ОБЩИЕ СВЕДЕНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ

В соответствии со статьей 8 Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности» Президент Российской Федерации устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых он осуществляет и решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты информации и государственной тайны.

Соответствующими указами Президентом определены федеральные органы исполнительной власти, реализующие полномочия по защите информации:

Федеральная служба то техническому и экспортному контролю Российской Федерации (ФСТЭК России) - Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- противодействия иностранным техническим разведкам на территории Российской Федерации;
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения государственными органами и организациями.

ФСТЭК России осуществляет методическое руководство деятельностью государственных органов и организаций в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.

Федеральная служба безопасности Российской Федерации (ФСБ России) - Указ Президента РФ от 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации».

Основными задачами ФСБ России в области защиты информации являются:

- обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;
- формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;
- организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Различие компетенций вышеперечисленных органов исполнительной власти заключается в следующем:

ФСТЭК России формирует требования и производит контроль мероприятий по защите информации **некриптографическими методами** (разграничение прав пользователей, защита информации от побочных электромагнитных излучений, защита речевой информации и др.);

ФСБ России формирует требования и производит контроль мероприятий по защите информации **криптографическими методами** (защита каналов связи, электронная подпись).

Защита информации некриптографическими методами является наиболее массовым видом при создании защищенных информационных систем.

В соответствии со статьей 12 федерального закона «О безопасности» органы государственной власти субъектов Российской Федерации и органы местного самоуправления в пределах своей компетенции **обеспечивают исполнение законодательства Российской Федерации в области обеспечения безопасности**.

2. Нормативно-правовая база защиты информации

Основным документом, определяющим порядок создания системы защиты информации и проведения контроля, является «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденное Постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 № 912-51.

Организация работ по защите информации в органах исполнительной власти осуществляется **их руководителями**. Для организации и проведения работы по защите информации создаются специальные **подразделения по защите информации** (или штатные специалисты).

В органах исполнительной власти субъекта может циркулировать два вида информации подлежащей обязательной защите в соответствии с действующим законодательством:

1. **Информация, составляющая государственную тайну** (Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»).

2. **Конфиденциальная информация** (Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»), которая в свою очередь делится на несколько составляющих, наиболее часто встречающихся в исполнительных органах власти:

персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу);

служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами (**служебная тайна – сведения, содержащие информацию ограниченного доступа, документы с пометкой «Для служебного пользования»**).

Для вышеперечисленных видов информации должны в обязательном порядке применяться меры по защите информации.

Одна из основных целей защиты информации – это предотвращение ее утечки по техническим каналам.

В соответствии со статьей 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, **обладатель информации, обязан** обеспечить:

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

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

6) постоянный контроль за обеспечением уровня защищенности информации.

3. Требования по защите информации

Конкретные требования по защите информации, которые должен обеспечить обладатель информации, отражены в руководящих документах ФСТЭК и ФСБ России. Документы также делятся на ряд направлений:

- защита информации при обработке сведений, составляющих государственную тайну;
- защита конфиденциальной информации (в т.ч. персональных данных);
- защита информации в ключевых системах информационной инфраструктуры.

Конкретные требования по защите информации определены в руководящих документах ФСТЭК России.

При создании и эксплуатации государственных информационных систем (а это все информационные системы областных органов исполнительной власти) методы и способы защиты информации должны соответствовать требованиям ФСТЭК и ФСБ России.

Документы, определяющие порядок защиты конфиденциальной информации и защиты информации в ключевых системах информационной инфраструктуры имеют пометку «Для служебного пользования». Документы по технической защите информации, как правило, имеют гриф «секретно».

4. Аттестация объектов информатизации

Основной единицей в терминах защиты информации принято считать **объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров (*если упрощенно, объекты информатизации – это автоматизированные системы, на которых обрабатывается защищаемая информация и защищаемые помещения, в которых ведутся конфиденциальные переговоры*).

Подтверждением того, что объект информатизации защищен, является наличие на объекте «аттестата соответствия» («Положение по аттестации объектов информатизации по требованиям безопасности информации». Утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября1994 г.).

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленным в «Аттестате соответствия».

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки конфиденциальной информации, информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация проводится органом по аттестации (организация, имеющая лицензии ФСТЭК России).

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители.

Для проведения аттестации объектов информатизации, на которых обрабатывается:

информация, содержащая сведения, составляющие государственную тайну, требуется лицензия ФСТЭК России на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны (в части технической защиты информации);

конфиденциальная информация требуется лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

5. Сертификация средств защиты информации

В соответствии с Постановлением Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации» технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Оценка соответствия средств, предназначенных для защиты информации конфиденциального характера проводится на основании Постановления Правительства РФ «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)» от 15 мая2010 г. № 330дсп.

На аттестованных объектах информатизации должны применяться сертифицированные по требованиям безопасности информации средства защиты информации. Сертификация средств защиты осуществляется испытательными лабораториями.

Федеральными органами по сертификации являются ФСТЭК России и ФСБ России в части:

- разработки и производства средств защиты информации, составляющей государственную тайну;
- разработки и производства средств защиты конфиденциальной информации.
-

6. Построение системы защиты информации в организации

Вопросы создания и непосредственного руководства подразделениями по защите информации в органах государственной власти возлагаются на руководителей органов государственной власти или их заместителей.

Для организации и проведения работ по защите информации создаются специальные **подразделения по защите информации (или штатные специалисты).**

Указанные подразделения организуют свою деятельность в соответствии с «Типовым положением о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации», утвержденным решением Гостехкомиссии России от 14 марта1995 г. № 32.

7. Контроль состояния защиты информации

Контроль состояния защиты информации (далее - контроль) осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки защиты ее от иностранных технических разведок.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений ФСТЭК России, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

Контроль организуется ФСТЭК России, ФСБ России, другими органами государственной власти, входящими в государственную систему защиты информации, и предприятиями в соответствии с их компетенцией.

ФСТЭК России организует контроль силами центрального аппарата и территориальных Управлений ФСТЭК России.

Центральный аппарат ФСТЭК России осуществляет в пределах своей компетенции контроль в органах государственной власти и на предприятиях, обеспечивает методическое руководство работами по контролю.

Территориальные управления ФСТЭК России, в пределах своей компетенции осуществляют контроль в органах государственной власти и на предприятиях, расположенных в зонах ответственности этих управлений.

Органы государственной власти организуют и осуществляют контроль на подчиненных им предприятиях через свои подразделения по защите информации. Повседневный контроль за состоянием защиты информации на предприятиях проводится силами их подразделений по защите информации.

Контроль на предприятиях негосударственного сектора при выполнении работ с использованием сведений, отнесенных к государственной или служебной тайнам, осуществляется органами государственной власти, ФСТЭК России, ФСБ России и заказчиком работ в соответствии с их компетенцией.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.