## 1. Общие положения

### 1.1. Назначение документа

Положение по организации и проведению работ по обеспечению безопасности информации при их обработке в информационных системах (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите информации в департаменте внутренней и кадровой политики Белгородской области (далее – департамент).

Настоящее Положение разработано в соответствии с требованиями законодательства РФ, руководящих документов ФСТЭК и ФСБ России в области обеспечения безопасности информации ограниченного доступа, не составляющей сведения государственной тайны.

Цель Положения – регулирование работ по защите информации и обеспечение функционирования информационных систем департамента внутренней и кадровой политики области.

### 1.2. Область действия документа

Действие Положения распространяется на информационные системы департамента внутренней и кадровой политики области, в которых осуществляется обработка информации конфиденциального характера.

### 1.3. Вступление в силу документа

Настоящее Положение вступает в силу с момента его утверждения начальником департамента и действует бессрочно до замены его новым Положением.

Все изменения в Положение вносятся приказом начальника департамента.

## 2. Организация и проведение работ по обеспечению безопасности информации при их обработке в ИСПДн

### 2.1. Планирование работ по обеспечению безопасности информации

В целях исполнения настоящего Положения и на основании приказа о постоянно действующей экспертной комиссии по информационной безопасности (далее – комиссия), комиссия ежегодно составляет и утверждает у начальника департамента план мероприятий по обеспечению безопасности информации, обрабатываемых в ИС.

Проводимые в департаменте мероприятия по обеспечению безопасности информации учитываются в Журнале учета мероприятий по защите информации (Приложение 1).

**2.2. Выполнение работ по обеспечению безопасности информации**

В целях организации и проведения работ по обеспечению безопасности информации в департаменте приказом начальника назначаются:

– уполномоченное лицо, ответственное за проведение мероприятий по обеспечению безопасности информации и поддержание необходимого уровня информационной безопасности, а также за организацию и проведение инструктажа работников по основам информационной безопасности (Администратор ИБ);

– ответственный(-ые) за установку, настройку и обслуживание средств защиты информации, технических средств информационных систем (Администратор безопасности информации в корпоративной ЛВС).

Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности информации:

– определение и описание информационных систем;

– классификацию информационных систем обработки конфиденциальной информации по требованиям безопасности информации;

– определение актуальных угроз безопасности информации;

– проектирование системы защиты информации, включающей организационные, физические и технические меры и средства защиты;

– закупку, установку и настройку технических средств защиты информации;

– внедрение организационных мер и разработку соответствующих регламентов и положений;

– инструктаж и обучение лиц, которые будут использовать средства защиты информации.

Для выбора и реализации указанных мероприятий, может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Начальники отделов, в которых происходит обработка информации, являются лицами, ответственными за соблюдение требований по обеспечению безопасности информации.

Для обеспечения безопасности информации в департамента необходимо применение следующих мер:

– организационные меры безопасности:

• инструктаж работников по правилам обеспечения безопасности информации;

• учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

• мониторинг и реагирование на инциденты информационной безопасности, включая проведение внутренних проверок, разбирательств и составление заключений;

• постоянный контроль за соблюдением требований по обеспечению безопасности информации (реализуется путем внутренних аудитов);

– меры физической безопасности:

• ограничение доступа пользователей к техническим средствам информационных систем департамента, а также к носителям информации содержащим конфиденциальные сведения. Приказом начальника департамента устанавливается контролируемая зона, вводятся в действие Перечень лиц, имеющих доступ к ИС обработки конфиденциальной информации и техническим средствам. Лица, не указанные в Перечне, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при необходимости могут получать доступ к техническим средствам информационной системы в сопровождении ответственных лиц;

• размещение технических средств, позволяющих осуществлять обработку информации, в пределах контролируемой зоны;

• организация физической защиты помещений и технических средств, позволяющих осуществлять обработку информации;

– технические меры безопасности:

• разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

• регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

• резервирование технических средств, дублирование массивов и носителей информации;

• использование защищенных каналов связи;

• применение средств антивирусной защиты информации;

• предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Ремонтно-восстановительные работы технических средств обработки конфиденциальной информации проводятся под контролем администратора ИБ, лицами ответственными за данные работы. В случае необходимости ремонт

технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

### 2.3. Контроль выполнения работ по обеспечению безопасности информации

Контроль выполнения работ по обеспечению безопасности информации в департаменте осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

В рамках проведения контрольных мероприятий выполняются:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности информации за истекший период;

– проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности информации;

– проверка соответствия перечня лиц, которым предоставлен доступ к информации ограниченного доступа, фактическому состоянию;

– проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности информации, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности информации (при необходимости);

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности информации действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

Контрольные мероприятия проводятся как периодически, так и внепланово по решению руководителя и в случае возникновения инцидентов информационной безопасности.

Внутренние проверки в департаменте в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности информации;

– халатность и несоблюдение требований к обеспечению безопасности информации;

– несоблюдение условий хранения носителей информации;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальности, целостности, доступности) информации или другим нарушениям, приводящим к снижению уровня защищенности информации.

Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

### 2.4. Совершенствование системы защиты информации

Ежегодно по необходимости комиссия предоставляет начальнику департамента отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности информации, обрабатываемых в департаменте, вместе с перечнем предложений по совершенствованию системы защиты информации.

Необходимость реализации мероприятий по совершенствованию системы защиты информации может быть обусловлена:

– результатами проведенных аудитов и контрольных мероприятий;

– изменениями федерального законодательства в области информации;

– изменениями структуры процессов обработки информации в департаменте;

– результатами анализа инцидентов информационной безопасности;

– результатами мероприятий по контролю и надзору за обработкой информации, проводимых уполномоченным органом;

– жалоб и запросов субъектов информации.

По результатам предложений по совершенствованию системы защиты информации, комиссия составляет план работ по обеспечению безопасности информации, обрабатываемых в департаменте, на следующий год и утверждает его у начальника.

Приложение 1

**ФОРМА ЖУРНАЛА УЧЕТА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ**

| № п/п | Наименование мероприятия | Краткое описание | Дата проведения мероприятия | Ф. И. О. лица, проводившего мероприятие | Подпись лица, проводившего мероприятие | Примечание |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |