей Инструкцией.

Повторная аттестация (переаттестация) ИС осуществляется по окончании срока действия сертификатов средств защиты информации, изменении класса защищенности ИС или других изменений в СЗИ ИС. При изменении состава УБИ или проектных решений, реализованных при создании СЗИ, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Ввод в эксплуатацию СЗИ ИС осуществляется в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Губернатора Курской области от 05.08.2009 № 252 «О Положении о реестре и паспортах информационных систем Курской области» и при наличии аттестата соответствия.

## 3.5. Обеспечение защиты информации в ходе эксплуатации

Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется администратором безопасности информации ИС, в соответствии с эксплуатационной документацией на СЗИ и ОРД по защите информации и в том числе включает:

1. планирование и контроль мероприятий по защите информации в ИС;
2. анализ УБИ в ИС;
3. управление (администрирование) СЗИ;
4. выявление инцидентов и реагирование на них;
5. управление конфигурацией ИС и ее СЗИ;
6. информирование и обучение персонала ИС;
7. контроль за обеспечением уровня защищенности информации, содержащейся в ИС.

В ходе планирования мероприятий по защите информации в ИС осуществляется:

1. определение лиц, ответственных за планирование и контроль мероприятий по защите информации в ИС;
2. определение лиц, ответственных за выявление инцидентов и реагирование на них;
3. разработка, утверждение и актуализация плана мероприятий по защите информации в ИС;
4. определение порядка контроля выполнения мероприятий по защите информации в ИС, предусмотренных утвержденным планом.

Планирование мероприятий по защите информации в ИС и контроль выполнения мероприятий осуществляются в соответствии с Приложением № 4 к настоящей Инструкции.

В ходе анализа УБИ в ИС осуществляется выявление, анализ и устранение известных уязвимостей ИС.

Периодичность проведения указанных работ определяется в плане мероприятий по защите информации.

В ходе управления (администрирования) СЗИ осуществляются:

определение администратора безопасности СЗИ ИС;

управление учетными записями пользователей ИС и поддержание в актуальном состоянии правил разграничения доступа в ИС;

управление средствами защиты информации в ИС;

управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС;

обеспечение функционирования СЗИ в ходе ее эксплуатации, включая ведение эксплуатационной документации и ОРД по защите информации.

В ходе выявления инцидентов и реагирования на них осуществляются:

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, ПО и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование операторами ИС и администраторами ИС лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

планирование и принятие мер по устранению и повторному возникновению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов, руководствуясь Приложением № 5 к настоящей Инструкции.

В ходе управления конфигурацией ИС и ее СЗИ осуществляются:

1. определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и ее СЗИ, их полномочия;
2. определение компонентов ИС и ее СЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;
3. управление изменениями ИС и ее СЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на защиту информации, санкционирование внесения изменений в ИС и ее СЗИ, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации ИС;
4. контроль действий по внесению изменений в ИС и ее СЗИ.

В ходе информирования и обучения персонала ИС осуществляется:

1. информирование персонала ИС о появлении актуальных УБИ, о правилах безопасной эксплуатации ИС;
2. доведение до персонала ИС требований по защите информации, а также положений ОРД по защите информации с учетом внесенных в них изменений;
3. обучение персонала ИС правилам эксплуатации отдельных средств защиты информации и блокированию УБИ и реагированию на инциденты.

В ходе контроля за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

1. контроль (анализ) защищенности информации с учетом особенностей функционирования ИС;
2. анализ и оценка функционирования ИС и ее СЗИ, включая анализ и устранение уязвимостей и иных недостатков в функционировании СЗИ;
3. документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в ИС;
4. принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в ИС, о необходимости доработки (модернизации) ее СЗИ.

Регулярные мероприятия по обеспечению безопасности защищаемой информации проводятся в соответствии с планом мероприятий по защите информации. Внутренние проверки режима защиты информации проводятся в соответствии с планом внутренних проверок режима защиты информации. По результатам проведения внутренней проверки составляется акт (справка) с результатами внутренней проверки режима защиты информации в ОИВ.

## 3.6. Обеспечение защиты информации при выводе из эксплуатации информационной системы

Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации осуществляется администратором безопасности информации ИС ОИВ в соответствии с эксплуатационной документацией на СЗИ ИС и ОРД по защите информации и, в том числе, включает:

архивирование информации, содержащейся в ИС;

уничтожение (стирание) данных и остаточной информации с МНИ и (или) уничтожение МНИ.

Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности ОИВ в соответствии с постановлением Губернатора Курской области от 05.08.2009 № 252 «О Положении о реестре и паспортах информационных систем Курской области».

Уничтожение (стирание) данных и остаточной информации с МНИ производится при необходимости передачи МНИ другому оператору ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации МНИ, на которых осуществлялись хранение и обработка информации, осуществляется его физическое уничтожение и составляется акт уничтожения защищаемой информации.

# 4. МЕРОПРИЯТИЯ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ в органах исполнительной власти Курской области

## 4.1. Мероприятия по защите конфиденциальной информации

В целях защиты информации в ИС проводятся правовые, организационные, программно-технические, технические, специальные (криптографические) и другие мероприятия.

Правовые мероприятия предусматривают разработку ОРД руководствуясь п. 4.2 настоящей Инструкции.

Организационные мероприятия предусматривают:

1. назначение ответственного за организацию обработки ПДн (в должности не ниже заместителя руководителя), типовые обязанности которого приведены в приложении № 1 к настоящей Инструкции;
2. назначение администратора безопасности информации в ИС, типовые обязанности которого приведены в приложении № 2 к настоящей Инструкции;
3. назначение пользователей ПДн, типовые обязанности которых приведены в приложении № 3 к настоящей Инструкции;
4. подбор и подготовку кадров для работы в ИС;
5. повышение квалификации работников, обеспечивающих безопасность информации, в соответствии с постановлением Правительства Российской Федерации от 06.05.2016 № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»;
6. осуществление постоянного контроля над процессом обработки защищаемой информации.

Программно-технические и технические мероприятия обеспечивают:

1. создание СЗИ, в соответствии с ТЗ на создание ИС и (или) ТЗ на создание СЗИ ИС с учетом модели угроз безопасности информации, сформированные в соответствии с п. 3.1 настоящей Инструкции;
2. проведение мероприятий по защите информации в ИС;
3. предотвращение утечки обрабатываемой информации путем исключения НСД;
4. предотвращение специальных воздействий, вызывающих разрушение, уничтожение, искажение информации;
5. выявление внедренных программных или аппаратных закладочных устройств;
6. предотвращение перехвата информации, распространяющейся по техническим каналам, путем их выявления и локализации.

## 4.2. Рекомендованный перечень организационно-распорядительной документации

1. Модель угроз безопасности информации.
2. Техническое задание на создание СЗИ ИС.
3. Приказ о назначении лиц, ответственных за обеспечение безопасности ПДн в ИС.
4. Функциональные обязанности администратора безопасности информации в ИС.
5. Приказ об определении перечня помещений, предназначенных для обработки защищаемой информации в ИС и организации режима обеспечения безопасности в них.
6. Перечень лиц, имеющих доступ в кабинет, в котором обрабатывается защищаемая информация, в том числе ПДн.
7. Список лиц, допущенных к работе в ИС.
8. Перечень лиц, доступ которых к ПДн, подлежащим обработке в ИСПДн в составе ИС необходим для выполнения ими служебных обязанностей.
9. Перечень защищаемых информационных ресурсов ИС.
10. Технический паспорт ИС.
11. Перечень параметров настройки ПО в ИС.
12. Данные по уровню подготовки кадров, обеспечивающих защиту информации, в ИС.
13. Приказ об определении совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определения на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в ИС.
14. Акт определения совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определения на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в ИС в составе ИС.
15. Приказ о классификации ИС.
16. Акт классификации ИС.
17. Инструкция по организации режима обеспечения безопасности помещений ИС
18. Инструкция о действиях сотрудников при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров) в помещениях ИС.
19. Инструкция администратора безопасности информации в ИС.
20. Инструкция по работе пользователей в ИС.
21. Инструкция по парольной защите.
22. Инструкция по антивирусной защите.
23. Инструкция по учету и маркированию МНИ.
24. Инструкция по обеспечению доступности информации в ИС.
25. Расписка в ознакомлении лиц, доступ которых к информации ограниченного доступа, обрабатываемой в ИС, необходим для выполнения ими своих служебных обязанностей с перечнем и содержанием нормативно-правовых актов, в том числе локальных, устанавливающих требования по соблюдению конфиденциальности персональных данных, а также требований по обеспечению безопасности информации ограниченного доступа, в том числе персональных данных, и мерами ответственности за их несоблюдение.
26. Порядок хранения, использования и передачи ПДн сотрудников.
27. Политика в отношении обработки ПДн.
28. Приказ о комиссии по уничтожению защищаемой информации.
29. Приказ об обеспечении безопасности МНИ.
30. Инструкция ответственного за реализацию мер, необходимых для обеспечения сохранности защищаемой информации в части обработки ПДн и исключающих НСД при хранении МНИ.
31. Перечень мест хранения МНИ, содержащие защищаемую информацию.
32. Приказ о назначении ответственного за планирование и контроль мероприятий по защите информации в ИС.
33. Приказ о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них.
34. Приказ о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию ИС СЗИ.
35. Регламент внесения изменений в конфигурацию ИС и СЗИ.
36. Приказ о вводе в эксплуатацию ИС.

# 5. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И КОНТРОЛЮ

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 планирование мероприятий по защите информации в ИС ОИВ является одним из основных мероприятий при обеспечении защиты информации в ходе эксплуатации ИС.

Планирование мероприятий по защите информации включает следующие этапы:

планирование организационных мероприятий (организация разработки и использования документов и носителей защищаемой информации, их учет, исполнение, организацию работ по анализу внутренних и внешних угроз защищаемой информации, обучение сотрудников правилам работы с защищаемой информацией и другое);

планирование контрольных мероприятий (планирование внутренних проверок СЗИ);

планирование мероприятий по созданию СЗИ, которое включает планирование финансирования данных мероприятий.

Финансирование мероприятий по защите информации в ОИВ и их подведомственных учреждениях осуществляются за счет средств подпрограммы «Развитие системы защиты информации Курской области» государственной программы Курской области «Развитие информационного общества в Курской области», утвержденной постановлением Администрации Курской области от 24.10.2013 № 775-па «Об утверждении государственной программы Курской области «Развитие информационного общества в Курской области», средств ОИВ и их подведомственных учреждений, выделяемых на защиту ИС из бюджета Курской области и федеральных субсидий, выделяемых в рамках региональных проектов.

При планировании проведения мероприятий по защите информации ОИВ, учреждений и организаций Курской области объём финансирования на проведение указанных мероприятий рассчитывается в соответствии с требованиями действующего законодательства.

При планировании мероприятий по защите информации, ОИВ должны согласовывать их объемы и состав с Комитетом и ежегодно до 1 октября предоставлять в Комитет перечень запланированных мероприятий по защите информации в ОИВ и их подведомственных учреждениях и объемы финансовых средств, необходимых для реализации указанных мероприятий, в том числе предусмотренных в бюджете Курской области на следующий год.

Планирование работ по защите информации в ОИВ, с правами юридического лица, осуществляется специалистами по защите информации (администраторами безопасности информации). Планы утверждаются руководителями соответствующих подразделений.

В органах, обеспечивающих деятельность Администрации Курской области, планирование работ по защите информации осуществляют сотрудники ОКУ «ЦЭВ»(администраторы безопасности информации), планы утверждаются руководителями соответствующих подразделений.

По результатам выполнения этих планов в подразделениях составляются годовые отчеты о проделанной работе по защите информации, которые до 15 декабря текущего года направляются в Комитет.

# 6. ОРГАНИЗАЦИЯ КОНТРОЛЯ НАД СОСТОЯНИЕМ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Контроль над состоянием СЗИ заключается в проверке выполнения требований нормативных актов по защите информации, решений ФСТЭК России, приказов ФСБ России, руководящих документов Роскомнадзора, решений и методических рекомендаций Комиссии по информационной безопасности при Губернаторе Курской области, а также в оценке обоснования и эффективности принятых мер по защите информации в ОИВ.

Контроль состояния и эффективности СЗИ организуется и проводится в целях:

своевременного выявления и предотвращения утечки защищаемой информации;

исключения или существенного затруднения НСД к информации, хищения или утраты технических средств и МНИ;

разработки рекомендаций по защите информации в ИС при их эксплуатации.

Организация и проведение контроля – необходимое условие осуществления эффективной защиты конфиденциальной информации. Основными формами контроля защиты конфиденциальной информации являются периодические, плановые и внезапные проверки, обследования объектов, их аттестация, а также организация повседневного контроля.

Плановый и внеплановый внешний контроль осуществляется федеральными органами контроля, а также Комитетом. Периодический внутренний контроль состояния защиты информации в ОИВ осуществляется соответствующими руководителями и специалистами по защите информации (администраторами безопасности информации).

Контроль состояния защиты конфиденциальной информации федеральными органами осуществляется в установленные ими сроки и в пределах предоставленных полномочий в соответствии с действующим законодательством.

Плановый внешний контроль состояния системы защиты конфиденциальной информации осуществляется Комитетом в соответствии с утвержденными годовыми планами работ.

Периодический внутренний контроль за реализацией мероприятий по информационной безопасности ОИВ, которые не являются юридическими лицами, осуществляет ОКУ «ЦЭВ».

Периодический внутренний контроль за реализацией мероприятий по информационной безопасности ОИВ, с правами юридического лица, осуществляется самостоятельно данными органами. Результаты проведения внутреннего контроля направляются в адрес Комитета не позднее 5 рабочих дней с даты их утверждения.

Периодический внутренний контроль за реализацией мероприятий по информационной безопасности учреждений, подведомственных ОИВ, осуществляется самостоятельно данными органами.

Типовой план проведения контроля состояния СЗИ в ОИВ представлен в Приложении № 4 к Основным направлениям политики информационной безопасности органов исполнительной власти Курской области, утвержденным распоряжением Администрации Курской области от 30.08.2018 № 347-ра «Об утверждении Основных направлений политики информационной безопасности органов исполнительной власти Курской области».

Внеплановый контроль осуществляется Комитетом при выявлении инцидентов информационной безопасности (признаков утечки защищаемой информации или предпосылок к утечке защищаемой информации) в ОИВ и на основании предписания на проведение контроля без предварительного уведомления объекта контроля.

Руководитель проверенного структурного подразделения в соответствии с полученными материалами о результатах контроля должен провести необходимые мероприятия по устранению выявленных нарушений, о чем в месячный срок должен проинформировать Комитет.

При обнаружении нарушений руководитель проверенного подразделения обязан организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц, а также устранение выявленных нарушений.

На этапе эксплуатации ИС для проверки выполнения требований нормативных документов по защите информации осуществляется периодический внутренний контроль. Периодичность проведения контроля специалистами по защите информации (администраторами безопасности информации) – не реже одного раза в год.

Кроме того, внутренней контроль осуществляется ответственными сотрудниками ОИВ (ответственным за организацию обработки ПДн или администратором безопасности информации) в течении 20 дней после реконструкции или ремонта помещений, в которых располагаются технические средства ИСПДн.

Защита информации в ИС считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам. Несоответствие мер установленным требованиям и нормам ОРД по защите информации является нарушением.

# Приложение № 1

к Инструкции по защите конфиденциальной информации в информационных системах органов исполнительной власти

Курской области

**ТИПОВЫЕ ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Функции ответственного за организацию обработки ПДн (далее – Ответственный) заключаются в изучении всех сторон деятельности ОИВ для формирования рекомендаций по организации обработки ПДн, решая ряд основных вопросов:

* + - организация доступа к ПДн и учет сотрудников ОИВ, допущенных к обработке ПДн, как в программных комплексах, входящих в состав информационных систем, так и на бумажных носителях;
    - контроль за поддержанием в актуальном состоянии действующих локальных актов, журналов и форм учета по работе с ПДн;
    - контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
    - организация работы по заключению договоров на работы по защите ПДн;
    - контроль за поддержанием в актуальном состоянии уведомления об обработке ПДн;
    - рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Администратором, в ИС ОИВ;
    - осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами ОИВ.

Обязанности Ответственного:

* + - Знать цели обработки ПДн в ОИВ и перечень обрабатываемых ПДн.
    - Соблюдать требования Политики в отношении обработки персональных данных в ОИВ и иных локальных актов ОИВ, устанавливающих порядок работы с ПДн.
    - Обеспечивать доведение до сведения сотрудников ОИВ нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн, локальных актов ОИВ по вопросам обработки ПДн.
    - Осуществлять внутренний контроль за соблюдением сотрудниками ОИВ норм действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.
    - Контролировать ведение документации, предусмотренной локальными актами ОИВ в части обеспечения безопасности ПДн.
    - Обеспечивать доработку локальных актов по защите ПДн ОИВ.
    - Расследовать нарушения по вопросам защиты информации, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.
    - Обеспечивать организацию проведения занятий со специалистами ОИВ по организационным вопросам обработки ПДн (проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ОИВ).
    - Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п. 3 ч. 4 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1. Права ответственного за организацию обработки персональных данных

Ответственный имеет право:

* + - Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач.
    - Проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных и (или) территориальных подразделениях ОИВ (при их наличии).
    - Требовать от сотрудников ОИВ соблюдения требований Политики в отношении обработки персональных данных в ОИВ, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.
    - Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн.
    - Требовать от сотрудников ОИВ письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн.
    - Вносить предложения руководителю ОИВ об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн.
    - Давать сотрудникам ОИВ обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и требованиями ОИВ.
    - Привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

1. Ответственность ответственного за организацию обработки персональных данных

Ответственный в соответствии с возложенными на него обязанностями несет ответственность за:

* + - Несоблюдение требований локальных актов ОИВ, устанавливающих порядок работы с ПДн в пределах, установленных трудовым договором (служебным контрактом).
    - Разглашение ПДн в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

# Приложение № 2

к Инструкции по защите конфиденциальной информации в информационных системах органов исполнительной власти

Курской области

**ТИПОВЫЕ ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

1. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАНОСТИ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

1.1. Функции администратора безопасности информации (далее – Администратор):

1.1.1. Управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в информационной системе.

1.1.2. Управление средствами защиты информации информационной системы.

1.1.3. Управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования информационной системы.

1.1.4. Централизованное управление системой защиты информации информационной системы (при необходимости).

1.1.5. Мониторинг и анализ зарегистрированных событий в информационной системе, связанных с обеспечением безопасности информации.

1.1.6. Обеспечение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

1.2. Администратор обязан:

1.2.1. Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации.

1.2.2. Знать состав, структуру, назначение и выполняемые задачи информационной системы, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку защищаемой информации.

1.2.3. Знать состав, структуру и назначение системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов.

1.2.4. В рамках обеспечения функционирования системы защиты информации информационной системы в ходе ее эксплуатации обеспечивать:

– исполнение требований по защите информации в соответствии с проектной и организационной-распорядительной документацией на систему защиты информации информационной системы;

– реализацию принятых решений по обеспечению защиты информации, обрабатываемой в информационной системе;

– информирование Ответственного за организацию обработки ПДн о выявленных недостатках по результатам выполнения контрольных мероприятий;

– контроль работ, проводимых сторонними организациями на технических средствах информационной системы;

– неразглашение информации ограниченного доступа, ставшую доступной в ходе исполнения должностных обязанностей.

1.2.5. В рамках реализации функции управления учетными записями пользователей и поддержании в актуальном состоянии правил разграничения доступа в информационной системе, обеспечивать:

– верификацию (проверку) личности пользователя, его должностных (функциональных) обязанностей при заведении учетной записи пользователя;

– заведение, активацию, блокирование и уничтожение учетных записей пользователей в соответствии с установленным в ОИВ порядком;

– пересмотр и, при необходимости, корректировку учетных записей пользователей в соответствии с установленным в ОИВ порядком;

– своевременное уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

– реализацию правил разграничения доступа и полномочий пользователей в информационной системе на основе утвержденной руководителем ОИВ системы разграничения доступа;

– контроль правил генерации и смены паролей пользователями информационной системы, реализации правил разграничения доступом, полномочий пользователей в информационной системе;

– устранение нарушений, связанных с генерацией и сменой паролей пользователями, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступа, установлением полномочий пользователей.

1.2.6. В рамках реализации функций управления средствами защиты информации информационной системы обеспечивать:

– корректную эксплуатацию пользователями средств защиты информации;

– консультирование пользователей, участвующих в процессах обработки и обеспечения безопасности информации, по вопросам использования средств защиты информации;

– техническое обслуживание средств защиты информации информационной системы в соответствии с эксплуатационной документацией на средства защиты информации;

– устранение выявленных в средствах защиты информации уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации;

– периодический контроль работоспособности (неотключения) средств защиты информации;

– периодический контроль целостности программного обеспечения средств защиты информации;

– периодический контроль соответствия настроек средств защиты информации;

– принятие мер по восстановлению работоспособности (правильности функционирования) и параметров настройки средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов, в случае выявления фактов нарушения работоспособности или отклонения параметров настроек средства защиты информации;

– периодический контроль соответствия состава средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;

– периодическое выполнение тестирования функций безопасности средств защиты информации, в том числе с помощью тест- программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств;

– периодический контроль состава средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

– периодический контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

– исключение из состава информационной системы несанкционированно установленных средств защиты информации;

– восстановление несанкционированно удаленных средств защиты информации;

– настройку средств защиты информации, направленные на устранение возможности использования выявленных уязвимостей (при необходимости);

– согласование изменения конфигурации системы защиты информации и настроек средств защиты информации с Ответственным за организацию обработки ПДн.

1.2.7. В рамках реализации функций управления обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации обеспечивать:

– получение из доверенных источников и установку обновлений программного обеспечения, включая программное обеспечение средств защиты информации.

– контроль целостности файлов обновлений.

– проверку соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком;

– запись об установке (применении) обновлений в соответствующей эксплуатационной документации;

– обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты;

– обновление базы решающих правил систем обнаружения вторжений, применяемых в информационной системе (при наличии таковых);

– выполнение обновления программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств с целью устранения выявленных уязвимостей.

1.2.8. В рамках реализации функций централизованного управления системой защиты информации информационной системы обеспечивать:

– централизованное управление установкой, удалением, обновлением, конфигурированием и (или) контролем актуальности версий программного обеспечения средств защиты информации, эксплуатируемых в информационной системе.

1.2.9. В рамках реализации функций мониторинга и анализа зарегистрированных событий в информационной системе, связанных с обеспечением безопасности обеспечивать:

– регистрацию событий безопасности в соответствии с перечнем событий, подлежащим регистрации в информационной системе;

– периодический просмотр журналов регистрации событий безопасности;

– реагирование на сбои при регистрации событий безопасности;

– оперативное информирование лиц, ответственных за выявление инцидентов и реагирование на них о попытках и (или) фактах несанкционированного доступа или подозрительных событиях;

– содействие при проведении расследований инцидентов информационной безопасности.

1.2.10. Обеспечивать неразглашение информации о параметрах настройки ПО и СЗИ.

2.ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

2.1. Администратор имеет право:

2.1.1. Знакомиться с локальными актами ОИВ, регламентирующими процессы обработки защищаемой информации.

2.1.2. Вносить предложения Ответственному за организацию обработки ПДн по совершенствованию существующей системы защиты информации.

2.1.3. Требовать от пользователей информационных систем соблюдения требований Инструкции пользователя информационных систем ОИВ, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации.

2.1.4. Требовать от Ответственного за организацию обработки ПДн оказания содействия в исполнении функций и обязанностей, предусмотренных настоящей Инструкции.

2.1.5. Участвовать в расследовании инцидентов информационной безопасности и получать информацию об инцидентах информационной безопасности с целью совершенствования системы защиты информации информационной системы.

2.1.6. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность информации, вносить свои предложения по совершенствованию организационных и технических мер обеспечения безопасности информации.

2.1.7. Требовать прекращения работы в информационной системе, как в целом, так и отдельных пользователей информационной системы, в случае выявления нарушений требований по обеспечению безопасности информации или в связи с нарушением функционирования информационной системы.

2.1.8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности информации к Ответственному за организацию обработки ПДн.

3. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

3.1. Администратор несет персональную ответственность:

3.1.1. За работоспособность и надлежащее функционирование системы защиты информации.

3.1.2. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией.

3.1.3. За разглашение информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

3.1.4. За несоблюдение требований локальных актов ОИВ, устанавливающих порядок работы с защищаемой информацией, не содержащей сведения, составляющие государственную тайну, в пределах, установленных трудовым договором (служебным контрактом).

# Приложение № 3

к Инструкции по защите конфиденциальной информации в информационных системах органов исполнительной власти

Курской области

**ТИПОВАЯ ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Обязанности и права пользователя информационных систем

* 1. Пользователь обязан:
* соблюдать требования Политики в отношении обработки персональных данных в ОИВ и иных локальных актов ОИВ, устанавливающих порядок работы с защищаемой информацией;
* выполнять в информационных системах только те процедуры, которые необходимы для исполнения его должностных обязанностей;
* использовать для выполнения должностных обязанностей только предоставленное ему АРМна базе персонального компьютера;
* пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;
* обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;
* немедленно сообщать руководителю структурного подразделения и (или) администратору безопасности информации в информационных системах ОИВ (далее – Администратор) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;
* перед началом обработки в ИС файлов, хранящихся на съемных носителях информации, Пользователь должен осуществлять проверку файлов на наличие компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;
* располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами;
* соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.
  1. Пользователям ИС запрещается:
* записывать и хранить защищаемую информацию, на неучтенных материальных носителях информации;
* оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка защищаемой информации;
* отключать средства антивирусной защиты;
* отключать (блокировать) средства защиты информации;
* производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
* самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
* обрабатывать в ИС информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИС;
* сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИС;
* работать в ИС при обнаружении каких-либо неисправностей;
* хранить на учтенных носителях информации программы и данные, не относящиеся к защищаемой информации данной ИС;
* вводить в ИС защищаемую информацию под диктовку или с микрофона;
* привлекать посторонних лиц для производства ремонта технических средств ИС без согласования с Администратором.
  1. Пользователь имеет право знакомиться с внутренними документами ОИВ, регламентирующими его обязанности по занимаемой должности.

1. Организация парольной защиты в информационных системах
   1. Пароли доступа к ИС устанавливаются администратором или пользователем.
   2. При формировании пароля необходимо руководствоваться следующими требованиями:

* длина пароля должна быть не менее 8-и буквенно-цифровых символов;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;
* запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
* запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
* запрещается использовать ранее использованные пароли.
  1. При организации парольной защиты запрещается:
* записывать свои пароли в очевидных местах, таких как внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;
* хранить пароли в записанном виде на отдельных листах бумаги;
* сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от НСД.
  1. Плановую смену паролей доступа в ИС рекомендуется проводить один раз в квартал.
  2. Пользователь обязан незамедлительно сообщить администратору факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.
  3. Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:
* компрометации или подозрении на компрометацию пароля (производится пользователем или администратором безопасности информации);
* в случае прекращения полномочий пользователя (увольнение, переход на должность в организации) в течение 24 часов после окончания последнего сеанса его работы с ИС (производится администратором безопасности информации);
* по инициативе администратора безопасности информации.

1. Технология обработки защищаемой информации
   1. При первичном допуске к работе с ИС пользователь:

* проходит инструктаж по использованию ИС;
* знакомится с требованиями локальных актов, регламентирующих обработку и обеспечение безопасности защищаемой информации;
* получает у администратора безопасности информации идентификатор и личный пароль для входа в ИС.
  1. Перед началом работы пользователь визуально проверяет целостность АРМ, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.
  2. В процессе работы на АРМ ИС пользователь использует технические средства и установленное программное обеспечение согласно техническому паспорту ИС.
  3. Копирование защищаемой информации на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.
  4. При необходимости создания на АРМ пользователя дополнительных электронных документов, содержащих защищаемую информацию, пользователь создает и хранит такие документы в строго отведенном для этого месте.
  5. Печать документов, содержащих защищаемую информацию, осуществляется только при наличии производственной необходимости на принтер, подключенный администратором к АРМ пользователя. Печать документов, содержащих защищаемую информации, на общий сетевой принтер, возможна только в том случае, когда в локальной сети все АРМ входят в состав одной ИСПДн. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих защищаемую информацию, уничтожаются.
  6. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИС, пользователь обязан выключить компьютер, либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих ОИВ, пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.
  7. Покидая рабочее помещение в конце рабочего дня, пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.

# Приложение № 4

к Инструкции по защите конфиденциальной информации в информационных системах органов исполнительной власти

Курской области

ПОРЯДОК ПЛАНИРОВАНИЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ КУРСКОЙ ОБЛАСТИ.

1. Планирование мероприятий по защите информации
   1. В рамках планирования мероприятий по защите информации в ОИВ применительно к каждой ИС. Осуществляется разработка, согласование и утверждение ежегодного Плана мероприятий по защите информации в ИС.
   2. По решению руководителя ОИВ допускается разработка единого Плана мероприятий на несколько ИС.
   3. План мероприятий разрабатывается ответственным за планирование и контроль мероприятий по защите информации в ИС (далее – Ответственный) с участием пользователей, эксплуатирующих ИС, и ответственных, обеспечивающих функционирование ИС.
   4. В план мероприятий должны быть включены мероприятия по защите информации сегментов ИС, функционирующих в обособленных подразделениях (филиалах, представительствах) ОИВ, при наличии таковых.
   5. План мероприятий должен включать комплекс организационных и технических мероприятий по защите информации, направленных на решение задач обеспечения информационной безопасности ИС.
   6. Разработка мероприятий по защите информации должна осуществляться в соответствии с требованиями нормативных правовых актов в области защиты информации и принятыми в ОИВ локальными актами по защите информации.
   7. План мероприятий должен, как минимум, содержать:
      * Наименования мероприятий по защите информации.
      * Основания для проведения мероприятий.
      * Сроки выполнения мероприятий.
      * Наименования подразделений (сотрудников), ответственных за реализацию каждого мероприятия.
   8. План мероприятий должен содержать мероприятия по защите конфиденциальной информации в ИС в хронологическом порядке.
   9. План мероприятий формируется в следующем порядке:
      * В срок, не позднее 1 октября каждого года, Ответственный формирует проект Плана мероприятий.
      * Сформированный проект Плана мероприятий подлежит согласованию с руководителем ОИВ, администратором безопасности информации ИС, ответственным за организацию обработки ПДн, пользователями ИС и Комитетом в срок, не позднее 1 ноября каждого года.
      * Согласованный проект Плана мероприятий предоставляется ответственным руководителю ОИВ на утверждение.

Проект Плана мероприятий подлежит рассмотрению и утверждению руководителем ОИВ не позднее 30 декабря каждого года.

Утвержденный План мероприятий доводится Ответственным до работников ОИВ в части, их касающейся.

* 1. Изменения в действующий План мероприятий вносятся в соответствии с разделом 2 Приложения № 4 настоящей Инструкции.

1. Порядок внесения изменений в план мероприятий
   1. Внесение изменений в План мероприятий осуществляется на основании приказа руководителя ОИВ, на основе предложений Ответственного.
   2. Предложения о внесении изменений в План мероприятий могут быть сформированы в случаях:
      * Изменения законодательства Российской Федерации в области защиты информации.
      * Выявления в ходе контроля выполнения мероприятий, предусмотренных утвержденным Планом мероприятий, обстоятельств, требующих изменения Плана мероприятий (сроков, состава мероприятий, формулировок и т.д.).
      * Возникновения иных причин, препятствующих проведению мероприятия.
2. Контроль выполнения плана мероприятий
   1. Каждое мероприятие Плана мероприятий должно быть реализовано в установленные сроки. Контроль за выполнением мероприятий, предусмотренных Планом мероприятий осуществляется Ответственным.
   2. Ответственный, руководствуясь сроками выполнения мероприятий, осуществляет проверку выполнения мероприятий ответственными лицами, основываясь на документальном подтверждении факта выполнения мероприятий.
   3. В случаях выявления фактов неисполнения мероприятий (в том числе неполного исполнения), предусмотренных Планом мероприятий, ответственный при взаимодействии с лицами, ответственными за выполнение мероприятий, проводит:
      * Установление причин неисполнения мероприятий (в срок не более 5 рабочих дней с момента выявления факта неисполнения мероприятия).
      * Подготовку предложений по корректировке Плана мероприятий (в срок не более 10 рабочих дней с момента установления причин неисполнения мероприятия).
   4. С целью оценки эффективности обеспечения безопасности информации, Ответственный ежегодно готовит отчет о выполнении Плана мероприятий, который представляется руководителю ОИВ.
3. Ответственность ответственного за планирование и контроль мероприятий по защите информации в информационных системах

Ответственный несет персональную ответственность за:

* + - Качественную и своевременную подготовку плана мероприятий.
    - Своевременный и качественный контроль выполнения мероприятий.

# Приложение № 5

к Инструкции по защите конфиденциальной информации в информационных системах органов исполнительной власти

Курской области

Порядок выявления инцидентов информационной безопасности и реагирование на них

1. В качестве источников информации об инцидентах могут использоваться:

* журналы и оповещения системного и прикладного ПО ИС, обрабатывающих защищаемую информацию;
* журналы и оповещения СЗИ;
* оповещения средств обнаружения вторжений;
* информация, получаемая от работников ОИВ;
* информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

1. При обнаружении инцидента, ответственный за выявления инцидентов информационной безопасности и реагирование на них, должен оповестить Ответственного за организацию обработки ПДн в ИС и руководителя ОИВ.
2. Ответственный за управление инцидентами должен провести анализ инцидента информационной безопасности в целях выявления факта или предпосылки негативного воздействия на защищаемую информацию. В ходе анализа инцидента по возможности следует выявить следующие показатели:

* факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее – угрозы);
* опасность угрозы;
* области, перечни информационных ресурсов, затрагиваемые воздействием угрозы;
* потенциальные нарушители, цели и причины реализации угрозы;
* перечень мер по локализации и остановке распространения действия угрозы.

1. Ответственный за управление инцидентами оповещает Ответственного за организацию обработки ПДн о ходе и результатах реагирования на инциденты.
2. Ответственный за управление инцидентами составляет предложения Ответственному за организацию обработки ПДн о недопущении повторных инцидентов. При необходимости Ответственный за организацию обработки ПДн обеспечивает реализацию данных предложений.