|  |  |
| --- | --- |
|  | Приложение 3 к приказу комитета по культуре города Барнаулаот 29 июля 2021 №64 |

ПОРЯДОК

организации и проведения работ по защите информации в

информационных системах

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

АТС – автоматическая телефонная станция.

ВТСС – вспомогательные технические средства и системы.

ИС – информационная система.

ГИС – государственная информационная система.

ЗП – защищаемое помещение.

ИСПДн – информационная система персональных данных.

КЗ – контролируемая зона.

КИ – конфиденциальная информация.

ЛВС – локальная вычислительная сеть.

НСД – несанкционированный доступ.

ОТСС – основные технические средства и системы.

ПЭМИН – побочные электромагнитные излучения и наводки.

РФ – Российская Федерация.

СВТ – средства вычислительной техники.

СЛЗ – средства линейного электромагнитного зашумления.

СПЗ – системы электромагнитного пространственного зашумления.

ТКУИ – технические каналы утечки информации.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к конфиденциальной информации – процедура оформления права работника комитета по культуре города Барнаула на ознакомление со сведениями, относящимися к конфиденциальным.

Доступ к информации – возможность получения информации и ее использование.

Доступ к конфиденциальной информации – ознакомление определенных лиц с КИ с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Защита конфиденциальной информации – деятельность, направленная на предотвращение НСД к КИ и (или) её утечки.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

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

Информационные системы общего пользования – федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

Контрагент – сторона гражданско-правового договора, которой обладатель КИ передал эту информацию.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Обладатель конфиденциальной информации – лицо (физическое или юридическое), которое владеет сведениями, отнесенным к конфиденциальным, на законном основании, ограничило доступ к ним и установило в отношении ее режим конфиденциальности.

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Общедоступная информация – общеизвестные сведения и иная информация, доступ к которой не ограничен.

Передача конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

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

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Предоставление конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых сведения, отнесенные к конфиденциальным, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

1. Общие положения

1.1. Порядок по организации и проведению работ по защите информации в ИС, в том числе ИСПДн (далее – Порядок) разработан с целью соблюдения правил обращения с указанной информацией в комитете по культуре города Барнаула (далее – комитет) и определяет единый для всех пользователей ИС, в том числе ИСПДн комитета, порядок допуска к этим сведениям, а также меры ответственности, применяемые за нарушение требований, установленных Порядком.

1.2. Порядок разработан на основе действующего законодательства Российской Федерации, в том числе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы по техническому и экспортному контролю Российской Федерации 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».

1.3. В Порядке отражены вопросы защиты:

ГИС;

ИСПДн;

ИС общего доступа;

других ИС, обрабатывающих сведения конфиденциального характера.

Общее название информации, обрабатываемой в данных системах, употребляемое в Порядке – защищаемые информационные ресурсы.

1.4. Защищаемые информационные ресурсы могут быть представлены в виде отдельных документов и отдельных массивов документов (на бумажных носителях), а также в виде документов (файлов) и массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных и т.п.).

1.5. Действие Порядка распространяется на сотрудников комитета, работающих по трудовому договору, заключенному с комитет, которые дали обязательство о неразглашении КИ, в том числе ПДн (далее – КИ), а также на лиц, работающих по гражданско-правовым договорам, заключенным с комитетом, взявших на себя обязательство о неразглашении КИ, в порядке и на условиях, предусмотренных Порядком.

1.6. Порядок не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

2. Принципы отнесения сведений к категории конфиденциальных, состав защищаемой информации

1.1. К категории конфиденциальных относятся сведения:

не относящиеся к сведениям, указанным в постановлении Правительства РСФСР от 05.12.1991 №35 «О перечне сведений, которые не могут составлять коммерческую тайну»;

не относящиеся к сведениям, составляющим государственную тайну;

не относящиеся к сведениям, составляющим государственную тайну;

в отношении которых комитет обязан обеспечить реализацию необходимых мер защиты (персональные данные, служебная тайна);

монопольное обладание которыми позволяет комитету при существующих или возможных обстоятельствах избежать неоправданных расходов.

1.2. Сведения, отнесенные к конфиденциальным, оформляются в виде «Перечня сведений конфиденциального характера комитета по культуре города Барнаула» (далее – Перечень сведений).

1.3. Перечень сведений конфиденциального характера должен включать:

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

сведения, составляющие тайну следствия и судопроизводства;

сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т. д.);

сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

сведения, составляющие служебную тайну, определяются действующим в субъекте Российской Федерации «Перечнем сведений, составляющих служебную информацию ограниченного распространения».

3. Порядок защиты информации в государственных информационных системах комитета

3.1. Обработка информации в ГИС осуществляется с учетом требований приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.2. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее – аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

3.3. Для пользователей ГИС, работающих в комитете, обязательным является выполнение положений, инструкций и регламентов, утвержденных в приложениях к Порядку, а также отдельных положений, инструкций и регламентов, утвержденных председателем комитета, если они регулируют вопросы обеспечения безопасности ГИС. Обязанность по ознакомлению сотрудников с регламентами лежит на ответственном за обеспечение защиты информации.

4. Порядок защиты информации в ИСПДн комитета

4.1. Обработка информации в ИСПДн осуществляется с учетом требований приказа 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».

4.2. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее – инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

4.3. Для пользователей ИСПДн, работающих в комитете, обязательным является выполнение положений, инструкций и регламентов, утвержденных в приложениях к Порядку, а также отдельных положений, инструкций и регламентов, утвержденных председателем комитета, если они регулируют вопросы обеспечения безопасности ПДн. Обязанность по ознакомлению сотрудников с регламентами лежит на ответственном за обеспечение безопасности персональных данных.

5. Порядок допуска к КИ

5.1. Все сотрудники, принимаемые на работу в комитет, должны:

ознакомиться с Порядком, а также иными документами комитета, регламентирующими вопросы обеспечения ИБ;

подписать индивидуальное письменное обязательство о неразглашении КИ в двух экземплярах по форме, утвержденной в комитете (один экземпляр передается сотруднику, второй экземпляр хранится в личном деле сотрудника не менее 3-х лет после его увольнения).

5.2. Сотрудники комитета не допускаются к работе с КИ до выполнения требований, указанных в пункте 6.1 Порядка.

5.3. Председатель комитета и его заместители имеют доступ к КИ, определенной в «Перечне сведений», в полном объеме.

5.4. Доступ сотрудников комитета к КИ, определенной в «Перечне сведений», осуществляется в пределах, необходимых для исполнения должностных обязанностей.

5.5. Доступ сотрудников комитета к КИ в ЛВС соответствует их должностным обязанностям и осуществляется в порядке, установленном в комитете.

6. Обязанности сотрудников комитета

6.1. Руководство технической защитой КИ возлагается на АИБа.

6.2. АИБ организуют и обеспечивают техническую защиту информации, циркулирующей в технических средствах и помещениях комитета.

6.3. АИБ осуществляет непосредственное руководство разработкой мероприятий по технической защите КИ и контролю в комитете.

6.4. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

6.5. Владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием КИ в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения направляются программисту комитета.

6.6. АИБ имеет право привлекать к проведению работ по технической защите КИ в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

6.7. Сотрудники комитета обязаны:

знать и соблюдать требования

 Порядка;

знать и неукоснительно выполнять все требования других нормативных документов, регламентирующих вопросы обеспечения ИБ в комитете;

соблюдать порядок работы с КИ, установленный в комитете;

принимать меры по защите КИ, соблюдать правила работы со средствами защиты информации и режим разграничения доступа к файлам с КИ при её обработке;

не разглашать и не передавать третьим лицам КИ без письменного согласия лица, предоставившего эту информацию.

7. Ответственность сотрудников комитета за разглашение КИ

7.1. Под разглашением КИ в Порядке понимается действие или бездействие, в результате которых КИ в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без письменного согласия лица, предоставившего эту информацию.

7.2. Разглашение КИ влечет за собой дисциплинарную, гражданско-правовую или уголовную ответственность в отношении лица, нарушившего режим КИ.

7.3. За умышленное или неосторожное разглашение КИ, а также нарушение порядка обращения с КИ сотрудник комитета может быть привлечен к дисциплинарной ответственности в соответствии с законодательством РФ (вплоть до увольнения).

7.4. За умышленное или неосторожное разглашение КИ, а также нарушение порядка обращения с КИ сотрудник комитета может быть привлечен к административной, гражданско-правовой или уголовной ответственности в соответствии с законодательством РФ.

7.5. По факту нарушения положений Порядка проводится служебное разбирательство, по результатам которого принимается соответствующее решение.

8. Требования к порядку учета, хранения и обращения конфиденциальных документов в комитете

8.1. Председатель комитета устанавливает и утверждает порядок учета, хранения и обращения с конфиденциальными документами и их носителями. Данный порядок должен соответствовать требованиям порядка.

8.2. В комитете учет документов и магнитных носителей с КИ должен осуществляться лицами (далее – делопроизводителями), которым поручен прием и учет несекретной документации.

9. Технические каналы утечки КИ, несанкционированного доступа и специальных воздействий на нее

9.1. Доступ к КИ, нарушение ее целостности и доступности возможно реализовать за счет:

НСД к КИ при ее обработке в информационных системах и ресурсах;

утечки КИ по техническим каналам;

9.2. Детальное описание возможных ТКУИ, НСД к информации и специальных воздействий на нее содержится в Моделях угроз безопасности информационных систем комитета.

10. Оценка возможностей технических разведок и других источников угроз безопасности КИ

10.1. Для добывания конфиденциальных сведений могут использоваться:

портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки ПЭМИН;

автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

компьютерная разведка, использующая различные способы и средства НСД к информации и специальных воздействий на нее.

10.2. Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи здания комитета.

10.3. Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.

10.4. Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

НСД к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных АРМ, в ЛВС, в распределенных телекоммуникационных системах.

10.5. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;

случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;

некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

просмотра информации с экранов дисплеев и других средств ее отображения.

10.5. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.

10.6. Наиболее опасной является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям комитета территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

10.7. Оценка возможности НСД к информации в СВТ и АС осуществляется с использованием следующих руководящих документов ФСТЭК России:

концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, утвержденная решением Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992;

средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, утвержденные решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992;

автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, утвержденные решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992.

10.8. НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к КИ и режимов обработки данных в АС.

11. Организационные и технические мероприятия по технической защите КИ

11.1. Разработка мер и обеспечение защиты КИ осуществляются специалистами, назначаемыми председателем комитета. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

11.2. Для защиты КИ должны использоваться сертифицированные по требованиям безопасности технические средства защиты.

11.3. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

11.4. Ответственность за обеспечение требований по технической защите КИ возлагается на АИБа.

12. Техническая защита информации в ЗП

12.1. Работы по технической защите КИ в ЗП должны включать следующие мероприятия:

определение перечня ЗП по результатам анализа циркулирующей в них КИ и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России;

назначение сотрудников, ответственных за выполнение требований по технической защите КИ в ЗП (далее – сотрудники, ответственные за безопасность информации);

разработка частных инструкций по обеспечению безопасности информации в ЗП;

обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения;

инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите КИ;

проведение в ЗП обязательных визуальных (непосредственно перед совещаниями) и инструментальных (перед ответственными совещаниями и периодически раз в квартал) проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП;

исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре;

оснащение телефонных аппаратов городской АТС, расположенных в ЗП, устройствами высокочастотной развязки подавления слабых сигналов, а также поддержание их в работоспособном состоянии. Для спаренных телефонов достаточно одного устройства на линию, выходящую за пределы ЗП;

осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах;

обеспечение требуемого уровня звукоизоляции входных дверей ЗП;

обеспечение требуемого уровня звукоизоляции окон ЗП;

демонтирование или заземление (с обеих сторон) лишних (незадействованных) в ЗП проводников и кабелей;

отключение при проведении совещаний в ЗП всех неиспользуемых электро- и радиоприборов от сетей питания и трансляции;

выполнение перед проведением совещаний следующих условий: окна должны быть плотно закрыты и зашторены; двери плотно прикрыты;

защита информации, циркулирующей в ОТСС и наводящейся в ВТСС;

при эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию;

при невозможности обеспечения КЗ заданных размеров необходимо применение СПЗ в районе размещения защищаемого ОТСС, применение СЛЗ линий электропитания, радиотрансляции, заземления, связи;

Техническая защита информации в СВТ и АС от НСД в соответствии с требованиями руководящих документов ФСТЭК России должна обеспечиваться путем:

проведения классификации СВТ и АС;

выполнения необходимых организационных мер защиты;

установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД;

защита каналов связи, предназначенных для передачи КИ;

защиты информации от воздействия программ-закладок и компьютерных вирусов.

12.2. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются Порядком, действующими государственными стандартами и другими нормативными и методическими документами ФСТЭК России.

12.3. Организация антивирусной защиты информации на объектах информатизации достигается путём:

установки и применения средств антивирусной защиты информации;

обновления баз данных средств антивирусной защиты информации;

действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

12.4. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

13. Планирование работ по технической защите КИ и контролю

13.1. В комитете должны составляться годовые планы работ по технической защите КИ и контролю.

13.2. В годовые планы по технической защите КИ и контролю должны включаться:

мероприятия по выполнению требований законодательства по вопросам защиты КИ;

подготовка проектов распорядительных документов по вопросам организации технической защиты информации в комитете, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на АРМ, в ЗП;

аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите КИ;

проведение периодического контроля состояния технической защиты информации;

мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

мероприятия по совершенствованию технической защиты информации на объектах комитета.

13.3. Контроль выполнения планов и отчетность по ним возлагается на АИБа.

14. Взаимодействие с предприятиями, учреждениями и организациями

14.1. При проведении совместных работ комитете с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита информации, составляющей КИ, независимо от места проведения работ.

14.2. В технических заданиях на выполнение совместных работ с использованием КИ, должны быть предусмотрены требования (или меры) по ее технической защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с ответственным по технической защите КИ сотрудником и взаимодействующих предприятий (учреждений, организаций).

14.3. Организация технической защиты информации возлагается на руководителей совместных работ, а ответственность за обеспечение технической защиты информации – на исполнителей работ (пользователей) при использовании ими технических средств для обработки и передачи информации, подлежащей защите.

15. Заключительные положения

15.1. Проверка наличия документов, магнитных носителей информации и дел с грифом «Конфиденциально» проводится один раз в год комиссией, назначаемой председателем комитета, проверки оформляются актом.

15.2 Доступ правоохранительных органов Российской Федерации к КИ комитета, определенной в «Перечне сведений», осуществляется в соответствии с действующим законодательством Российской Федерации.

15.3 Раскрытие юридическим или физическим лицам сведений конфиденциального характера комитета возможно в случае привлечения их к совместной хозяйственной, финансовой и иной деятельности, требующей передачи конфиденциальных сведений, и только в том объеме, который необходим для реализации целей и задач комитета, а также при условии принятия ими на себя обязательств по неразглашению и исключению неправомерного использования полученных сведений.

15.4. Конфиденциальные сведения других юридических или физических лиц, переданные комитету для выполнения работ или осуществления иной совместной деятельности, и в отношении которых комитет взял на себя обязательство о неразглашении и исключении неправомерного их использования, подлежат защите наравне с другими сведениями конфиденциального характера комитета.

15.5. Контроль состояния технической защиты КИ осуществляется:

ФСТЭК России (силами Центрального аппарата и Управления по соответствующему федеральному округу);

ФСБ России;

внутренней комиссией комитета– не реже 1 раза в год;

структурным подразделением, ответственным по обеспечению информационной безопасности – непрерывно.

15.5. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты КИ, решений ФСТЭК России, комитета, наличия соответствующих документов по технической защите КИ, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.