Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

сборник учебно-методических материалов

для направления подготовки 10.03.01 Информационная безопасность

Благовещенск
2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
университета

Составитель: Самохвалова С.Г.

Организационное и правовое обеспечение информационной безопасности: сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019

КРАТКОЕ ИЗЛОЖЕНИЕ ЛЕКЦИОННОГО МАТЕРИАЛА

Организационные системы обеспечения безопасности информации

Основой современной политики Российской Федерации в сфере информационной безопасности можно считать "Доктрину информационной безопасности РФ", утвержденную Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Этот документ:

- описывает основные предпосылки формирования государственной политики в данной сфере (потребность в безопасности, существующие интересы, угрозы, *источники угроз* и т.п.);
- формулирует базовые задачи государства и общества, основанные непосредственно на необходимости выполнения требований Конституции, обеспечения суверенитета страны и т.п.;
- описывает состояние дел в сфере общегосударственного регулирования процессов информационной безопасности на момент утверждения Доктрины (основные достижения и недостатки);
- перечисляет приоритетные направления деятельности государства (задачи, требующие безотлагательного решения) по обеспечению информационной безопасности;
- формулирует основные методики, которые государство должно использовать для обеспечения информационной безопасности, а также специфику применения этих методов в отдельных областях общественной жизни;
- перечисляет основные информационные объекты (в различных сферах), на охрану которых должна быть направлена государственная политика;
- описывает основные направления международного сотрудничества в сфере информационной безопасности;
- перечисляет основные организационные инструменты, используемые для реализации государственной политики и осуществления государственного управления в сфере информационной безопасности;
- описывает распределение ответственности между основными органами государственной власти, решающими задачи в сфере информационной безопасности.

В соответствии с Доктриной государство должно уделять внимание информационной безопасности в таких основных сферах, как:

- экономика;
- внутренняя политика;
- внешняя политика;
- наука и техника;
- духовная жизнь;
- информационные системы государственного управления;
- оборона.

К числу первоочередных мероприятий, которые должны быть реализованы на государственном уровне, Доктрина относит:

- совершенствование законодательной базы в сфере информационных отношений;
- разработку механизмов управления государственными средствами массовой информации и реализации государственной информационной политики;
- подготовку кадров для работы в сфере информационной безопасности;
- совершенствование и развитие системы государственных стандартов в сфере информатизации и обеспечения информационной безопасности;
- принятие и реализацию федеральных программ, решающих определенные задачи информатизации и обеспечения информационной безопасности: создание информационных архивов и информационно-телекоммуникационных систем органов власти, развитие информационной культуры населения и т.п.

Как можно видеть из этого перечня, а также в целом из текста Доктрины, она предполагает определенное расширение понятия "*информационная безопасность*" и включение в него некоторых вопросов, которые связаны с деятельностью средств массовой информации и другими аспектами информационной политики, не имеющими прямого отношения к категории "*информационная безопасность*" в ее первоначальном понимании.

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- Федеральный Закон "О *государственной тайне*";
- Федеральный Закон "Об информации, информационных технологиях и о защите информации".

Структура органов государственной власти, обеспечивающих информационную безопасность в РФ

Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является **Совет безопасности РФ**.

Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является **Федеральная служба по техническому и экспортному контролю – ФСТЭК**. Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также **Служба специальной связи и информации ("Спецсвязь России")**, с 2004 года входящая в состав Федеральной службы охраны. Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

- Министерство связи и массовых коммуникаций РФ;
- Министерство внутренних дел РФ.

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия *по* обеспечению защиты информации:

- ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);
- Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр "Атомзащитаинформ");
- Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации)
- и некоторые другие.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, **информационной**, экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

- подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;
- рассмотрение законопроектов, в рамках своей компетенции;
- организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ, осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и др.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия *по* информационной безопасности. Функциями Управления информационной безопасности являются:

- подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;
- анализ и прогнозирование ситуации в области информационной безопасности РФ;
- выявление источников опасности, оценка внешних и внутренних *угроз информационной безопасности* и подготовка предложений Совету Безопасности по их предотвращению;

• рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;

• участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ;

• подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;

• подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ.

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как **Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия РФ)**, была создана в январе 1992 года на базе Гостехкомиссии СССР *по* противодействию иностранным технологическим разведкам, которая, в свою *очередь* ведет отсчет своего существования с декабря 1973 года. Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и других.

Основными функциями ФСТЭК являются:

• проведение единой технической политики и координация работ по защите информации;

• организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;

• поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.

Для реализации функций *по* лицензированию в составе ФСТЭК функционируют 7 региональных управлений (*по* федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь России), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

При этом задачами Спецсвязи также являются:

• проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;

• организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи России;

• участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;

• участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих *государственную тайну*;

• участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров;

• организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи России;

• выполнение требований обеспечения информационной безопасности объектов государственной охраны.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды *работ* в сфере информационной безопасности:

• подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

• ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;

• выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий.

Уполномоченным органом *по* ведению реестра доверенных удостоверяющих центров является ФГУП НИИ "Восход".

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)является уполномоченным федеральным органом исполнительной власти *по* защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ.

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является **Комитет по безопасности Государственной думы Федерального собрания Российской Федерации**. В составе этого Комитета функционирует **Подкомитет по информационной безопасности**. В законодательной работе в рамках этого Комитета принимают участие:

• специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и других ведомств;

• руководители Совета безопасности РФ и других правительственных органов;

• представители общественных организаций, фондов и профессиональных объединений;

• представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и др.);

• представители ведущих научно-исследовательских учреждений и учебных заведений.

Организационная структура системы обеспечения информационной безопасности представлена на рисунке 1.

Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры по координации работ в области информационной безопасности.

Основным международным органом является Организация Объединенных Наций и созданный ею Совет Безопасности. Эти органы координируют усилия государств по осуществлению мероприятий в области обеспечения информационной безопасности и борьбе с преступлениями в сфере информационных технологий. Спорные вопросы на межгосударственном уровне решает международный суд.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти фе-

дерального уровня, уровня субъектов Российской Федерации, ведомственных структур, а также служб предприятий и организаций.

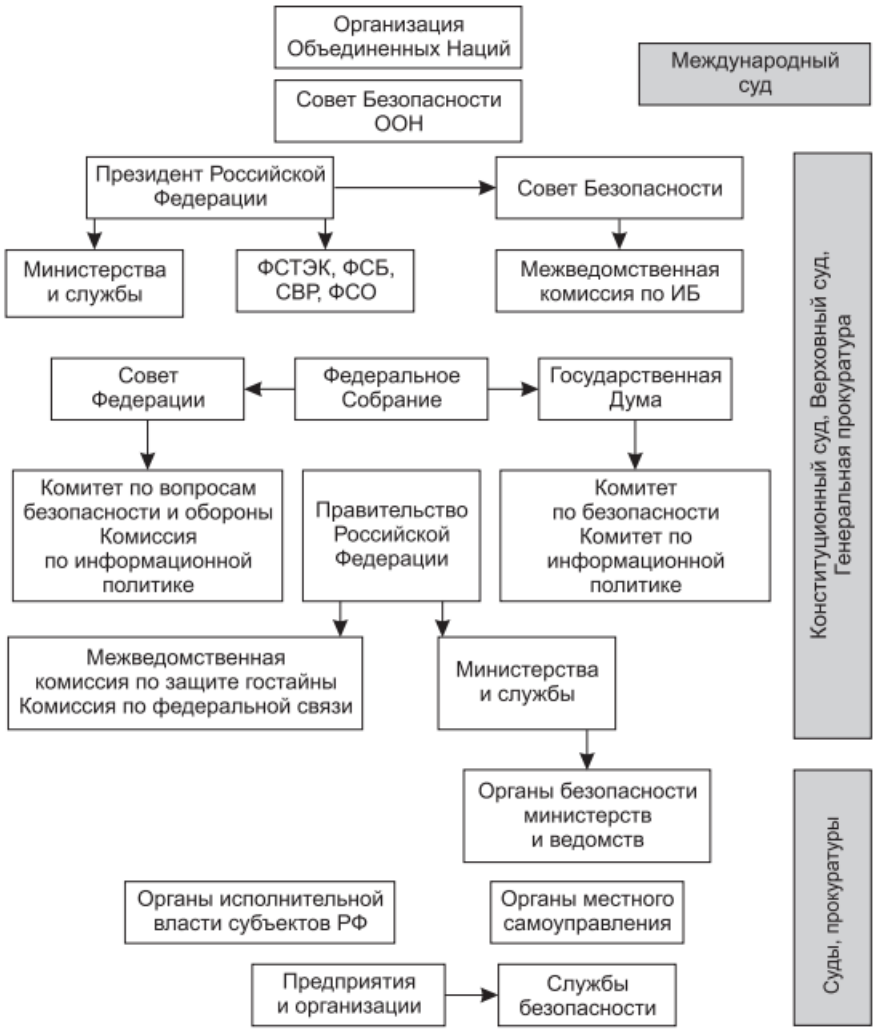


Рис. 1. Структура органов обеспечения информационной безопасности

Организационная защита информации по своей сути является организационным началом, так называемым "ядром" в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия организационных задач зависит эффективность решения проблем в данной области в целом.

Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исходя из исключительной важности принятия руководством правильного и своевременного управленческого решения на основе действующего нормативно-методического аппарата, а также имеющихся в его распоряжении сил, средств, методов и способов защиты информации. Основные направления защиты информации представлены на рисунке 2.

Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности руководителя предприятия сегодня являются: планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений по непосредственному доступу к конфиденциальной информации своих сотрудников и представителей других организаций; распределение обязанностей и задач между должностными лицами и структурными подразделениями; аналитическая работа и т.д.

Рис. 2. Основные направления защиты информации

Цель принимаемых руководством предприятия и должностными лицами организационных мер - исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые в свою очередь определяются состоянием устремленности разведок противника (действиями конкурента на рынке товаров и услуг), направленным на овладение информацией, подлежащей защите. Это правило действует как на государственном уровне, так и на уровне отдельного предприятия.

Таким образом, для раскрытия понятия "организационная защита информации", могут использоваться два, равных по своей сути, определения организационной зашиты информации.

Организационная защита информации - составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационно-правовая защита информации - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе - раскрывает ее структуру на уровне предприятия.

Вместе с тем, оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

Основные направления организационной защиты информации приведены на рисунке 3.

Рис. 3. Основные направления организационной защиты информации

Таким образом, организационная защита информации сегодня является важнейшим элементом в общей системе защиты информации предприятия, с высокой эффективностью обеспечивающим ее защиту при условии соблюдения должностными лицами предприятия норм и правил защиты информации, определенных в соответствующих нормативно-методических документах.

Основными принципами организационной защиты информации являются следующие принципы:

принцип комплексного подхода к решению задач защиты информации;

принцип оперативности принятия управленческих решений;

принцип персональной ответственности.

Принцип комплексного подхода заключается в использовании сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу возможной утечки конфиденциальной информации.

Принцип оперативности принятия управленческих решений существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает целеустремленность должностных лиц на решение задач защиты информации.

Принцип персональной ответственности заключается в наиболее эффективном и полном распределении сил структурных подразделений предприятия, участвующих в процессе защиты информации.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа состояния системы защиты информации с целью принятия своевременных мер по повышению ее эффективности;
- неукоснительное соблюдение должностными лицами и сотрудниками структурных подразделений предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении вышеперечисленных условий будет обеспечено наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Нормативные акты, служащие основанием для организационно-распорядительной документации по защите информации

Правовое обеспечение информационной безопасности заключается в исполнении существующих или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц, руководителей, пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной им информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к техническим средствам и информации. Целью законодательных мер по защите информации являются предупреждение и сдерживание потенциальных нарушителей.

Нормативная правовая информация создается в порядке правотворческой деятельности и содержится в нормативных правовых актах. Классификация такой информации по уровню принятия актов или по видам актов приведена на рис.4.

На следующем рис. 5 представлена обобщенная схема нормативно-правового и справочного обеспечения информационной безопасности (ИБ) информационных технологий (ИТ).

В соответствии с Конституцией России международные документы, подписанные от имени Российской Федерации, имеют приоритет над соответствующими документами федерального уровня. Документы, не подписанные от имени России, могут использоваться, если они не противоречат законодательству страны.

К числу международных актов относят: декларации; конвенции; рекомендации; соглашения; стандарты. Разработкой этих документов занимаются различные структурные подразделения международных организаций, такие как: Организация Объединенных Наций; Совет Европы (комитет министров) и др.

Рис. 4. Классификация нормативной правовой информации по видам актов

Рис. 5. Обобщенная схема нормативно-справочного обеспечения информационной безопасности (ИБ) информационных технологий

Среди всех международных нормативных актов в области информационной безопасности в нашей стране чаще всего применяются организационно-технические документы, в частности стандарты.

Большая часть из них принята в качестве национальных стандартов в сфере защиты информации.

Отечественная федеральная и ведомственная нормативная база по защите информации к настоящему времени включает более сотни нормативных документов, относящихся к вопросам информационной безопасности на государственном, региональном, местном, ведомственном уровнях. По своему назначению и содержанию их можно разделить на три группы:

1. Концептуальные документы, определяющие основу защиты информации в России.
2. Федеральные законы, определяющие систему защиты информации в России.
3. Вспомогательные нормативные акты в виде указов Президента РФ, постановлений Правительства РФ, межведомственных и ведомственных руководящих документов и стандартов, регулирующих процесс и механизмы исполнения положений и требований к системе обеспечения информационной безопасности государства.

Стандарты по ЗИ подразделяют на следующие категории:

международные (ГОСТ ИСО);

межгосударственные (ГОСТ);

государственные стандарты Российской Федерации, оформленные на основе аутентичного текста международного стандарта (ГОСТ Р ИСО/МЭК);

государственные стандарты Российской Федерации (ГОСТ Р);

государственные военные стандарты Российской Федерации (ГОСТ РВ);

стандарты отраслей, в том числе и на оборонную продукцию (ОСТ);

стандарты предприятий.

Зарубежные стандарты в области информационной безопасности Стандарты и спецификации можно условно разделить на два вида:

- оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;
- технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Важно отметить, что между этими видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Технические спецификации имеют ряд положительных и отрицательных аспектов. Главные достоинства этих стандартов состоят в следующем:

Стандарт гарантирует большой сектор рынка для определенного типа оборудования или программного обеспечения. Это поощряет массовое производство и в некоторых случаях использование методов интеграции высокого и сверхвысокого уровня, что приводит к снижению цен.

Стандарт обеспечивает взаимодействие устройств, разработанных различными производителями, что обеспечивает большую гибкость при выборе и использовании оборудования.

Ниже перечислены основные недостатки технических стандартов:

Стандартизация ведет к замораживанию технологии. За то время пока стандарт разрабатывается, проходит проверку, согласуется, пересматривается и, наконец, публикуется, могут появиться новые, более эффективные технологии.

Существует множество стандартов, относящихся к одной и той же области деятельности. Это не является недостатком самих стандартов, а отражает сегодняшнюю технологию стандартизации. К счастью, в последние годы многие организации, занимающиеся разработкой стандартов, начали тесно сотрудничать. Тем не менее, существуют сферы, в которых стандарты иногда конфликтуют друг с другом.

Исторически первым широко распространившимся документом, получившем статус стандарта, были Критерии безопасности компьютерных систем Министерства обороны США. Критерии безопасности компьютерных систем (TCSEC – Trusted Computer System Evaluation Criteria), получившие неформальное, но прочно закрепившееся название «Оранжевая книга» (по цвету изданной брошюры), были разработаны Министерством обороны США в 1983 г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.

В 1985 г. «Оранжевая книга» была принята в качестве стандарта Министерства обороны США (DoD TCSEC). В 1987 и 1991 гг. стандарт был дополнен требованиями для гарантированной поддержки политики безопасности в распределенных вычислительных сетях и базах данных.

В данном документе впервые нормативно определены такие понятия, как «политика безопасности», вычислительная база защиты или ядро защиты (TCB, Trusted Computing Base) и т.д.

Проблемы стандартизации в сфере информационной безопасности оказались актуальны не только для Соединенных Штатов. Вслед за выходом «Оранжевой книги» страны Европы разработали согласованные «Критерии безопасности информационных технологий» (Information Technology Security Evaluation Criteria, далее – Европейские критерии).

Европейские критерии рассматривают следующие задачи средств информационной безопасности:

- защита информации от несанкционированного доступа с целью обеспечения ее конфиденциальности;
- обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;
- обеспечение доступности компьютерных систем с помощью противодействия угрозам отказа в обслуживании.

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и доступности, необходимо реализовать соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев и т.д. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования. Для решения этой проблемы в Европейских критериях впервые вводится понятие адекватности (assurance) средств защиты.

Адекватность включает в себя два аспекта: эффективность, отражающую соответствие средств безопасности решаемым задачам, и корректность, характеризующую процесс их разработки и функционирования.

Рекомендации X.800 . Технические спецификации X.800 появились немногим позднее «Оранжевой книги», но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем. Рекомендации X.800 – документ довольно обширный.

Руководящие документы Гостехкомиссии (ФСТЭК) России. Рассмотрим два важных Руководящих документа – Классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и аналогичную Классификацию межсетевых экранов (МЭ).

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Классификации межсетевых экранов – представляется принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования. РД получил высокую оценку не только в России, но и в мире.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» относится к разновидности стандартов, оформленных на основе аутентичного текста. Основой для него стал описанный выше международный стандарт ISO/IEC 15408-99 «Общие критерии безопасности информационных технологий» (далее –ОК).

Общие критерии состоят из 3-х частей:

1. Введение и общая модель.
2. Функциональные требования безопасности.
3. Требования доверия к безопасности.

Область использования ОК включает как процесс разработки ИТ-продуктов или АС, так и приобретение коммерческих продуктов и систем. При проведении оценки такой продукт или систему информационных технологий называют объектом оценки (ОО), к числу которых ОК относят: ВС, ОС, распределенные системы, вычислительные сети и приложения.

Концепция построения системы безопасности предприятия

Успешное решение комплекса задач по защите конфиденциальной информации не может быть достигнуто без создания единой основы, так называемого "активного кулака" предприятия, способного концентрировать все усилия, имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ему ущерба.

Таким "кулаком" призвана стать система защиты информации на предприятии, создаваемая на нормативно-методической основе в данной области и отражающая все направления и специфику его деятельности.

Под системой защиты информации понимается совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях. Структура системы защиты информации приведена на рисунке 6.

Для решения организационных задач по созданию и функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

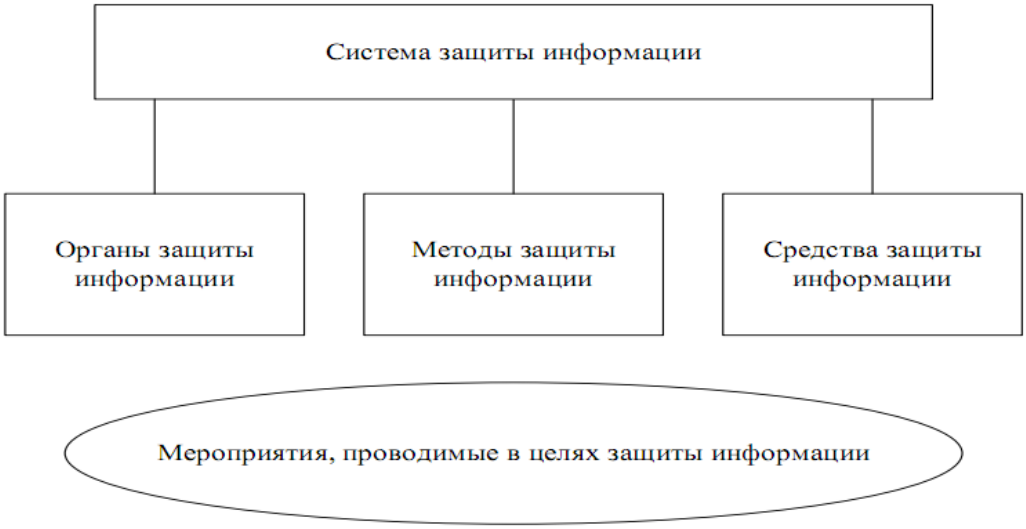


Рис. 6. Структура системы защиты информации

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также наработанных деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, связанным с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. На этой основе формируется перечень возможных угроз информации, подлежащей защите, и определяются предполагаемые к использованию в этих целях конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

централизованной - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия;

плановой - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием;

конкретной и целенаправленной - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций;

активной - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

надежной и универсальной - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

Одним из важнейших факторов, оказывающих существенное влияние на эффективность системы защиты конфиденциальной информации, является совокупность сил и средств предприятия, используемых для организации защиты информации и непосредственно участвующих в этом процессе.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, осуществляющие работу с конфиденциальной информацией и решающие задачи по ее защите на постоянной основе, то есть в каждодневной деятельности, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации.

Предприятиями, осуществляющими эпизодическую работу с конфиденциальной информацией, в силу ее небольших объемов, вместо создания вышеупомянутых подразделений в штаты своих предприятий могут включаться самостоятельные должности специалистов по защите информации.

Наряду с этим, данные предприятия на договорной основе могут использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников и высокоэффективные средства защиты информации. Эти вопросы регулируются нормативными актами, определяющими порядок оказания услуг в данной области.

Ведущую роль в организации защиты информации на предприятии играет руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия в соответствии с законодательством несет персональную ответственность за организацию и осуществление необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации.

Руководитель предприятия при организации работ по защите информации обязан:

- знать фактическое состояние дел по этим вопросам, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- предъявлять высокую требовательность к сотрудникам предприятия в вопросах сохранности сведений конфиденциального характера;
- оценивать деятельность должностных лиц по защите информации и эффективность проводимых в целях защиты соответствующих сведений мероприятий.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия с целью принятия своевременных мер по защите информации; руководить работой службы безопасности (структурных подразделений по защите государственной тайны), а также выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.

В структуре предприятий с целью организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

- режимно-секретные;
- подразделения по противодействию иностранным техническим разведкам и технической защите информации;
- подразделения криптографической защиты информации;
- мобилизационные;
- подразделения охраны и пропускного режима.

Функции, возлагаемые на вышеперечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

По решению руководителя предприятия вышеупомянутые подразделения могут быть структурно объединены в службу режима предприятия, руководитель которой наделяется статусом за-

местителя руководителя предприятия, и полномочиями должностного лица, имеющего право осуществлять непосредственное руководство деятельностью всех подразделений предприятия, если их деятельность связана с использованием информации, отнесенной к конфиденциальной информации (государственной тайне) и подлежащей защите.

Кроме вышеперечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения предприятия, основным направлением деятельности которых защита информации не является. Это - кадровые органы, органы юридической службы, органы психологической работы. Особо необходимо отметить участие в организации защиты информации производственных, так называемых "тематических" подразделений, непосредственно создающих продукцию, товары и услуги, и, в этой связи, непосредственно взаимодействующих с другими предприятиями и органами государственной власти.

При проведении работ по организации защиты информации используются и возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. Это - постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов автоматизации и другие.

Однако, для достижения наиболее эффективного результата при решении задач защиты конфиденциальной информации, наряду с использованием возможностей вышеупомянутых штатных и нештатных подразделений, необходимо комплексное применение имеющихся на предприятии средств защиты конфиденциальной информации.

Под средствами защиты информации понимаются технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, специальные средства, в которых они реализованы, а также средства, устройства и системы контроля эффективности защиты информации.

Общие методы защиты информации разделяются на правовые, организационно-технические и экономические.

Содержание правовых методов защиты информации направлено на решение следующих задач:

- разработку, совершенствование и обеспечение функционирования механизмов отнесения сведений к информации ограниченного доступа, засекречивания (рассекречивания) носителей информации, составляющей государственную тайну и иную охраняемую законом тайну, установления (снятия) ограничительных грифов для носителей конфиденциальной информации;
- определение перечней сведений, отнесенных к государственной (коммерческой) тайне;
- установление правового режима работы органов защиты информации;
- установление порядка доступа и допуска должностных лиц и граждан к государственной тайне и т.д.

Организационные методы защиты информации подразделяются по следующим классам:

- организация и соблюдение определенного порядка управленческой деятельности предприятия, направленная снижение риска утраты, утечки, модификации сведений конфиденциального характера;
- установление и соблюдение требований по организации и ведению конфиденциального делопроизводства, в том числе по размещению, оборудованию и охране;
- работа по ограничению (разграничению) круга должностных лиц предприятия по доступу к государственной тайне и конфиденциальной информации;
- осуществление принципа персональной ответственности должностных лиц за сохранность доверенной информации;
- организация подбора лиц, работающих с важной информацией их воспитание и обучение;
- систематический контроль за соблюдением режима защиты данных и оказание помощи подчиненным структурным подразделениям;
- мероприятия по сокращению оборота носителей секретной и конфиденциальной информации, систематический отбор и уничтожение ненужных носителей.

Таким образом, эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия методов защиты информации и соответствующих сил и средств.

Организация и функции службы безопасности предприятия

Внутриобъектовый и пропускной режимы устанавливаются на предприятиях, осуществляющих в предусмотренном законодательством РФ порядке работу со сведениями, составляющими государственную тайну.

Внутриобъектовый и пропускной режимы являются основными элементами системы защиты информации предприятия.

Их организация является обязательным условием соблюдения требований нормативно-методических документов по защите государственной (коммерческую) тайны, предоставляющим предприятию право на проведение в установленном порядке работ, связанных с использованием сведений, составляющих государственную (коммерческую) тайну.

Основными общими целями организации внутриобъектового и пропускного режимов на предприятии являются исключение (предотвращение):

- проникновения посторонних лиц на охраняемую (режимную) территорию и объекты предприятия, а также в служебные помещения, в которых проводятся работы с использованием сведений, составляющих государственную (коммерческую) тайну;
- посещения режимных помещений без служебной необходимости сотрудниками предприятия, не имеющими к ним прямого отношения, а также командированными лицами, не имеющими служебного задания на их посещение (работу в них);
- вноса (ввоза) на территорию предприятия личных технических средств: кино-, фото-, видео-, звукозаписывающей аппаратуры и других технических средств;
- несанкционированного выноса (вывоза) с территории предприятия носителей сведений, составляющих государственную (коммерческую) тайну;
- нарушений установленного регламента служебного времени, распорядка работы структурных подразделений по защите государственной (коммерческой) тайны, а также установленного порядка и режима работы сотрудников предприятия и командированных лиц с носителями сведений, составляющих государственную (коммерческую) тайну.

Организация и обеспечение внутриобъектового и пропускного режимов на предприятии в совокупности направлены на соблюдение всеми сотрудниками предприятия и командированными лицами надлежащего режима секретности.

Режим секретности - это установленный нормативными актами единый порядок обеспечения защиты сведений, составляющих государственную (коммерческую) тайну, включающий систему административно-правовых, организационных, инженерно-технических и других мер.

Таким образом, внутриобъектовый и пропускной режимы являются неотъемлемой частью системы установления и реализации комплекса мероприятий, направленных на защиту сведений, составляющих государственную (коммерческую) тайну, и сохранность их носителей.

Внутриобъектовый режим - совокупность комплекса мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия.

Основными целями внутриобъектового режима на предприятии являются:

- определение требований по общему режиму секретности на предприятии на основе положений нормативных правовых актов и указаний вышестоящих органов государственной власти (предприятий);
- ограничение круга лиц, допускаемых к сведениям, составляющим государственную (коммерческую) тайну, и их носителям;
- регламентация порядка и правил непосредственной работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную (коммерческую) тайну;

- планирование комплекса мероприятий, направленных на исключение утечки сведений, составляющих государственную (коммерческую) тайну, и утрат носителей этих сведений;

- организация контроля со стороны должностных лиц предприятия и структурных подразделений по защите государственной (коммерческой) тайны за выполнением требований по режиму секретности на предприятии;

- организация работы с персоналом предприятия, допущенным к сведениям, составляющим государственную (коммерческую) тайну, а также с вновь принимаемыми на работу гражданами.

Задачи по организации внутриобъектового режима на предприятии возлагаются, как правило, на заместителя руководителя предприятия, отвечающего за вопросы защиты государственной (коммерческой) тайны. Заместитель руководителя предприятия работу по формированию внутриобъектового режима организует на основе всестороннего анализа возможных каналов утечки сведений, составляющих государственную (коммерческую) тайну, при проведении предприятием всех видов работ.

Важнейшую роль в организации внутриобъектового режима выполняют руководитель предприятия и его заместитель, в соответствии со своими должностными обязанностями непосредственно возглавляющий работу по защите государственной (коммерческой) тайны.

В соответствии с нормативными актами непосредственная ответственность за организацию и осуществление необходимых мероприятий по защите государственной (коммерческой) тайны возлагается на руководителя предприятия.

Основными структурными подразделениями предприятия, участвующими в организации внутриобъектового режима, являются: режимно-секретное подразделение, служба безопасности предприятия, подразделение противодействия техническим средствам разведки конкурента, подразделение охраны (в части вопросов контроля внутренних объектов и служебных помещений предприятия).

Организация информационно-аналитической работы

Информационно-аналитическая деятельность – это особая сфера человеческой деятельности, призванная обеспечить информационные потребности общества с помощью аналитических технологий, за счет переработки исходной информации, получения качественно нового знания. В ней выделяют три уровня: информационно-технологический, информационный и аналитический. Главная цель информационно-аналитической деятельности – создание на базе добываемых и собираемых сведений и материалов, которые часто имеют отрывочный, разрозненный и противоречивый характер, обобщенной, а поэтому качественно новой специальной информации.

Информационно-аналитическая работа – это специфический вид мыслительной деятельности человека, связанный с извлечением из некоторого массива входных данных информации (нового знания). Основная задача информационно-аналитической работы состоит в извлечении максимального количества релевантной (относящейся к решаемой задаче) информации из наличествующих или поступающих данных. Необходимость поиска существующих связей между отдельными явлениями обусловливает появление и развитие аналитических методов.

Аналитические методы обработки информации очень важны и успешно используются большинством фирм. Не в последнюю очередь в аналитической обработке нуждаются сведения, получаемые и используемые службой безопасности фирмы. Такие сведения отрывочны, противоречивы, зачастую недостоверны, но именно на их основе принимаются жизненно важные для фирмы решения.

Информационно-аналитическая деятельность службы безопасности фирмы представляет собой системное получение, анализ и накопление информации с элементами прогнозирования по вопросам, относящимся к безопасности фирмы, и на этой основе консультирование и подготовка рекомендаций руководству о правомерной защите от противоправных посягательств.

Служба безопасности проводит аналитическую работу не только с целью предотвратить утрату собственной информации, но и с целью получения информации о конкурентах. Являясь ядром такого понятия, как «разведка в бизнесе», аналитическая обработка информации позволяет

получать по различным оценкам от 80 до 90 % необходимой информации при использовании только открытых источников.

Руководитель каждой фирмы имеет собственный взгляд на построение, направления работы и структуру информационно-аналитической службы (ИАС). На основе многолетнего опыта работы в этой области как отечественных, так и зарубежных специалистов сформировалось мнение, что в силу определенных причин наиболее эффективно такие службы функционируют как ядро службы безопасности.

В первую очередь это объясняется тем, что основным потребителем аналитически обработанных данных является сама служба безопасности как подразделение, наиболее нуждающееся в аналитически обработанных данных, работающее на опережение и прогнозирование событий. Кроме того, в ходе аналитической работы очень часто используются (или могут быть получены) конфиденциальные сведения, что также подтверждает рациональность размещения ИАС в службе безопасности. Даже не являющиеся конфиденциальными аналитически обработанные данные представляют собой наиболее ценные информационные ресурсы фирмы.

В настоящее время ИАС фирмы рассматривается как основной поставщик аналитически обработанной информации для нужд всех подразделений фирмы.

Основной задачей ИАС становится информационно-аналитическое обеспечение принятия решений по вопросам прежде всего основной деятельности. Таким образом, сотрудники фирмы или его подразделений могут заказать аналитический отчет по интересующему вопросу для принятия более рационального и взвешенного решения. В этой связи очень важной проблемой становится обеспечение информационной безопасности аналитически обработанных данных, представляющих собой ценный информационный ресурс фирмы наряду с другими конфиденциальными сведениями. Процесс заказа аналитического отчета должен быть четко регламентирован, чтобы только сотрудники определенного уровня имели право давать задания ИАС фирмы. Все заказы на аналитические исследования должны фиксироваться, причем темы исследований и авторы заказов на них должны тщательно регламентироваться. Доступ к аналитически обработанным данным должен быть строго ограничен.

Защита информации внутри ИАС представляет собой крайне сложную задачу, так как специфика аналитической работы в ряде случаев вступает в прямое противоречие с нормами защиты информации. Например, обеспечение такого важного принципа, как дробление информации в работе реальных ИАС, в большинстве случаев практически невозможно, так как это тормозит работу всей системы ИАС, где сотрудники должны иметь представление обо всей картине событий. Сокрытие какой-либо информации от сотрудников ИАС может привести их к ложным выводам, а фирму – к принятию неверных решений, а следовательно, и к убыткам. ИАС, являясь ядром службы безопасности фирмы, не имеет и не должна иметь властных функций. Такое положение исключает намеренное искажение обрабатываемой информации и позволяет работать «на стыках» по пограничным вопросам.

Функции ИАС:

• обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;

• описать сценарии действий конкурентов, которые могут затрагивать текущие интересы фирмы;

• осуществлять постоянный мониторинг событий во внешней конкурентной среде и на рынке, которые могут иметь значение для интересов фирмы;

• обеспечить безопасность собственных информационных ресурсов;

• обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

ИАС все в большей степени становится важным и функционально емким подразделением любой фирмы и, как правило, входит в состав службы безопасности. В последнее время специалисты все чаще сходятся во мнении, что в ИАС должна быть сосредоточена вся работа по прогнози-

рованию ситуаций, а также формированию соответствующих информационных комплексов, необходимых для эффективного и взвешенного принятия решений.

Направления аналитической работы определяются каждой фирмой самостоятельно и отражают области ее интересов. К основным направлениям аналитической работы, разрабатываемым на многих фирмах, можно отнести: анализ объекта защиты, анализ угроз, анализ каналов несанкционированного доступа к информации, анализ комплексной безопасности фирмы, анализ нарушений режима конфиденциальности, анализ подозрений утраты конфиденциальной информации и т. д.

Можно выделить моменты, общие для всех ИАС. Направления аналитической работы, ведущейся ИАС фирмы, могут быть постоянными, периодическими и разовыми.

Постоянные направления аналитической работы являются наиболее важными. Периодические и разовые направления аналитической работы характеризуются своей жесткой зависимостью от постоянных направлений. Промежутки времени, через которые проводятся исследования в области периодических направлений аналитической работы, всецело зависят от результатов анализа по постоянным направлениям.

Разовые направления аналитической работы не только жестко зависят от постоянной аналитической работы, но и в подавляющем большинстве случаев являются следствием результатов таких исследований.

В концептуальном отношении ИАС должна представлять собой единую систему анализа, контроля и прогнозирования внешней и внутренней ситуации. Все направления аналитической работы должны быть связаны определенной логикой взаимодействия.

Результаты исследований в одном направлении должны влиять на ход других исследований таким образом, чтобы результаты постоянных направлений аналитической работы инициировали проведение периодических и разовых исследований, а результаты последних не выпали из внимания специалистов по постоянным направлениям.

Следовательно, ИАС должна быть единой и взаимосвязанной структурой обеспечения фирм достоверной и аналитически обработанной информацией, направленной на информационную поддержку принятия эффективных решений по всем направлениям безопасности бизнеса.

Каждая фирма ведет индивидуальные направления аналитической работы и самостоятельно решает, следует ли разрабатывать их постоянно, периодически или только по мере надобности. Более того, каждая фирма имеет свои специфические области интересов, в рамках которых проводит аналитические исследования. Направления аналитической работы могут быть различными, но логика взаимодействия и система связей между направлениями исследований должны сохраняться.

Принципиально важными представляются ключевые направления, работа по которым ведется постоянно. Как указывалось выше, наиболее сложными для обнаружения являются организационные каналы несанкционированного доступа к защищаемой информации фирмы, связанные с так называемым человеческим фактором.

Например, трудно обнаружить инициативное сотрудничество злоумышленника с сотрудником фирмы – секретарем-референтом, экспертом, оператором ЭВМ и др. В основе поиска и обнаружения таких каналов лежит постоянная аналитическая работа, которая должна носить превентивный характер и использовать в качестве инструмента учетный аппарат, предназначенный для фиксирования (протоколирования) необходимых для анализа сведений. В данном случае аналитическая работа представляет собой комплексное исследование различной целевой направленности в целях выявления, структуризации и изучения опасных объективных и субъективных, потенциальных и реальных ситуаций, которые могут создать риск для экономической и информационной безопасности фирмы, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа фирмы или ее продукции.

Результаты аналитической работы показывают степень безопасности интеллектуальной собственности, условий функционирования фирмы и являются основой для построения и совершенствования системы защиты традиционных и электронных информационных ресурсов, формирова-

ния рубежей охраны территории, здания, помещений, оборудования, продукции и персонала фирмы. Аналитическое исследование позволяет выработать способы пассивного и активного противодействия злоумышленнику в организационных и технических каналах, разработать и систематически совершенствовать систему защиты информации, определять ее структуру и стоимость в соответствии с реальными опасностями, Угрожающими ценным информационным ресурсам фирмы.

Обнаружение действующего или предполагаемого канала несанкционированного доступа к информации, а также предотвращение его появления возможны только при наличии постоянного контроля и анализа объекта защиты, уровня безопасности информационных ресурсов в источнике и канале распространения информации. Уязвимым является любой элемент информационных ресурсов и информационных систем. Другие пути носят случайный характер ожидания ошибки в тайных действиях злоумышленника.

Обнаружение канала или каналов несанкционированного доступа к ценной информации фирмы входит в число постоянных направлений аналитической работы и в общем виде включает в себя:

• анализ источников конфиденциальной информации;

• анализ каналов объективного распространения информации; • аналитическую работу с источником угрозы информации. Аналитическое исследование источников конфиденциальной информации предусматривает:

• выявление и классификацию существующих и возможных конкурентов и соперников фирмы, криминальных структур и отдельных преступных элементов, интересующихся фирмой;

• выявление и классификацию максимально возможного числа источников конфиденциальной информации фирмы;

• выявление, классификацию и ведение перечня (учетного аппарата) реального состава циркулирующей в фирме конфиденциальной информации (в разрезе источников, обеспечиваемых функций и видов работы, с указанием носителей – документов, дискет, файлов и т. д.);

• изучение данных учета осведомленности сотрудников в тайне фирмы в разрезе каждого руководителя и сотрудника (в том числе технического и вспомогательного), т. е. изучение степени и динамики реального владения (в том числе случайного) сотрудниками конфиденциальной информацией;

• изучение состава конфиденциальной информации в разрезе документов, т. е. изучение правильности расчленения тайны (конфиденциальной информации) между документами и определение избыточности ценной информации в документах;

• учет и изучение выявленных внутренних и внешних, потенциальных и реальных (пассивных и активных) угроз каждому отдельному источнику информации, контроль процесса формирования канала несанкционированного доступа к информации;

• ведение и анализ полноты перечня защитных мер, предпринятых по каждому источнику, и защитных мер, которые могут быть использованы при активных действиях злоумышленника, заблаговременное противодействие злоумышленнику.

Обязательному учету подлежат все санкционированные и несанкционированные обращения сотрудников фирмы к конфиденциальной информации, документам, делам и базам данных.

По отношению к каналам объективного (естественного) распространения защищаемой информации (управленческие и производственные действия, функциональные связи персонала, информационные сети, технические каналы излучения информации и т. п.) применяются следующие аналитические действия и меры превентивного контроля:

• выявление и классификация реального максимального состава каналов объективного распространения конфиденциальной информации в фирме;

• изучение составных элементов каждого канала с целью нахождения опасных участков, способствующих возникновению канала несанкционированного доступа к информации;

• исследование и обобщение способов и сферы распространения информации в каждом канале;

• изучение (учет) состава конфиденциальной информации, циркулирующей в каждом канале;

• изучение (учет) состава конфиденциальной информации, циркулирующей между источниками;

• изучение сферы распространения информации при коммуникативных связях фирмы (по конкурентам, средствам массовой информации, выставкам и ярмаркам, рекламным изданиям и т. п.);

• контроль и перекрытие каналов несанкционированного ознакомления с информацией ограниченного доступа для третьих лиц, случайных, посторонних людей;

• исследование состава и эффективности методов защиты, предпринятых по каждому каналу, и дополнительных мер противодействия злоумышленнику при активных угрозах, экстремальных ситуациях.

Анализ угроз является одним из самых важных разделов аналитической работы и представляет собой ответ на вопрос, от чего или кого следует защищать определенные ранее объекты защиты. Источники угрозы конфиденциальной информации – объективные и субъективные события, явления, факторы, действия и обстоятельства, содержащие опасность для ценной информации.

К объективным источникам можно отнести: экстремальные ситуации, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают: злоумышленников Различного рода, посторонних лиц, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы и др. Источники угрозы могут быть внешними и внутренними. Внешние источники находятся вне фирмы и представлены чрезвычайными событиями, а также организационными структурами и физическими лицами, проявляющими определенный интерес к фирме. Внутренние источники угрозы связаны с фатальными событиями в здании фирмы, а также с персоналом. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях.

Аналитическая работа с источником угрозы конфиденциальной информации предусматривает:

• выявление и классификацию максимального состава источников угрозы конфиденциальной информации;

• учет и изучение каждого отдельного субъективного внутреннего и внешнего источника, степени его опасности (анализ риска) при реализации угрозы;

• разработку превентивных мероприятий по локализации и ликвидации объективных угроз.

В области внешних источников угрозы аналитическая работа связана с маркетинговыми исследованиями, которые регулярно ведет любая фирма. Анализ внутренних источников угрозы имеет целью выявление и изучение недобросовестных интересов и злоумышленных устремлений отдельных сотрудников фирмы и партнеров. В процессе анализа источников выявляются факты получения злоумышленником секретов фирмы, факты сотрудничества персонала фирмы с конкурентами или наличия в составе сотрудников фирмы злоумышленника.

Контрольная и аналитическая работа проводится при потенциальных и пассивных угрозах источникам и каналом распространения информации. При активной угрозе одновременно осуществляется заранее спланированное, продуманное и решительное противодействие злоумышленнику. При несколько упрощенной схеме целью проведения анализа угроз можно считать выявление фигуры противника и его планов по дестабилизирующему воздействию на фирму. В ряде случаев более эффективно проводить анализ не от выявления и рассмотрения всех объектов защиты и каналов распространения информации, а от выявления лица (лиц), которое заинтересовано в реализации каких-либо угроз как конфиденциальной информации, сотрудникам, так и фирме в целом, т. е. от выявления злоумышленника.

Этот метод позволяет не только более четко спрогнозировать дальнейшие действия этого лица, но и оценить границы его действий и материальные возможности. Сначала нужно выяснить, кто является злоумышленником и что ему нужно, затем, исходя из имеющихся у него средств и возможностей, будет гораздо легче спрогнозировать, как именно он попытается достигнуть своей

цели. Однако не следует забывать и о том, что достаточно серьезную угрозу могут представлять и субъекты (объекты), не заинтересованные в нанесении ущерба фирме.

Следовательно, наличие, ведение и результаты постоянной аналитической работы определяют необходимость, структуру и содержание системы защиты информации, степень ее требуемой эффективности и направления совершенствования. При отсутствии в фирме серьезной аналитической работы становится практически невозможным выявление и контроль каналов несанкционированного доступа к ценной, конфиденциальной информации фирмы.

Сотрудники ИАС фирмы должны учитывать все каналы несанкционированного доступа к конфиденциальной информации, выявлять, определять наиболее вероятные из них и контролировать их. С этой целью сотрудники ИАС должны принимать непосредственное участие в мероприятиях, в ходе которых имеется вероятность возникновения указанных каналов доступа к конфиденциальной информации фирмы. Так, целесообразным является предварительная оценка аналитиками подготовленных к публикации материалов о фирме, выставочных проспектов, рекламных изданий и т. п., их участие в презентациях, выставках, собраниях акционеров, переговорах, а также собеседованиях и тестированиях кандидатов на должности. Последнее является одной из основных и наиболее важных обязанностей ИАС, так как именно на этом этапе можно с определенной долей вероятности перекрыть один из основных организационных каналов – поступление злоумышленника на работу в фирму. В состав ИАС должны входить профессиональные психологи – специалисты по проведению опросов и тестов среди персонала.

Аналитически обработанные сведения вносятся в электронную базу данных. Аналитические отчеты по каждому направлению представляются с определенной периодичностью. В любой момент времени по требованию руководства ИАС должна быть в состоянии представить сводный обзор по всем направлениям. При выявлении каких-либо подозрений, угроз, пробелов в защите и т. п. сразу же ставятся в известность руководители, а аналитический отчет готовится в кратчайшие сроки.

Не менее важными являются и так называемые периодические направления аналитической работы, которые проводятся через определенные промежутки времени с целью контроля эффективности и возможности внесения улучшений в действующую в фирме систему защиты информации. К такому виду направлений аналитической работы прежде всего относится анализ степени безопасности фирмы. Очевидно, что постоянная и каждодневная аналитическая работа по данному направлению не имеет смысла. Вполне достаточно проводить анализ через определенные, специально установленные промежутки времени. Это направление аналитической работы находится в прямой зависимости от анализа состава угроз – постоянного направления аналитической работы. Именно результаты аналитической работы по выявлению угроз позволяют установить рациональную периодичность анализа эффективности структуры действующей системы безопасности фирмы. Так, при появлении дополнительных угроз, аналитическую работу (и следовательно, проверки, контрольные мероприятия и т. п.) следует проводить более часто.

Необходимо также периодически проводить анализ нарушении режима конфиденциальности, причем это направление относится также и к разовым направлениям. Рассматриваемые в рамках периодического направления аналитической работы нарушения режима безопасности за определенный период времени анализируются с целью выявления вызвавших их причин и выработки мер для их устранения. Частота проведения исследований такого рода также напрямую зависит от результатов исследований по другим направлениям.

Разовые направления аналитических исследований также являются очень важными в силу того факта, что чаще всего бывают вызваны чрезвычайными обстоятельствами, происшествиями, неожиданно появившимися проблемами и т. п., требуют проведения исследований в кратчайшие сроки. Типичным примером разового направления аналитической работы является проверка подозрения утраты конфиденциальной информации фирмы и злоумышленных действий, а также анализ нарушения режима конфиденциальности в фирме. Последнее направление включается также и в подсистему периодических направлений. Тем не менее факт каждого нарушения режима конфиденциальности должен сразу же расследоваться и анализироваться.

Все направления аналитической работы независимо от их типа, в том числе имеющие разовый характер, должны быть связаны в единую систему, позволяющую эффективно принимать решения, предотвращать угрозы и прогнозировать развитие событий – работать на опережение.

Этапы аналитической работы

Этап 1. Общее знакомство с проблемой: Ознакомление с проблемой в целом, а также со смежными вопросами, изучение которых может оказаться полезным. Составление общего плана работы с указанием срока выполнения, исполнителей и основных источников данных и информации, которые предположительно могут быть использованы.

Этап 2. Определение используемых терминов и понятий. Необходимо определить и объяснить тот или иной термин или понятие так, чтобы это было ясно нам самим, тем, кто контролирует нашу работу, и тем, кто пользуется нашей информацией. «Определение понятий» является одним из базовых принципов.

Этап 3. Сбор фактов: Умение находить и выбрать достоверные источники валидной информации. Главными носителями перспективных материалов всегда являются:

— знающие люди;

— документы;

— средства беспроводной и проводной связи (телефоны, телефаксы, радиостанции...);

— электронные системы обработки информации (компьютеры, электрические пишущие машинки...);

— разные отслеживаемые факторы (поведение, разговоры, результаты действий).

Выйдя на тот или иной источник информации, просчитайте:

— его наличные и потенциальные возможности,

— допустимые пределы использования,

— степень его надежности

Этап 4. Истолкование фактов. Так кратко можно назвать процесс изучения и обработки фактов с целью выжать из них все, что они значат. Этот этап включает оценку, классификацию, анализ и уяснение фактов.

Этап 5. Построение гипотезы Рабочие гипотезы, выдвигаемые на этом этапе, обычно связаны с какими-либо конкретными вопросами, отвечая на которые можно проверить сами гипотезы. Многие считают построение гипотезы важнейшим моментом любого исследования как в области естественных или общественных наук, так и в области информационно-аналитической работы. По мере изучения данного этапа мы открываем все новые полезные стороны рабочей гипотезы.

Этап 6. Выводы. На этом этапе производятся исследования, необходимые для доказательства или опровержения рабочих гипотез, выдвинутых на этапе 5, и формулируются окончательные выводы, являющиеся душой почти любого информационного документа. («Выводы» — последний из девяти принципов информационной работы).

Этап 7. Изложение. Составление документа, завершающее работу. Составитель информационного документа должен не только ясно представлять себе то, о чем он пишет, но и уметь выразить свои мысли в ясной форме.

Ведение аналитической работы возможно только при наличии необходимой информации, поэтому в первую очередь нужно определить, какая именно информация будет необходима аналитикам для работы, где можно ее получить и какой из источников можно при этом использовать. Как правило, получение информации не относится специалистами непосредственно к аналитической работе, тем не менее, определение круга исходной информации, а также мест и способов ее получения должно решаться непосредственно сотрудниками ИАС.

Интерпретация информации является первым этапом предварительного анализа. Под интерпретацией подразумевается выявление истинного значения той или иной информации. В первую очередь это относится к вербальной информации, так как очень часто то или иное высказывание бывает понято превратно. Это происходит, когда фраза вырвана из контекста либо неправильно понята иностранная речь, интонация, жесты, сленг и т. п. При возникновении такой ситуации в

помощь аналитикам целесообразно пригласить знающего специалиста, который сможет правильно интерпретировать то или иное сообщение.

В интерпретации нуждаются не только слова, но и действия. Зачастую факт, внешне подозрительный, на самом деле может иметь абсолютно положительный характер, а многие по сути угрожающие факты могут иногда выглядеть как неопасные.

Язык, используемый для описания информации, может допускать неоднозначность ее понимания. Это создает определенные трудности при интерпретации вербальной информации, но в этом случае истинный смысл можно понять из контекста. Информация, которая хранится в персональных компьютерах, как правило, лишена контекста, поэтому ошибочная интерпретация становится гораздо более вероятной. Западные специалисты определяют цену информации через те действия, которые могут быть предприняты в результате знания этой информации.

Вся информация подразделяется на факты, личные мнения и аналитически обработанные данные. Смешивание или неправильное определение этих различных по своей сути видов информации может приводить к ошибкам в интерпретации и, как следствие, к принятию неправильных решений. Следовательно, процесс интерпретации требует максимальной осторожности и тщательности. В каждом конкретном случае необходимо выявить истинный смысл поступившей информации. Здесь аналитики сталкиваются с такой проблемой, как выделение не относящейся к делу информации.

Выделение посторонней информации составляет следующий этап предварительного анализа. Этот процесс является одним из самых сложных и ответственных моментов во всей процедуре. Избыток ""формации, так же как и ее недостаток, представляет собой серьезную проблему и затрудняет проведение аналитической работы. Тактика выделения нескольких ключевых деталей гораздо более эффективна, чем разбрасывание между многими разрозненными данными. Вместе с тем именно на этом этапе существует опасность отбросить важную информацию. Как правило, это может произойти в случае неправильной интерпретации сведений на предыдущем этапе. Кроме того, аналитики могут стремиться сохранить не относящуюся напрямую к делу информацию в надежде, что она может пригодиться в будущем. Такая информация должна заноситься в банк данных ИАС таким образом, чтобы впоследствии ее можно было легко найти. С созданием такого информационного фонда и его постоянным пополнением задача поиска и сбора исходной информации для анализа будет значительно облегчена. Тем не менее избыток информации представляет собой серьезную проблему, так как значительно замедляет ведение аналитической работы, старение же и обесценивание информации может происходить очень быстро. Кроме того, избыток не относящейся к делу информации является для руководителя ИАС сигналом того, что поиск и сбор информации организованы неэффективно.

Оценка информации составляет следующий этап. Под оценкой понимается метод ранжирования источников информации, самой информации и способов ее получения. Как правило, пользуются системой оценок информации, при которой аналитик может выразить свою точку зрения относительно надежности и достоверности полученных сведений, хотя очевидным недостатком данной системы будет определенная субъективность оценок. Например:

Оценка источника:

• надежный источник;
• обычно надежный источник;
• довольно надежный источник;
• не всегда надежный источник;
• ненадежный источник;
• источник неустановленной надежности. Оценка информации:
• подтвержденная другими фактами;
• вероятно правдивая (75 %);
• возможно правдивая (50 %);
• сомнительная (25 %);
• неправдоподобная;

• достоверность не поддается определению.

Оценка способа получения информации источником:

• получил информацию сам (сам видел, слышал и т. п.);

• получил информацию через постоянный источник (через информатора, открытые источники и т. п.);

• получил информацию через разовый источник (случайно подслушанный разговор, слухи и т. п.).

На этапе оценки необходимо установить, насколько информация может соответствовать истине. При этом нужно учитывать, что можно получить не соответствующую истине информацию следующих типов:

• дезинформацию, доведенную до сведения источника;

• преднамеренно или непреднамеренно искаженную источником;

• произвольно или непроизвольно измененную в ходе передачи. При намеренной дезинформации применяется заведомая ложь, полуправда, а также правдивые сведения, которые в данном контексте подтолкнут воспринимающих информацию лиц к ложным выводам.

Искажения, возникающие в процессе передачи исходных данных, могут происходить по многим причинам:

• передача только части сообщения;

• пересказ услышанного своими словами;

• факты, искаженные чьим-либо субъективным восприятием.

Для своевременного выявления искаженной информации, а также для успешной борьбы с вероятной дезинформацией необходимо различать факты и мнения, учитывать субъективные характеристики источника и его предполагаемое отношение к выдаваемому сообщению. Следует четко осознавать, способен ли источник по своему положению иметь доступ к сообщаемым фактам. В качестве страховочных мер всегда нужно иметь дублирующие источники, использовать дублирующие каналы связи и стараться исключать все лишние промежуточные звенья передачи информации. Кроме того, необходимо помнить, что особенно легко воспринимается та дезинформация, которая хорошо соответствует принятой ранее версии, т. е. та, которую предполагают или желают получить.

Следующим этапом является построение предварительных версии, объясняющих место основных полученных фактов в цепи событий. Первым шагом является составление списка сведений, приготовленных для анализа. Это необходимо для дальнейшего ранжирования их по степени важности, кроме того, это является некой гарантией того, что сведения не выпадут из поля зрения и о них не забудут. Далее необходимо выделить ключевые моменты, отделить их от менее важных, не играющих главной роли в данной ситуации. Полученные сведения должны быть четко классифицированы по степени достоверности источника, самих сведений и способа их получения. Самые свежие и полные сведения должны рассматриваться в первую очередь. В перечне сведений, приготовленных для анализа, наиболее важные сведения специально помечаются. Материалы с пометками «источник неустановленной надежности» и «достоверность не поддается определению» откладываются и не участвуют в анализе без крайней необходимости.

Затем необходимо выявить все возможные гипотезы, которые могут объяснять ключевые события, и, расположив их по степени вероятности, поочередно проверять на стыкуемость со всеми данными. Если обнаружено значительное расхождение какой-либо предварительной гипотезы с полученными сведениями, причем последние имеют достаточно высокие оценки достоверности, то следует переходить к следующей гипотезе. Таким образом, выбираются наиболее вероятные предположения. На этом этапе возникает одна из самых серьезных проблем аналитической работы – противоречия в сведениях. Для ее преодоления необходимо сравнить оценки информации и источника, даты получения спорных сведений. Решающее же значение имеет интуиция, знания и опыт самого сотрудника, проводящего анализ. Конфликты в информации должны быть устранены в процессе анализа, для их разрешения собирается дополнительная информация, что соответствует следующему этапу аналитической работы. Если решение, которое будет принято на основе анали-

тически обработанной информации, является очень важным и нет возможности получить дополнительную информацию для устранения противоречий, то окончательный выбор возлагается на лиц, ответственных за принятие решения. Тем не менее общая доля таких ситуаций должна сводиться к минимуму, так как это свидетельствует о неудовлетворительной работе ИАС.

Следующим этапом является определение потребности в дополнительной уточняющей информации, а также выяснение, какая именно информация необходима и почему. На этом этапе выявляются пробелы в информации. Часть пробелов может быть быстро установлена, так как является результатом недостаточного исследования, другая же часть пробелов в информации может и не быть обнаружена аналитиком, потому что упущена на этапе сбора самих сведений. Очевидно, что второй вид пробелов в информации является гораздо более опасным.

Необходимо четко различать понятия «неполная информация» и «пробел в информации». Неполная информация означает отсутствие не имеющих особой важности сведений, что является естественным, так как никогда нельзя получить абсолютно все сведения. Более того, такая информация была бы избыточной и осложнила бы анализ. Пробел же в информации подразумевает отсутствие сведений, являющихся ключевыми в данной ситуации или необходимыми для устранения противоречий. Такие сведения крайне важны для проведения анализа.

Выявив пробелы в информации, нужно определить их важность для дальнейшего анализа. Нельзя до бесконечности откладывать составление аналитического отчета под предлогом того, что в информации выявлены пробелы. На определенном этапе следует признать, что для решения задачи собрано достаточно данных. Кроме того, имеют значение факторы времени и денег, потому что решение проблемы ограничено тем и другим. Сотрудники ИАС должны стремиться к решению поставленной задачи имеющимися средствами и в разумные сроки.

На основе выполнения предыдущих этапов приступают к подготовке аналитических отчетов по определенному вопросу, выработке конкретных выводов и предложений. Подготовка отчетов является основной обязанностью аналитика, а готовый отчет представляет собой результат функционирования системы аналитической работы. Отчеты могут быть представлены в различных формах. Наиболее часто отчет составляется в письменном виде, но он также может быть устным, иллюстрируемым графиками, таблицами, диаграммами и т. п. Если сроки жестко ограничены, отчет излагается устно, в форме вопросов и ответов.

В зарубежной литературе выделяют три основных вида аналитических отчетов.

Первый вид называют тактическим (оперативным) отчетом. К этому типу относятся экстренные отчеты по какому-либо вопросу небольшого объема, которые необходимы для срочного принятия решения. При этом аналитика редко знакомят с причиной или целью данного задания. Такие отчеты составляются по разовым направлениям аналитической работы.

Второй вид составляют стратегические отчеты. Они содержат более полную информацию и менее ограничены сроками. В них включается подробная предыстория данной проблемы и прогноз ее дальнейшего развития, причем для построения реалистичной гипотезы анализируется вся предшествующая информация по данной теме. Отчеты такого типа соответствуют постоянным направлениям аналитической работы.

Третий вид представлен периодическими отчетами, основной отличительной особенностью которых является то, что они готовятся по графику. Интервалы между сроками предоставления составляют дни, недели или месяцы. Как правило, такой вид отчетов готовится по проблемам, являющимся объектом постоянного пристального внимания со стороны ИАС фирмы. Этот вид может соответствовать как периодическим, так и постоянным направлениям аналитической работы.

Все письменные отчеты должны содержать глубокий анализ и быть представлены в регламентированной (типовой, унифицированной) форме. Потребителями аналитических отчетов являются ответственные за планирование и принятие решений лица, которые вправе предъявлять определенные требования к содержанию и оформлению отчетов. Аналитический отчет должен быть четко, логично и грамотно составлен. Кроме того, отчет должен абсолютно соответствовать месту сотрудника – потребителя информации в разрешительной системе доступа к конфиденциальной информации: по степени конфиденциальности используемых в отчете сведений, профилю

профессиональных знаний сотрудника и деловой необходимости информации для конкретной работы. Нужно учитывать также и то, что внешний вид отчета обязательно будет влиять на восприятие содержащейся в нем информации.

За рубежом используется, как правило, следующая форма изложения данных аналитического отчета:

1) Заключение. Здесь должны содержаться ответы на вопросы, какова степень важности полученной информации, ее значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторах и т. п., какое отношение имеет предмет отчета к другим областям аналитической работы. Факты и сведения, на основе которых получены результаты анализа, не должны смешиваться с самими результатами.

2) Рекомендации. Должны быть указаны конкретные направления дальнейших действий службы безопасности и других структурных подразделений предприятия для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений и т. п.

3) Обобщение информации. Изложение самой существенной информации без излишней детализации.

4) Источники и надежность информации. Должны быть указаны предполагаемые оценки надежности данных и источника на момент написания отчета, так как для принятия решений необходимо оценить надежность материалов, являющихся их базой.

5) Основные и альтернативные гипотезы. Обязательно должны указываться рассмотренные в ходе анализа наиболее вероятные гипотезы, что помогает принимать более взвешенные и адекватные решения, а также позволяет еще раз оценить правильность выбранной гипотезы.

6) Недостающая информация. Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения. Описанная структурная схема проведения аналитического исследования позволяет предоставить в распоряжение пользователя, принимающего решение, структурированный массив ценной информации, отражающей с определенной степенью достоверности сложившуюся ситуацию с обеспечением безопасности информационных ресурсов фирмы.

Методы аналитической работы

Основным назначением всех аналитических методов является обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации. Существует широкий спектр специальных методов анализа: графические, табличные, матричные и т. п., например, диаграммы связи и матрицы участников, схемы потоков данных, временные графики, графики анализа визуальных наблюдений VIA (visual investigative analysis) и графики оценки результатов PERT (program evaluation review technique). Тем не менее следует отметить, что у каждого аналитика есть свой собственный метод анализа, который может быть как комбинацией вышеперечисленных методов, так и сугубо индивидуальным, уникальным методом аналитической работы.

С помощью диаграмм связей выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов. На диаграмме связей отмечают как наиболее прочные, так и вспомогательные связи между субъектами. Анализируются все связи без исключения, так как в ходе развития событий и получения дополнительной информации вспомогательные связи могут выступить на первый план. Для большей наглядности следует также указывать на диаграмме связи должностей (для физических лиц) или род деятельности (для юридических лиц).

Обеспечение безопасности информации на наиболее уязвимых направлениях деятельности предприятия

В ходе повседневной деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну, и конфиденциальной информации, планируются и проводят-

ся служебные совещания, в ходе которых рассматриваются или обсуждаются вопросы, содержащие конфиденциальную информацию.

Это могут быть вопросы, отнесенные к государственной тайне, касающиеся проводимых предприятием научно-исследовательских, опытно-конструкторских и иных видов работ, предусмотренных уставом предприятия, или вопросы, носящие конфиденциальный характер, отражающие коммерческую сторону деятельности предприятия.

Вышеперечисленные мероприятия могут быть внутренними (к участию в них привлекается только персонал данного предприятия) или внешними (с участием представителей сторонних организаций-партнеров).

Решение на проведение совещания во всех случаях принимается непосредственно руководителем предприятия или его заместителем по ходатайству руководителя подразделения, в чьих интересах оно будет проведено.

Принимаемые должностными лицами предприятия (структурным подразделением, его организующим) меры по защите конфиденциальной информации в ходе подготовки и проведения совещания должны носить как организационный, так и технический характер.

Мероприятия по защите информации проводятся при подготовке, в ходе проведения и по окончании совещания.

Одним из важных элементов в работе руководства и должностных лиц предприятия по защите информации при проведении совещания является этап планирования конкретных организационно-технических мер, направленных на исключение утечки конфиденциальной информации и на ее защиту.

Планирование мероприятий по защите информации включает выработку конкретных мер, определение ответственных за их реализацию должностных лиц (структурных подразделений) предприятия и сроков их выполнения (проведения).

Планирование мероприятий по защите информации, проводимых в ходе совещания с участием представителей сторонних организаций, осуществляется под руководством руководителя предприятия и при непосредственном участии его заместителя, возглавляющего на предприятии работу по защите информации. При отсутствии в структуре предприятия данного должностного лица, непосредственная ответственность за проведение планирования мероприятий по защите информации возлагается на руководителя режимно-секретного подразделения (службы безопасности).

Проведение совещания без приглашения представителей сторонних организаций может проводиться без участия режимно-секретного подразделения (службы безопасности). В этих случаях ответственность за планирование и проведение мероприятий по исключению утечки конфиденциальной информации и по ее защите возлагаются на руководителя структурного подразделения предприятия, организующего данное совещание.

При планировании совещания предусматривается такая очередность рассмотрения вопросов, при которой будет исключено участие в их обсуждении лиц, не имеющих к ним прямого отношения.

Непосредственная разработка плана подготовки и проведения совещания возлагается на структурное подразделение предприятия, организующее его проведение.

Подготовка плана осуществляется заблаговременно до начала совещания и включает мероприятия, проводимые перед проведением совещания, во время проведения совещания и по его завершении.

В плане указываются время и место проведения совещания, состав участников, перечень предприятий, участвующих в совещании.

План мероприятий по защите информации при подготовке и в ходе проведения совещания содержит следующие основные разделы:

1. Определение состава участников и их оповещение. В разделе отражаются: порядок формирования списка лиц, привлекаемых к участию в совещании, а также перечня предприятий, которым необходимо направить запросы с приглашениями; порядок подготовки и направления таких запросов; формирование содержания запросов.

2. Подготовка служебных помещений, в которых планируется проведение совещания. В разделе отражаются:

работа по выбору служебных помещений;

проверка соответствия помещений требованиям по защите информации;

необходимость и целесообразность принятия дополнительных организационно-технических мер, направленных на исключение утечки информации;

оборудование рабочих мест участников совещания, в том числе средствами автоматизации, на которых разрешена обработка конфиденциальной информации.

Определяется порядок использования средств звукоусиления, кино- и видеоаппаратуры (проекторов).

3. Определение объема обсуждаемой информации. В данном разделе отражаются: порядок определения перечня вопросов, выносимых на совещание, и очередности их рассмотрения; порядок оценки степени конфиденциальности вопросов; выделение вопросов, к которым допускается узкий круг лиц, участвующих в совещании.

4. Организация пропускного режима на территорию и в служебные помещения, в которых проводится совещание. В разделе отражаются вопросы организации и осуществления пропускного режима:

виды пропусков и проставляемых на них условных знаком (шифров) для прохода в конкретные служебные помещения; порядок учета, хранения, выдачи и выведения их из действия (сроки уничтожения);

режим прохода, посещения и пребывания в помещениях участников совещания.

Определяются количество и регламент работы основных и дополнительных контрольно-пропускных пунктов для прохода участников совещания на территорию и в служебные помещения.

5. Организация допуска участников совещания к рассматриваемым вопросам. Раздел содержит мероприятия, касающиеся непосредственного допуска участников к вопросам, выносимым на совещание, с учетом порядка их обсуждения и степени конфиденциальности информации, к которой допущен каждый участник совещания.

6. Осуществление записи (стенограммы), фото-, кино-, видеосъемки совещания. В разделе определяются порядок и возможные способы записи, съемки (стенографирования) хода совещания и обсуждаемых вопросов с учетом их конфиденциальности, а также должностные лица (подразделения), отвечающие за техническое обеспечение данного процесса.

7. Меры по защите информации непосредственно при проведении совещания. В разделе отражаются: порядок и способы охраны служебных помещений, меры по исключению прохода (проникновения) в них посторонних лиц, а также участников совещания, не участвующих в рассмотрении конкретных вопросов; мероприятия по предотвращению утечки информации по техническим каналам, силы и средства, задействованные при их проведении. Также определяются конкретные меры, исключающие визуальный просмотр и прослушивание ведущихся переговоров и обсуждения вопросов участниками совещания.

8. Организация учета, хранения, выдачи и рассылки материалов совещания. В разделе отражаются порядок учета, хранения, размножения (печатания, ксерокопирования), выдачи, рассылки и уничтожения материалов совещания, а также рабочих тетрадей (блокнотов), предназначенных для записи обсуждаемых вопросов участниками совещания. Определяется порядок обращения с данными носителями информации непосредственно в ходе совещания и после его окончания. Особое внимание уделяется порядку учета, хранения, размножения и использования материалов совещания, зафиксированных на магнитных носителях (исполненных в электронном виде).

9. Оформление документов лиц, принимавших участие в совещании. В данном разделе отражается порядок и сроки оформления документов, подтверждающих право доступа участников совещания к конфиденциальной информации, предписаний (доверенностей) на участие в совещании, командировочных удостоверений;

10. Проверка и обследование места проведения совещания после его окончания. Раздел содержит мероприятия по организации и проведению визуальной проверки, а также проверки с использованием специальных технических средств (аппаратуры) помещений, в которых проводилось совещание с целью выявления оставленных (забытых) технических устройств, носителей конфиденциальной информации и личных вещей участников совещания.

11. Организация контроля выполнения требований по защите информации. В разделе отражается порядок, способы и методы контроля полноты и качества проводимых мероприятий, направленных на предотвращение утечки сведений конфиденциального характера, разглашения информации, содержащей такие сведения, и утрат (хищений) носителей информации. Указываются структурные подразделения (должностные лица), на которые возлагаются вопросы контроля.

Определяется система и порядок представления ответственными должностными лицами докладов о наличии носителей конфиденциальной информации и выявленных нарушениях в работе по защите конфиденциальной информации.

Для каждого включаемого в план мероприятия определяются: срок (время) его проведения и ответственное за выполнение мероприятия должностное лицо (подразделение).

При использовании в ходе совещания сведений конфиденциального характера или обсуждении вопросов, содержащих такие сведения, руководство предприятия-организатора, осуществляет комплекс мероприятий, направленных на исключение ознакомления с ней посторонних лиц и сотрудников фирм-конкурентов.

На совещание приглашаются работники, имеющие непосредственное отношением к рассматриваемым (обсуждаемым) вопросам.

При обсуждении в ходе совещания вопросов, содержащих сведения, составляющие государственную тайну, его участники должны иметь допуск к этим сведениям по соответствующей форме, а при рассмотрении вопросов, отнесенных к иным видам конфиденциальной информации, в установленном порядке оформленное решение руководителя предприятия на допуск к данной категории (виду) информации.

При последовательном рассмотрении вопросов, имеющих различную степень конфиденциальности, к участию в совещании по каждому из рассматриваемых вопросов допускаются лица, имеющие к ним непосредственное отношение.

Непосредственно перед началом совещания руководитель предприятия или должностное лицо, ответственное за его проведение, обязан проинформировать участников совещания о степени конфиденциальности обсуждаемых вопросов.

В ходе совещания, в том числе и во время перерывов, работник, ответственный за его проведение, совместно со службой безопасности (режимно-секретным подразделением) осуществляет необходимые организационно-технические мероприятия, направленные на исключение утечки сведений конфиденциального характера.

Во время перерывов в совещании, а также после завершения обсуждения одного вопроса и перехода к обсуждению следующего, сотрудники службы безопасности (службы охраны) организуют контроль прохода (нахождения) в служебные помещения, в которых проводится совещание, лиц в соответствии с утвержденным списком участников.

На все время проведения совещания запрещается пронос в служебные помещения, в которых оно проводится, индивидуальных видео- и звукозаписывающих устройств, а также средств связи (в том числе мобильных телефонов и приемников персонального вызова). В целях обеспечения их сохранности организуется камера хранения личных вещей участников совещания.

Звуко- и видеозапись, а также кино- и видеосъемка хода совещания и обсуждения вопросов совещания проводится с разрешения руководителя предприятия-организатора совещания только на учтенных в режимно-секретном подразделении (службе безопасности) носителях. При этом использование в этих целях соответствующей аппаратуры и технических устройств осуществляется при соблюдении требований по защите информации.

Носители конфиденциальной информации, а также сведений, составляющих государственную тайну, выдаются режимно-секретным подразделением (службой безопасности) участникам

совещания под роспись, а после окончания совещания возвращаются. Контроль за своевременным возвратом этих носителей осуществляется сотрудниками вышеуказанных подразделений.

Для осуществления записей хода совещания и обсуждаемых вопросов участникам совещания установленным порядком выдаются рабочие тетради или рабочие блокноты, учтенные в службе безопасности (режимно-секретном подразделении) и имеющие соответствующий гриф секретности (степень конфиденциальности). Эти рабочие тетради (блокноты) по окончании совещания возвращаются в службу безопасности (режимно-секретное подразделение). При необходимости они могут быть секретной (конфиденциальной) почтой направлены для дальнейшего хранения и использования на предприятия, представители которых производили в них записи на совещании.

Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия

В настоящее время невозможно представить деятельность современного предприятия без его участия в издательской деятельности и рекламных акциях различного характера. Вместе с тем, для предприятий, осуществляющих работу с конфиденциальной информацией, такие его виды деятельности могут привести к распространению охраняемой информации о направлениях его деятельности и проводимых работах.

В связи с этим, в повседневной деятельности предприятия мероприятия по защите информации в процессе подготовки и реализации рекламных и издательских проектов занимают важное место.

Основными направлениями защиты конфиденциальной информации в ходе осуществления предприятием рекламной деятельности являются:

- подготовка и экспертиза предполагаемых к распространению рекламных материалов на предмет отсутствия в них информации с ограниченным доступом;
- анализ материалов, подготавливаемых рекламопроизводителем и рекламораспространителем к размещению в средствах рекламы;
- постоянный контроль порядка выхода и содержания рекламных материалов независимо от способа, формы и периодичности их распространения.

При принятии руководителем предприятия решения на рекламирование деятельности предприятия, а также производимых им товарах или услугах должностное лицо, назначенное ответственным за подготовку рекламных материалов и их передачу рекламопроизводителю и (или) рекламораспространителю организует работу, направленную на предотвращение распространения в рекламе конфиденциальной информации. Комплекс мероприятий по защите информации включает проведение экспертизы предполагаемых к распространению материалов комиссией предприятия, анализ возможных форм, способов распространения рекламных материалов и непосредственное взаимодействие по вопросам организации и распространения материалов с рекламопроизводителем и рекламораспространителем.

Одним из важных элементов в этой работе является оценка комиссией предприятия, состоящей из компетентных специалистов, содержания материалов на предмет возможности их распространения, в том числе и объема этих материалов. После получения положительного заключения экспертной комиссии предприятия осуществляется подготовка договорных материалов на передачу рекламных материалов рекламопроизводителю и (или) рекламораспространителю а также непосредственная передача материалов, предполагаемых к рекламному распространению.

В дальнейшем предприятие осуществляет постоянный контроль содержания рекламы при ее выходе в свет.

Организация подготовки материалов к открытому опубликованию

С целью исключения распространения в средствах массовой информации сведений конфиденциального характера на предприятии планируется и проводится работа по анализу содержания материалов, предполагаемых к открытому распространению в средствах массовой информации.

Цель данной работы - недопущение утечки информации о деятельности предприятия, содержащей сведения с конфиденциального характера, а также сведений, составляющих государственную тайну, или служебную информацию ограниченного распространения (служебную тай-

ну). Для достижения этой цели проводится комплекс организационных мероприятий. Планирование и осуществление данных мероприятий проводят: служба безопасности, структурное подразделение по защите государственной тайны или специально создаваемое в структуре предприятия подразделение (должностное лицо), на которое возлагаются вышеуказанные задачи.

Сотрудники предприятия, принимающие непосредственное участие в подготовке материалов к открытому опубликованию, должны знать и руководствоваться положениями статьи 5 Закона РФ "О государственной тайне", "Перечнем сведений, отнесенных к государственной тайне", другими нормативными актами, а также перечнем информации, составляющей коммерческую тайну предприятия.

Подготовка материалов к открытому опубликованию включает в себя их разработку авторами, предварительную проверку их содержания руководителями структурных подразделений предприятия, согласование возможности опубликования материалов со службой безопасности (подразделением по защите государственной тайны) предприятия.

Подготовленные к открытому опубликованию материалы не должны содержать сведений, составляющих государственную, коммерческую тайну, служебной информации ограниченного распространения (сведений, содержащих служебную тайну) и иной информации с ограниченным доступом, определенной нормативными правовыми актами.

Организация работы с персоналом предприятия

В соответствии со статьей 6 Федерального закона РФ "Об информации, информационных технологиях и защите информации" вопросы ограничения доступа к информации, определения порядка и условий такого доступа отнесены к компетенции обладателя информации.

Обладатель информации при осуществлении своих прав обязан ограничивать доступ к информации и принимать меры по ее защите, если такая обязанность установлена федеральными законами.

В настоящее время в нашем государстве законодательно урегулированы (определены) и подробно раскрыты вопросы допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную или коммерческую тайну. Порядок допуска лиц к иным видам информации с ограниченным доступом с учетом положений Федерального закона РФ "Об информации, информационных технологиях и защите информации" находится в компетенции соответствующих должностных лиц (обладателей такой информации).

Доступ граждан к сведениям (информации), в установленном порядке отнесенным к коммерческой тайне, осуществляется в соответствии со статьями 7 и 10 Федерального закона РФ "О коммерческой тайне".

С момента установления в отношении информации, составляющей коммерческую тайну, режима коммерческой тайны, полномочия по принятию решения о доступе к ней, переходят к обладателю информации.

Необходимо отметить, что определение порядка доступа лиц к коммерческой тайне и учет лиц, получивших такой допуск, являются одними из мер по охране конфиденциальности такой информации, принятие которых для обладателя информации в соответствии с Федеральным законом РФ "О коммерческой тайне" является обязательным.

Меры по охране конфиденциальности информации признаются разумно достаточными, если исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя.

Иные, не противоречащие законодательству России меры по ограничению порядка доступа к коммерческой тайне, могут быть дополнительно приняты ее обладателем.

Одним из вопросов государственного регулирования в сфере защиты государственной тайны является порядок допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную тайну. Эта область является наиболее значимой для решения задач по защите государственной тайны и, в связи с этим, будет в данном учебном пособии раскрыта подробнее.

Допуск и непосредственный доступ должностных лиц и граждан к сведениям, составляющим государственную тайну, и их носителям, осуществляется в соответствии с положениями Закона

РФ "О государственной тайне" на основании "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

Допуск граждан к государственной тайне осуществляется соответствующими руководителями органов государственной власти, предприятий и организаций.

Допуск граждан к государственной тайне осуществляется в добровольном порядке и предусматривает:

- принятие на себя допущенными к государственной тайне лицами обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- согласие на частичные временные ограничения их прав в соответствии с Законом РФ "О государственной тайне";
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных законодательством Российской Федерации;
- ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за их нарушение;
- принятие соответствующего решения руководителем предприятия о допуске оформляемого лица к государственной тайне.

Должностное лицо или гражданин, допущенные (ранее допускавшиеся) к государственной тайне, могут быть временно ограничены в следующих своих правах:

- в праве на выезд за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;
- в праве на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;
- в праве на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Ограничение гражданина в праве на выезд из Российской Федерации осуществляется в соответствии с Федеральным законом РФ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию".

В целях частичной компенсации ограничений в правах для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями и организациями организационных и (или) штатных мероприятий.

Для сотрудников подразделений по защите государственной тайны дополнительно к вышеперечисленным льготам устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности (приняты на работу) только после оформления в установленном порядке допуска по соответствующей форме.

Перечень должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну, в связи с возложением на них соответствующих должностных (функциональных) обязанностей, определяется номенклатурой должностей. Номенклатура должностей разрабатывается предприятием, согласовывается с соответствующим органом Федеральной службы безопасности РФ, и после этого согласования утверждается руководителем предприятия (его заместителем, возглавляющим работу по защите государственной тайны).

Изменения и дополнения в номенклатуру должностей вносятся в установленном порядке по мере необходимости. Полная переработка номенклатуры должностей осуществляется не реже од-

ного раза в 5 лет.

Порядок разработки, согласования, утверждения номенклатуры, а также внесения в нее изменений и дополнений определяются "Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

С целью подтверждения фактической работы (ознакомления) сотрудников предприятия со сведениями, составляющими государственную тайну, подразделение по защите государственной тайны ведет учет их осведомленности в этих сведениях.

Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну.

В соответствии со степенями секретности сведений, составляющих государственную тайну, и грифами секретности их носителей, установлены следующие формы допуска:

первая форма - для граждан, допускаемых к сведениям особой важности;

вторая форма - для граждан, допускаемых к совершенно секретным сведениям;

третья форма - для граждан, допускаемых к секретным сведениям.

Проверочные мероприятия, связанные с допуском граждан к государственной тайне, осуществляются соответствующими органами безопасности во взаимодействии с органами, осуществляющими в соответствии с законодательством оперативно-розыскную деятельность.

Уровень необходимого допуска личного состава определяется степенью секретности сведений (грифом секретности их носителей), с которыми они знакомятся (работают) в рамках исполнения должностных обязанностей. Уровень допуска для каждого должностного лица, работающего на предприятии, отражается в Номенклатуре должностей.

Доступ к сведениям, составляющим государственную тайну - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия или организации, а также на их структурные подразделения по защите государственной тайны.

Руководитель предприятия обязан осуществлять постоянный контроль за соответствием формы допуска граждан степени секретности сведений, к которым они фактически имеют доступ.

Он несет персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

Основанием для непосредственного доступа лица к сведениям, составляющим государственную тайну, и их носителям, является решение руководителя предприятия, оформляемое в карточке о допуске.

Персонал предприятия, допущенный в силу должностных (функциональных) обязанностей к сведениям конфиденциального характера, - основной субъект правоотношений в сфере защиты конфиденциальной информации. Одновременно он является и единственным ее "нематериальным носителем".

В решении проблемы комплексной защиты информации на предприятии все более значительное место занимает выбор эффективных способов и методов работы с персоналом предприятия. Персонал предприятия, являясь генератором новых идей, открытий и изобретений, ускоряющих научно-технический прогресс, направляет максимальные усилия на повышение благосостояния предприятия в целом и каждого его сотрудника в частности.

Вопросы охраны конфиденциальности информации, к которой допускается работник предприятия, закреплены в разделе III Трудового кодекса РФ.

В соответствии с его положениями в заключаемом работодателем с работником трудовом договоре могут предусматриваться условия о неразглашении работником охраняемой законом тайны (государственной, служебной, коммерческой и иной).

В работе с персоналом предприятия, допущенным к конфиденциальной информации, используются следующие методы:

- обучения;
- инструктажей;
- индивидуальной и воспитательной работы;
- проверки уровня знаний;
- контроля.

Содержание и структура правового обеспечения

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия этим угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского, административного, уголовного и информационного).

Предмет правового обеспечения информационной безопасности представляет собой совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз. Общественные отношения, относящиеся к данному предмету, имеют следующие основные признаки: - принадлежность к регулируемым правом информационным отношениям, т.е. общественным отношениям по поводу обладания необходимой информацией, передачи части имеющейся информации другим субъектам, а также сохранения в неизвестности оставшейся части информации; - принадлежность к объектам информационной безопасности, которые представляются важными руководству организаций или государственных органов для эффективного достижения целей их деятельности; - обусловленность проявлением угроз сохранности основных свойств объектов информационной безопасности организаций и государственных органов.

Совокупность норм и институтов права, регулирующих эти отношения, составляет содержание правового обеспечения информационной безопасности и может быть разделена по объектам безопасности на правовое обеспечение безопасности информации в форме сведений, правовое обеспечение безопасности информации в форме сообщений, правовое обеспечение безопасности информационной инфраструктуры и правовое обеспечение безопасности правового статуса субъекта информационной сферы. Правовое обеспечение безопасности информации в форме сведений образуется совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей.

Цель противодействия заключается в предупреждении проявления угроз безопасности этих объектов и минимизации последствий проявления угроз. Основная угроза сведениям, обладателем которых является субъект права, заключается в искажении этих сведений посредством навязывания ложной информации. В основу правового регулирования отношений в области противодействия навязыванию ложной информации положен принцип выделения социально опасных действий, связанных с передачей или распространением такой информации (клевета, обман и злоупотребление доверием, заведомо ложная реклама и т.п.), и их запрета под угрозой применения к виновным лицам административной или уголовной ответственности. Нормы права, регулирующие эти отношения, входят в состав отраслей административного или уголовного права.

Основная угроза свободе мысли заключается в применении средств нарушения независимости психической деятельности мозга человека, например, таких, как скрытые вставки, скрытая реклама. Скрытая вставка представляет собой изображение, сюжет, мелодию или текстовое сообщение, которые являются составной частью программ, фильмов или компьютерных программ, относящихся к специальным средствам массовой информации. Они воспринимаются человеком через подсознание и (или) оказывают вредное воздействие на его здоровье. В отличие от «скрытой вставки» дефиниция «скрытая реклама» в законодательстве определяется как реклама, которая

оказывает не осознаваемое потребителем воздействие, в том числе путем использования специальных видеовставок (двойной звукозаписи) и иными способами.

Основу правовой конструкции регулирования отношений в рассматриваемых областях составляют нормы конституционного права, гарантирующие каждому человеку осуществление права на свободу мысли, а также нормы, предусматривающие возможность использования для защиты этого права целой системы юридических институтов, включающей институты конституционного контроля, судебной защиты, административно-правовой защиты, государственного надзора, международного контроля и международной судебной защиты. Кроме того, в состав этой конструкции входят правовые нормы, закрепляющие конституционное право человека и гражданина на охрану здоровья и медицинскую помощь1, в частности на восстановление психического здоровья человека, а также нормы, регулирующие отношения в области оказания ему необходимой медицинской помощи.

Основная угроза субъективной значимости национальных культурных ценностей заключается в их девальвации вследствие пропаганды образцов массовой культуры, основанных на культе насилия, а также духовных и нравственных ценностей, противоречащих принятым в российском обществе3. Эта угроза проявляется в виде деятельности граждан или их объединений по распространению идей религиозного экстремизма и нетерпимости, этнического превосходства или унижения. Распространение таких идей при отсутствии контрпропаганды со стороны общества и государства приводит к размыванию в индивидуальном и общественном сознании значимости традиционных ценностей, формированию представлений об отсутствии социальной поддержки этих ценностей. Основу правового регулирования отношений в области противодействия этой угрозе составляет принцип закрепления в нормах права запрета на распространение и использование основных элементов культуры, основанной на идеях насилия, национальной и религиозной ненависти, оскорбляющих в связи с этим национальные культурные ценности российского народа, включая использование относящихся к ней символов, и юридической ответственности лиц и объединений граждан, нарушающих данный запрет.

Правовое обеспечение безопасности информации в форме сообщений определяется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы. Основная цель правового регулирования в этой области состоит в предупреждении, выявлении и пресечении проявлений угроз безопасности этих объектов и минимизации последствий таких проявлений. Основная угроза безопасности информации в форме сообщений заключается в их несанкционированной модификации, уничтожении или задержке. Эта угроза проявляется в форме соответствующих действий физических или юридических лиц.

В основу правового регулирования отношений в области противодействия данной угрозе положены следующие принципы:

- выделение социально опасных действий, направленных на нарушение безопасности сообщений (документов), передаваемых по каналам связи, данных, накапливаемых и обрабатываемых в информационных системах, в автоматизированных системах управления, и запрет этих действий под угрозой применения уголовной или административной ответственности;

- формирование механизмов установления, поддержания и снятия режимов общедоступной информации и информации органического доступа, в том числе режима тайны (коммерческой, государственной и иных охраняемых законом тайн);

- закрепление требований к информационным системам, техническим средствам передачи, обработка и хранение информации, контроль выполнения этих требований, а также установление в определенных случаях гражданской, административной и уголовной ответственности за нарушение этих требований;

- правовая охрана установленных режимов доступа к информации.

Правовое обеспечение безопасности информационной инфраструктуры образуется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации.

Основные угрозы безопасности информационной инфраструктуры представляют собой нарушения работоспособности и функционирования основных составляющих информационной инфраструктуры — информационных и телекоммуникационных систем, сетей связи, системы массовой информации и т.п.

Основной целью правового обеспечения безопасности информационной инфраструктуры является предупреждение, пресечение и минимизация последствий проявления этих угроз.

В основу правового регулирования отношений, связанных с обеспечением безопасности сети связи, средств автоматизации обработки информации и информационно-телекоммуникационных систем как средства взаимодействия между отдельными субъектами, положены принципы:

- установление правового режима радиочастотного спектра и государственный контроль его поддержания;

- закрепление требований к организации защиты объектов и сооружений связи и установление административной ответственности за их выполнение;

- лицензирование деятельности по предоставлению услуг связи и государственный контроль за соблюдением лицензионных условий;

- подтверждение соответствия средств связи и услуг установленным требованиям;

- запрет на распространение вредоносных программ и применение уголовной ответственности за его нарушения.

В основу правового регулирования отношений в области обеспечения безопасности функционирования средств массовой информации и информационно-телекоммуникационных систем как средства распространения массовой информации положены принципы:

- ограничение участия иностранных юридических лиц, лиц с двойным гражданством и лиц без гражданства в учреждении российских средств массовой информации;

- запрет на распространение продукции зарубежных средств массовой информации вместо продукции отечественных средств массовой информации в качестве одного из условий получения лицензии на вещание, распространение продукции средств массовой информации, возможность аннулирования лицензии на вещание в случае неоднократного нарушения лицензионных условий;

- запрет на осуществление гражданами, должностными лицами, предприятиями, учреждениями, организациями, государственными органами действий, направленных на воспрепятствование распространению продукции СМИ, и привлечение виновных лиц к установленной законом административной ответственности.

Правовое обеспечение безопасности правового статуса субъектов информационной сферы образуется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются: - права человека и гражданина на участие в информационных отношениях (на свободу поиска, получения, передачи, производства и распространения информации, на свободу мысли и слова, массовой информации; на неприкосновенность частной жизни, личную и семейную тайну, на защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и др.);

- обязанности граждан, возникающие в связи с участием в информационных отношениях (непротиводействие реализации конституционных прав и свобод в области информации; соблюдение запретов пропаганды и агитации, возбуждающих расовую, национальную, религиозную ненависть и вражду; забота о сохранении культурного наследия).

Основными угрозами безопасности правового статуса субъектов информационной сферы являются нерациональное ограничение доступа к общественно необходимой информации, открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, другой открытой социально значимой информации, манипулирование ин-

формацией, противодействие реализации гражданами их права на личную и семейную тайны, тайну переписки, телефонных переговоров и иных сообщений, а также нарушение других законных ограничений на сбор и распространение информации.

Основной целью правового обеспечения безопасности правового статуса субъектов информационной сферы является предупреждение, пресечение и минимизация последствий проявления этих угроз.

В основу правового регулирования отношений, связанных с обеспечением безопасности правового статуса субъектов информационной сферы, положены следующие принципы: - закрепление государственных гарантий доступа к общедоступной информации, в том числе к информации о деятельности государственных органов, органов местного самоуправления; - установление требований к созданию и функционированию государственных информационных систем и информационных систем органов местного самоуправления; - законодательное закрепление порядка и условий автоматизированной обработки персональных данных; - закрепление порядка использования электронной цифровой подписи в электронном документообороте для обмена юридически значимыми электронными документами.

Содержание и структура законодательства

Правовые нормы и институты, образующие правовое обеспечение информационной безопасности, закрепляются в нормативных правовых актах, являющихся источниками права в этой области и составляющих соответствующее законодательство.

В Конституции Российской Федерации закреплены следующие права и свободы: право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом; право на неприкосновенность частной жизни, личную и семейную тайну; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы; запрет на сбор, хранение и распространение информации о частной жизни лица без его согласия и другие нормы.

Федеральные законы закрепляют значительное количество норм, регулирующих отношения в области обеспечения информационной безопасности. К числу данных законов относятся Федеральный конституционный закон «О Правительстве Российской Федерации», Федеральный конституционный закон «Об Уполномоченном по правам человека в Российской Федерации», Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Налоговый кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Таможенный кодекс Российской Федерации и др. Так, Гражданский кодекс Российской Федерации закрепляет нормы, регулирующие отношения в области защиты конфиденциальной информации и некоторых иных видов тайн (коммерческой тайны, личной и семейной тайны), признания электронной цифровой подписи средством удостоверения сделки.

Кодекс Российской Федерации об административных правонарушениях устанавливает ответственность за отказ в предоставлении гражданину информации, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), за нарушение правил защиты информации, за незаконную деятельность в области защиты информации и другие некоторые правонарушения.

Уголовный кодекс Российской Федерации устанавливает ответственность за нарушение неприкосновенности частной жизни, тайны переписки и телефонных переговоров, отказ в предоставлении гражданину информации, незаконный экспорт научнотехнической информации, разглашение государственной тайны, преступления в сфере компьютерной информации и другие преступления в данной сфере.

Важную роль в правовом регулировании отношений в области обеспечения информационной безопасности играют такие основополагающие нормативные правовые акты, как законы Российской Федерации «О безопасности», «О средствах массовой информации», «О государственной тайне», Патентный закон Российской Федерации, федеральные законы «Об информации, информационных технологиях и о защите информации», «Об электронной цифровой подписи» и др.

Среди нормативных правовых актов Президента Российской Федерации можно выделить указы Президента Российской Федерации «О снятии ограничительных грифов с законодательных и иных актов, служивших основанием для массовых репрессий и посягательств на права человека», «О дополнительных правах граждан на информацию», «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» и др. Кроме того, важной составляющей рассматриваемого законодательства являются указы Президента Российской Федерации, устанавливающие компетенцию федеральных органов исполнительной власти в рассматриваемой области.

Подзаконные акты Правительства РФ разъяснения Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации. Важной составляющей законодательства в области обеспечения информационной безопасности являются также международные договоры Российской Федерации. Структура законодательства в области правового обеспечения информационной безопасности и структура нормативного правового обеспечения информационной безопасности в определенной степени различаются. Это обусловлено тем, что система права и система законодательства, образуя совместно объективное право, имеют разные назначение и механизмы развития.

В системе права отражается содержание права как регулятивной системы, состоящей из норм права, правовых институтов и отраслей права. Она выступает объективным основанием системы законодательства. В свою очередь, система законодательства призвана закрепить правовые нормы в системе нормативных правовых актов, взаимосвязанных по предмету правового регулирования и их юридической силе. В отличие от системы права, складывающейся в соответствии с исторически обусловленной структурой общественных отношений, система законодательства является продуктом рациональной деятельности людей, осуществляемой во времени и пространстве. Система законодательства, как и система права, подразделяется на отрасли — наиболее крупные объединения нормативных актов и их частей по определенным сферам правового регулирования. Элементами системы законодательства являются нормативные правовые акты, а также их структурные составляющие (разделы, главы, статьи пункты и т.д.), которые могут объединяться в различные композиции, выделенные по определенному основанию из всей совокупности признаков и характеристик объекта.

Структуру законодательства в области обеспечения информационной безопасности удобно представлять в качестве системы законодательных отраслей права, включающих, в частности:

- законодательство об информации, информационных технологиях и о защите информации;
- законодательство о персональных данных;
- законодательство об интеллектуальной собственности;
- законодательство о тайнах;
- законодательство о средствах массовой информации и о рекламе;
- законодательство о связи;
- законодательство о техническом регулировании;
- законодательство об электронной цифровой подписи.

Правовой режим информации

Объектом рассматриваемого правового режима является информация, под которой в законодательстве понимаются сведения (сообщения, данные) независимо от формы их представления. Информация, зафиксированная на материальном носителе путем документирования, с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель, называется документированной информацией.

Одной из важных форм документированной информации является электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Правовой режим информации включает:

- право использования информации в качестве объекта правовых отношений;
- право обладания информацией;
- право доступа к информации;
- право собственности и иные вещные права на магнитные носители, содержащие документированную информацию;
- документирование информации;
- право распространения и предоставления информации.

Право использования информации в качестве объекта правовых отношений заключается в возможности установления публичных, гражданских и иных правовых отношений, объектом которых является информация.

Законодательством установлено, что в целях заключения гражданско-правовых договоров или оформления иных правоотношений обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, при знается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе. Право обладания информацией заключается в возможности распоряжения ею (разрешение или ограничение доступа; использование, включая распространение; передача другим лицам; правовая защита и иные действия) по усмотрению обладателя.

Право доступа к информации заключается в возможности ее свободного получения и использования любым лицом и передачи одним лицом другому лицу, в случае если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию и информацию ограниченного доступа. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Условия отнесения к информации ограниченного доступа сведений, составляющих коммерческую, служебную и иную тайну, устанавливаются федеральными законами.

Граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законодательством.

Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении уставной деятельности.

Законодательством установлен запрет на ограничение доступа:

- к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;

- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Законодательством установлено, что право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством. Это означает, что такие носители являются объектами гражданских прав наряду с другими вещами.

Документирование информации как составляющая правового режима информации заключается в том, что недокументированная информация преобразуется в документированную в соответствии с требованиями, устанавливаемыми законодательством Российской Федерации или соглашением сторон. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

Право распространения и предоставления информации заключается в возможности свободного осуществления действий, направленных на получение информации неопределенным кругом лиц или на передачу информации неопределенному кругу лиц (распространение), и действий, направленных на получение информации определенным кругом лиц или на передачу информации определенному кругу лиц (предоставление), при соблюдении требований, установленных законодательством Российской Федерации.

Информацию в зависимости от порядка ее предоставления или распространения подразделяют на

свободно распространяемую;

предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

подлежащую в соответствии с федеральными законами предоставлению или распространению; распространяемую в Российской Федерации ограниченно или запрещаемую к распространению.

К требованиям, предъявляемым к распространению и предоставлению информации, относят:

- включение в информацию, распространяемую без использования средств массовой информации, достоверных сведений о ее обладателе или об ином лице, распространяющем информацию, в форме и объеме, которые достаточны для идентификации такого лица;

- обеспечение получателю информации лицом, распространяющим информацию, возможности отказа от нее при использовании для распространения средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений;

- установление соглашения, определяющего порядок предоставления информации, между лицами, участвующими в обмене информацией;

- запрет распространения информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе обязательных экземпляров документов, устанавливаются федеральными законами. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Правовой статус обладателя информации

Обладателем информации считается лицо (физическое или юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование), самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

При осуществлении своих прав обладатель информации обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Обладатель информации, ставшей по его решению общедоступной, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации. Обладатель информации обязан обеспечить бесплатное предоставление: информации о деятельности государственных органов и органов местного самоуправления, если она размещена этими субъектами в информационно-телекоммуникационных сетях; информации, затрагивающей права и установленные законодательством Российской Федерации обязанности заинтересованного лица; иной установленной законом информации. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Защита информации

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Требования о защите общедоступной информации могут устанавливаться только для достижения указанных выше целей. Обладатель информации и оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

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

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

- постоянный контроль за обеспечением уровня защищенности информации.

Требования к защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям. Федеральными законами могут быть установлены ограничения на использование определенных средств защиты информации и на осуществление отдельных видов деятельности в области защиты информации.

Законодательство Российской Федерации **о коммерческой тайне** состоит из Гражданского кодекса Российской Федерации, Федерального закона «О коммерческой тайне» и других федеральных законов.

Предмет правового регулирования составляют отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции.

В законодательстве под коммерческой тайной понимается конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Режим коммерческой тайны образуется совокупностью правовых, организационных, технических и иных принимаемых обладателем информации, составляющей коммерческую тайну, мер по охране ее конфиденциальности. Цель правового регулирования заключается в защите права человека и гражданина на добросовестную конкуренцию, использование своих интеллектуальных способностей. В основу правового механизма регулирования рассматриваемых отношений положен правовой режим коммерческой тайны, включающий: порядок отнесения информации к коммерческой тайне; порядок охраны; порядок представления.

Порядок отнесения информации к коммерческой тайне определяет:

- объект, в отношении которого может быть установлен правовой режим коммерческой тайны;

- способ установления правового режима коммерческой тайны;

- субъекта коммерческой тайны, уполномоченного устанавливать данный правовой режим коммерческой тайны.

Объектом правового режима коммерческой тайны является научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация, самостоятельно полученная лицом при осуществлении иссле-

дований, систематических наблюдений или иной деятельности, считается полученной законным способом, несмотря на то что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо.

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или на другом законном основании, считается полученной законным способом. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности и составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Способ установления режима коммерческой тайны состоит в реализации системы мер по охране конфиденциальности информации, принимаемых ее обладателем, которая должна включать:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданскоправовых договоров;

- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, данных мер. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимая перечисленные выше меры по охране конфиденциальности информации, может не определять перечень информации, составляющей коммерческую тайну, не устанавливать ограничение доступа к информации, составляющей коммерческую тайну.

Наряду с указанными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Меры по охране конфиденциальности информации признаются разумно достаточными при условии, что:

- исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

- обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Основным субъектом коммерческой тайны является обладатель информации, составляющей коммерческую тайну. Под таким обладателем понимается лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, которое ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Обладатель информации, составляющей коммерческую тайну, имеет право:

- устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

- использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

- разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

- вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

- требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

- требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

- защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны. Обладателем ин-

формации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель. В случае получения работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

Государственным или муниципальным контрактом на выполнение научно-исследовательских, опытно-конструкторских, технологических или иных работ для государственных или муниципальных нужд должен быть определен объем сведений, признаваемых конфиденциальными, а также должны быть урегулированы вопросы, касающиеся установления в отношении полученной информации режима коммерческой тайны.

Законодательство Российской Федерации **о государственной тайне** включает Закон Российской Федерации «О государственной тайне», а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны. Предмет правового регулирования — отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием и рассекречиванием, распоряжением этими сведениями, а также их защитой. Субъектами права в области государственной тайны являются органы законодательной, исполнительной и судебной властей (далее — органы государственной власти), местного самоуправления, предприятия, учреждения и организации независимо от их организационно-правовой формы и формы собственности, должностные лица и граждане Российской Федерации, взявшие на себя обязательства либо обязанные по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Цель правового регулирования заключается в противодействии угрозам несанкционированного раскрытия сведений, составляющих государственную тайну. Правовой режим государственной тайны включает: порядок отнесения сведений к государственной тайне; порядок засекречивания и рассекречивания; порядок распоряжения сведениями, составляющими государственную тайну; систему защиты сведений, составляющих государственную тайну.

Объект правового режима государственной тайны — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Порядок отнесения сведений к государственной тайне Отнесение сведений к государственной тайне осуществляется уполномоченными субъектами в соответствии с закрепленным в законодательстве перечнем таких сведений. Государственную тайну составляют:

Сведения в военной области:

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск Российской Федерации, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», их боевой и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;

- планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, направлениях развития вооружения и военной техники, содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

- разработке, технологии, производстве, об объемах производства, хранении, утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

- тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

- дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для них;

- дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке.

2. Сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

- об использовании инфраструктуры Российской Федерации в целях обеспечения ее обороноспособности и безопасности;

- о силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административного управления, степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения ее безопасности;

- об объемах, о планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

- о достижениях науки и техники, научно-исследовательских, опытно-конструкторских, проектных работах и технологиях, имеющих важное оборонное или экономическое значение и влияющих на безопасность государства;

- о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации).

3. Сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства.

- финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства.

4 . Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

- о силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, разработке, изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения; - о методах и средствах защиты секретной информации;

- об организации и фактическом состоянии защиты государственной тайны;

- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

- о подготовке кадров, мероприятиях, проводимых в целях обеспечения безопасности государства.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с законодательством. Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну.

Субъектами отнесения сведений к государственной тайне являются:

1. Палаты Федерального Собрания, которые:

- осуществляют законодательное регулирование отношений в области государственной тайны;

- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;

- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в аппаратах палат Федерального Собрания.

2. Президент Российской Федерации, который:

- утверждает государственные программы в области защиты государственной тайны;

- утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

- утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

- заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;

- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;

- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

3. Правительство Российской Федерации, которое:

- организует исполнение Закона Российской Федерации «О государственной тайне»;

- представляет на утверждение Президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

- представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;

- устанавливает порядок разработки Перечня сведений, отнесенных к государственной тайне;

- организует разработку и выполнение государственных программ в области защиты государственной тайны;

- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;

- устанавливает порядок предоставления социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;

- заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;

- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;

- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;

- устанавливают размеры предоставляемых социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны на подведомственных им предприятиях, в учреждениях и организациях;

- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;

- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению социальных гарантий лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

Отнесение сведений к государственной тайне и их засекречивание

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в с положениям статей «Закона о государственной тайне» и законодательству РФ о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах РФ;
- о состоянии здоровья высших должностных лиц РФ;
- о фактах нарушения законности органами государственной власти и их должностными лицами. (ст. 7 Закона)

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно".

Порядок определения размеров ущерба, который может быть нанесен безопасности РФ вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством РФ.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с законом.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом, руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по раз-

работке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее – собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства РФ.

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- о регистрационном номере;

- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены (ст. 12 Закона).

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством РФ.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Практическое занятие. Изучение структуры государственной системы обеспечения информационной безопасности в РФ, основных нормативно–правовых документов, регламентирующих обращение с информацией ограниченного доступа.

Цель. Знакомство со структурой государственной системы обеспечения информационной безопасности в РФ и основными нормативно-правовыми документами.

Краткие теоретические сведения

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность (военных сведений, информации о космических и ядерных технологиях и т.п.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а вмешательство государства в эту сферу должно быть минимизировано.

На практике *деятельность* органов власти, как правило, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная *стабильность* и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания.

Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают *затраты* и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и т.п.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- сохранение суверенитета государства;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- укрепление законности и правопорядка;
- обеспечение социально-экономического развития страны и устойчивости финансовой системы;
- участие в жизни международного сообщества.

По своей природе факторы, определяющие состояние информационной безопасности и, соответственно, *деятельность* государства в этой сфере, подразделяются на:

- политические;
- социально-экономические;
- организационно-технические.

Организационная *деятельность* государства в сфере информационной безопасности, как правило, сводится к противодействию различным угрозам:

- внешним, таким как деятельность иностранных спецслужб и вооруженных сил, враждебная экономическая и техническая политика отдельных государств, агрессивные рыночные стратегии крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и террористических группировок и т.п.;
- внутренним, таким как деятельность криминальных структур в сфере обращения информации, неправомерные действия государственных структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем и обращении информации, нарушения в работе информационных и телекоммуникационных систем и т.п.

Таким образом, *деятельность* государства в этой сфере направлена на нейтрализацию существующих *угроз информационной безопасности* с учетом всех факторов, воздействующих как на сами *управляющие* государственные структуры, так и на *информационные системы*.

Для решения основных задач в сфере информационной безопасности действуют все основные органы государственной власти и управления: судебные, органы исполнительной власти, правоохранительные органы, организации и предприятия, которые контролируются государством и имеют *доступ* к информации, составляющей *государственную тайну*, и другие.

Для обеспечения информационной безопасности государственные органы выполняют следующие основные функции:

- создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства, таких как право на защиту частной информации, право на защиту коммерческой и *банковской тайны*, право на беспрепятственный доступ к информации и т.п. Данная функция осуществляется законодательными органами в сотрудничестве с органами исполнительной власти, общественными организациями, научно-исследовательскими учреждениями и другими заинтересованными участниками;
- осуществляют правоприменительную деятельность, непосредственно реализуют меры по защите информационных ресурсов государственного управления, а также выполняют все функции, необходимые для *реализации требований* законодательства;
- выполняют судебные функции в отношении лиц, которые допустили правонарушения, связанные с использованием информационных ресурсов, и участвуют в хозяйственных спорах, связанных с нарушениями информационной безопасности.

Вопросы совершенствования законодательства в сфере обеспечения информационной безопасности также могут решаться в различных профильных комитетах, подкомитетах и рабочих группах, специализирующихся на смежных проблемах государственного управления и социально-экономического регулирования, таких как:

- оборона;
- национальная безопасность;
- политика в сфере связи, информации и информатизации;
- промышленная и экономическая политика;
- наука и образование
- и других.

Для разработки соответствующих нормативно-правовых актов *подразделения* (комитеты и подкомитеты) органов законодательной власти могут привлекать для совместной работы ответственных специалистов, руководителей, аналитиков и экспертов, работающих в:

• органах исполнительной власти (министерствах, отвечающих за научное и техническое развитие, т.н. "силовых" министерствах и ведомствах, юридических ведомствах и т.п.);

• частных компаниях, а также общественных и профессиональных организациях, которые занимаются оказанием информационных услуг, поставкой информационно-технических продуктов, специализирующихся на развитии информационных технологий и т.п.;

• научно-исследовательских организациях, специализирующихся на соответствующих проблемах информационных технологий и управления.

Деятельность исполнительных органов государственной власти в сфере обеспечения информационной безопасности направлена на реализацию действующих в государстве законов и непосредственную защиту интересов государственной власти, гражданских прав и прав компаний, осуществляющих хозяйственную *деятельность*.

Конкретная работа органов исполнительной власти в сфере информационной безопасности, как правило, осуществляется *по* нескольким относительно самостоятельным направлениям.

• Установление конкретных правил производства, продажи, экспорта, импорта и использования средств защиты информации, а также организация системы контроля за соблюдением действующих законов и установленных правил.

• Лицензирование и сертификация предприятий и организаций, занимающихся производством, продажей установкой и настройкой программных и аппаратных средств защиты информации.

• Осуществление правоохранительной деятельности в сфере защиты информации (уголовного преследования лиц и преступных группировок, совершающих противоправные действия, содержащие признаки уголовных преступлений в соответствии с действующим уголовным законодательством).

• Непосредственное осуществление функций защиты информации в государственных учреждениях и службах (правительство, вооруженные силы, органы внутренних дел и т.п.).

• Разработка государственных стандартов, относящихся к организации и технологиям защиты информации (программным и аппаратным средствам, средствам криптографии и т.п.).

• Поддержка образования и подготовки кадров, а также регулирование деятельности образовательных учреждений (включая установку образовательных стандартов).

• Поддержка научных исследований в сфере информационной безопасности.

• Осуществление международного сотрудничества в сфере защиты информации (взаимодействие с правительствами и правоохранительными органами других стран) как в целях общего развития инфраструктуры информационной безопасности, так и для разрешения отдельных инцидентов (раскрытия преступлений и т.п.).

Специализированные органы, создаваемые в структуре исполнительной власти для решения задач информационной безопасности на государственном уровне, как правило, подчиняются непосредственно главе исполнительной ветви власти, носят статус федеральных агентств, комитетов или комиссий и наделены правом самостоятельно издавать нормативные акты в рамках имеющихся полномочий, установленных действующим законодательством. Издаваемые таким образом локальные нормативные акты (указы, постановления, инструкции, порядки, правила и т.п.) непосредственно регулируют отношения в сфере создания, распространения и использования средств автоматизации и защиты информации.

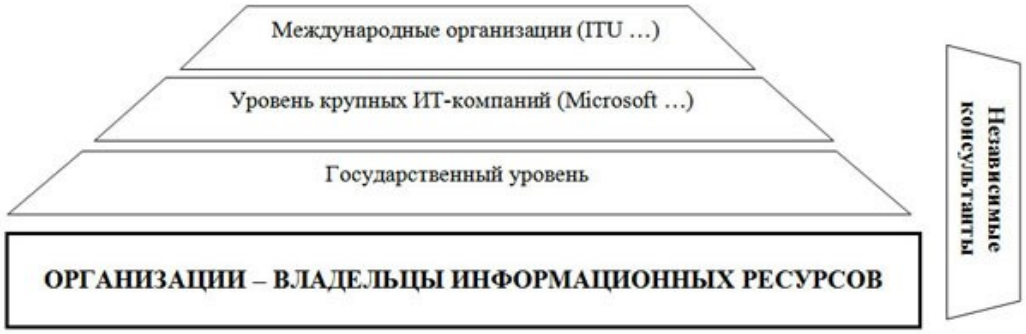
Государственная стандартизация технологий и методов, используемых в процессах защиты информации, осуществляется уполномоченными государственными органами с целью упорядочивания знаний о современном состоянии технологий и методов защиты и установления универсальных критериев надежности и функциональности для определенных технологий. Стандартизация, осуществляемая отдельными государственными органами, как правило, опирается на существующую систему имеющихся международных стандартов, а национальные органы, занимающиеся стандартизацией, могут принимать участие в разработке международных стандартов..

Основой современной политики Российской Федерации в сфере информационной безопасности можно считать "Доктрину информационной безопасности РФ".

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- Федеральный Закон "О *государственной тайне*";
- Федеральный Закон "Об информации, информационных технологиях и о защите информации".

Иерархия уровней организационной работы в сфере информационной безопасности представлена на рисунке.

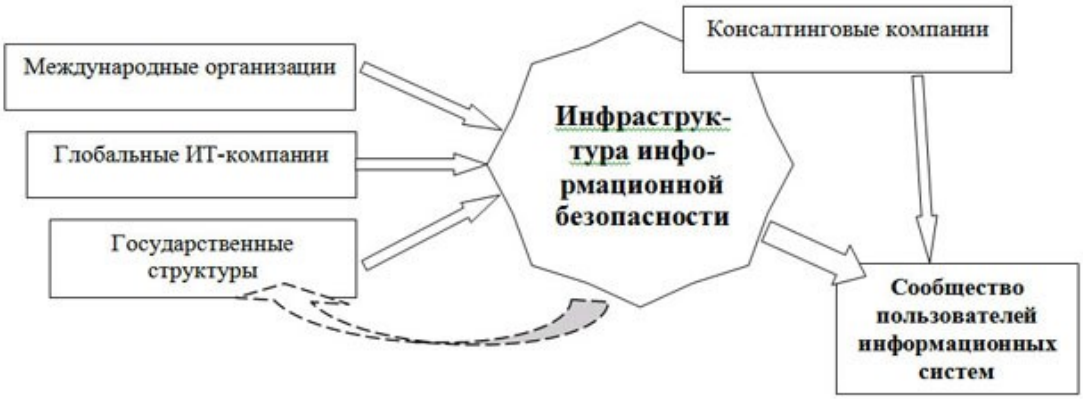


Субъекты, находящиеся на верхних ступенях данной иерархии (в частности, государственные органы, крупные IT-корпорации), выступают не только как владельцы собственных информационных ресурсов, требующих защиты, но и как субъекты, которые воздействуют на инфраструктуру, лежащую в основе обмена и хранения информации, а также на общественно-экономические отношения, влияющие на ИБ. Тот факт, что такие субъекты сами уделяют значительное внимание защите собственных ресурсов (вкладывают существенные средства в обеспечение ИБ, инициируют новые разработки для собственных нужд, используют наиболее передовые технологии в этой сфере и т.п.), не должен отвлекать внимание от того обстоятельства, что эти субъекты фактически создают инфраструктуру для повседневной деятельности *множества* компаний, организаций, людей, профессиональных и бизнес-сообществ и используют для этого организационные методы и приемы, которые существенно отличаются по своей природе от методов, характерных для работы по обеспечению ИБ отдельных субъектов и защите отдельных информационных активов.

Необходимость самостоятельного рассмотрения субъектов, относящихся к верхнему уровню, с точки зрения организационного обеспечения информационной безопасности обусловлена тем, что в связи со своей особой ("инфраструктурной") ролью в системе общественных отношений и информационного обмена эти субъекты используют специфичные методы организационно-управленческой работы. При этом, как правило, параллельно с применением таких специфичных методов они используют и методы, характерные для субъектов нижнего уровня представленной иерархии, т.к. являются владельцами собственных информационных ресурсов.

Представленное разделение на уровни должно быть основой для более целенаправленного развития системы менеджмента и налаживания взаимосвязей между различными уровнями организационной работы. Важность выделения и самостоятельного рассмотрения верхних уровней управленческой работы обусловлена тем, что целенаправленное осознание организационных вопросов, специфичных для верхних уровней иерархии, и их решение позволит более эффективно решать задачи развития национальных и региональных экономик в целом и отдельных отраслей (*телекоммуникации*, финансовые услуги и т.п.), а не только решать задачи отдельных субъектов, участвующих в информационном обмене.

Взаимосвязи уровней организации информационной безопасности отражены на рисунке



Основные особенности организационной работы на каждом из перечисленных уровней организации представлены в таблице

Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности

Организационный уровень	Основные задачи и роли	Основные специфичные методы организационной работы
1. Международные организации	Разработка правил и стандартов (в том числе и сетевых протоколов), имеющих глобальное значение Обмен актуальной информацией и предупреждениями о новых угрозах	Координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны
2. Глобальные ИТ-компании	Методологическая и организационная поддержка использования продуктов и услуг, поставляемых на рынок	Гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг
3. Государственные организации	Регулирование использования информационных систем и распространения информации с целью недопущения противоправных действий, ущерба другим участникам информационного обмена, обществу и государственным органам	Разработка национальных и международных правил (законов, конвенций, соглашений и т.п.), регулирующих отношения в информационной сфере Осуществление контроля (в различных формах) Осуществление правоприменительной и правоохранительной деятельности
4. Пользователи информационных систем – владельцы информации	Защита собственных информационных ресурсов	Выделение подразделений и специалистов, отвечающих за ИБ Разработка и применение внутренних политик и правил безопасности
5. Консалтинговые и внедренческие компании, работающие в сфере ИБ	Выполнение некоторых функций ИБ на условиях аутсорсинга Разработка и внедрение индивидуальных решений в сфере ИБ более эффективно, чем это могли бы сделать сами владельцы информационных ресурсов	Накопление и обобщение теоретических знаний и практических навыков с целью создания и внедрения организационных и технических решений в интересах клиентов

Основными элементами организационной структуры системы обеспечения информационной безопасности Российской Федерации на федеральном уровне являются: Президент Российской Федерации, Совет Безопасности, Совет Федерации, Государственная Дума, Правительство Российской Федерации, федеральные органы исполнительной власти, государственные и межведомственные комиссии, создаваемые Президентом и Правительством Российской Федерации для решения вопросов в соответствии с предоставленными им полномочиями, определяемыми Положениями о комиссиях.

Федеральные министерства и ведомства могут в своем составе создавать соответствующие службы и подразделения для решения вопросов обеспечения информационной безопасности на отраслевом уровне.

Контролирующими и правоохранительными органами федерального уровня, обеспечивающими соблюдение нормативно – правовых норм, являются: Конституционный суд, Верховный суд, Генеральная прокуратура.

Следующим уровнем в системе обеспечения информационной безопасности являются органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, которые могут также создавать различные комиссии.

Наконец, нижним уровнем системы обеспечения информационной безопасности являются структурные подразделения и должностные лица предприятий и организаций.

Вопросы

1. Назовите цели российского государства в сфере информатизации.
2. В каком нормативном акте названы цели российского государства в сфере информатизации?
3. Каким нормативным актом регулируется порядок публикации в СМИ сообщений и материалов федеральных органов государственной власти?
4. Перечислите органы государственной власти осуществляющие управление в информационной сфере.
5. Расскажите о полномочиях органов государственной власти осуществляющих управление в информационной сфере.
6. Расскажите о взаимодействие органов местного самоуправления и органов государственной власти в информационной сфере.
7. Назовите основные направления взаимодействия органов местного самоуправления и органов государственной власти в информационной сфере.
8. Каковы согласно Доктрине информационной безопасности РФ основные составляющие национальных интересов РФ в информационной сфере?
9. Назовите общие методы обеспечения информационной безопасности РФ.
10. Назовите основные элементы организационной основы системы обеспечения ИБ РФ.

Практическое занятие. Разработка организационных мероприятий обеспечения информационной безопасности на режимном предприятии. Функции, задачи и особенности службы безопасности организации. Принципы организации службы безопасности организации. Типовая структура службы безопасности

Цель. Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – **Концепции и Политики информационной безопасности.** Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит **КАК**, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании, содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Вопросы.

1. Мероприятия, проводимые службой безопасности по защите конфиденциальной информации.
2. Перечислите основные способы несанкционированного доступа к информации.
3. Что относится к числу основных задач службы безопасности?
4. Перечислите основные принципы построения системы безопасности предприятия.
5. Перечислите основные функции службы защиты информации.
6. Приведите типовую структуру службы безопасности.

Практическое занятие . Допуск и доступ к конфиденциальной информации и документам. Организация подготовки и проведения совещания по конфиденциальным вопросам. Первичный инструктаж при приеме на работу. Периодический инструктаж. Периодическая учеба персонала

Практическое занятие. Допуск и доступ к конфиденциальной информации и документам. Организация подготовки и проведения совещания по конфиденциальным вопросам.

Цель занятия. Выработка навыков действий по процедуре допуска и доступа к конфиденциальной информации. Выработка навыков выполнения мероприятий по защите информации при проведении конфиденциальных совещаний

Порядок выполнения занятия

Подписание работником обязательства о неразглашении сведений, составляющих коммерческую тайну, а также трудового договора, который в соответствии со ст. 57 Трудового кодекса Российской Федерации может содержать эти обязательства.

Оформление в установленном порядке допуска к сведениям, составляющим коммерческую тайну.

Оформление разрешения руководителя предприятия на ознакомление работника с конкретной информацией, являющейся коммерческой тайной, и ее носителями.

Составление именных (должностных) списков сотрудников, допускаемых к той или иной информации, составляющей коммерческую тайну предприятия, в обязательном порядке содержащих должности и фамилии сотрудников и категории сведений (документов), к которым они допускаются.

Оформление разрешения непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного конкретному сотруднику;

Разработать план проведения конфиденциального совещания.

Краткие теоретические сведения

Основные условия правомерного доступа персонала к коммерческой информации включают:

- подписание работником обязательства о неразглашении сведений, составляющих коммерческую тайну, а также трудового договора, который в соответствии со ст. 57 Трудового кодекса Российской Федерации может содержать эти обязательства;
- наличие у работника оформленного в установленном порядке допуска к сведениям, составляющим коммерческую тайну;
- наличие утвержденных руководителем предприятия должностных (функциональных) обязанностей работника, определяющих круг его задач и объем необходимой для их решения информации;
- оформление разрешения руководителя предприятия на ознакомление работника с конкретной информацией, являющейся коммерческой тайной, и ее носителями.
- составление именных (должностных) списков сотрудников, допускаемых к той или иной информации, составляющей коммерческую тайну предприятия, в обязательном порядке содержащих должности и фамилии сотрудников и категории сведений (документов), к которым они допускаются;
- оформление разрешения непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного конкретному сотруднику;
- указание (перечисление) в организационно-плановых и иных документах предприятия сотрудников (их фамилий), которые при решении конкретных производственных и иных задач должны быть допущены к определенной информации, составляющей коммерческую тайну предприятия.

Разработке положения предшествует всесторонний анализ различных документов (материалов), проводимый в целях выявления и классификации всех информационных потоков, существующих на предприятии. В ходе анализа изучаются все направления и стороны деятельности предприятия, в том числе его взаимодействие с организациями-соисполнителями и заказчиками, работа диссертационных советов, образовательная деятельность и т.п. После получения результа-

тов анализа формируется структура положения (готовится его проект). Основными разделами положения являются:

- общие требования по доступу работников к коммерческой тайне;
- порядок доступа к носителям информации, имеющим различные категории (степени) конфиденциальности;
- порядок доступа к делам и документам архивного хранения;
- порядок копирования (размножения) документов и рассылки их нескольким адресатам;
- порядок доступа к носителям информации командированных лиц, представителей органов местного самоуправления, различных территориальных и надзорных органов;
- порядок доступа к информации (ее носителям) в ходе проведения совещаний, конференций, семинаров и других мероприятий. После разработки положение утверждается руководителем предприятия и доводится до сведения непосредственных исполнителей указанных в нем мероприятий (работ), а также до сведения каждого сотрудника предприятия в части, касающейся данного сотрудника (в необходимых случаях — под расписку).

Договорное обязательство

Обязуюсь:.

1. В период оформления на работу и работы в _____ не разглашать сведения, составляющие ее коммерческую тайну, которые мне будут доверены или станут известны при исполнений обязанностей, собеседованиях, инструктировании и обучении.

2. Беспрекословно и аккуратно выполнять относящиеся ко мне требования приказов, инструкций и положений по защите коммерческой тайны, с которой я ознакомлен.

3. Не сообщать устно, письменно или иным способом кому бы то ни было сведений, составляющих тайну _____

4. В случае отказа от работы, окончания работы или увольнения не разглашать и не использовать для себя и других лиц сведений, составляющих тайну _____

Я предупрежден, что в случае нарушения данного обязательства должен возместить причиненный ущерб или буду привлечѐн к дисциплинарной (вплоть до увольнения) или другой ответственности в соответствии с действующим законодательством.

Проинструктировал _____
(должность, ФИО, подпись, дата)

Подпись лица, принимающего обязательство _____
(ФИО, подпись, дата)

Защита информации при проведении совещаний и переговоров Конфиденциальными именуются обычно совещания и переговоры, в процессе которых могут обсуждаться сведения, составляющие тайну предприятия или его партнеров. Порядок проведения подобных совещаний и переговоров регламентируется специальными требованиями, обеспечивающими безопасность конфиденциальной информации, которая в процессе этих мероприятий распространяется в разрешенном режиме. Основной угрозой ценной информации является разглашение большего объема сведений о новой идее, продукции или технологии, чем это необходимо.

Общеизвестны причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах. Это и слабое знание сотрудниками состава ценной информации и требований по ее защите, умышленное невыполнение этих требований, провоцированные и неспровоцированные ошибки сотрудников, отсутствие контроля за изданием рекламной и рекламно-выставочной продукции и др. Оглашение ценной информации в санкционированном режиме должно быть оправдано деловой необходимостью и целесообразностью для конкретных условий и характера обсуждаемых вопросов.

Выделяют следующие этапы проведения конфиденциальных совещаний и переговоров: подготовка к проведению, процесс их ведения и документирования, анализ итогов и выполнения достигнутых договоренностей (Рис. 1)

Разрешение на проведение конфиденциальных совещаний и переговоров с приглашением представителей других организаций и фирм дает директор предприятия. Решение директора о предстоящем конфиденциальном совещании доводится до сведения руководителя секретариата, секретаря-референта, специалиста по защите конфиденциальной информации и начальника службы безопасности. В целях дальнейшего контроля за подготовкой и проведением такого совещания информация об этом решении фиксируется в учетной карточке, в которой указываются: наименование совещания, дата, время, состав участников по каждому вопросу и руководитель, ответственный за проведение.

Доступ сотрудников предприятия на любые конфиденциальные совещания осуществляется на основе действующей разрешительной системы доступа персонала к конфиденциальной информации. Приглашение на конфиденциальные совещания лиц, не являющихся сотрудниками предприятия, разрешается только в случае крайней необходимости их личного участия в обсуждении конкретного вопроса.

Рисунок 1 Этапы проведения конфиденциальных совещаний и переговоров

Ответственность за обеспечение защиты ценной информации и сохранение тайны предприятия в ходе совещания несет руководитель, организующий данное совещание. Сотрудники службы безопасности оказывают ему помощь и осуществляют контроль за перекрытием возможных организационных и технических каналов утраты информации.

Подготовку конфиденциального совещания осуществляет организующий его руководитель с привлечением сотрудников предприятия, допущенных к работе с конкретной ценной информацией, составляющей тайну предприятия или ее партнеров. Из числа этих сотрудников назначается ответственный организатор, планирующий и координирующий выполнение подготовительных мероприятий и проведение самого совещания.

В процессе подготовки конфиденциального совещания составляются программа проведения совещания, повестка дня, информационные материалы, проекты решений и список участников совещания по каждому вопросу повестки дня. Все документы, составляемые в процессе подготовки конфиденциального совещания, должны иметь гриф «Конфиденциально», изготовляться и издаваться в соответствии с требованиями инструкции по обработке и хранению конфиденциальных документов. Документы, предназначенные для раздачи участникам совещания, не должны содержать конфиденциальные сведения. Эта информация сообщается участникам совещания устно при обсуждении конкретного вопроса.

Список участников конфиденциального совещания составляется отдельно по каждому обсуждаемому вопросу. К участию в обсуждении вопроса привлекаются только те сотрудники предприятия, которые имеют непосредственное отношение к этому вопросу. Это правило касается и руководителей.

Документы, составляемые при подготовке конфиденциального совещания, на котором предполагается присутствие представителей других фирм и организаций, согласовываются с руководителем службы безопасности. Отмеченные им недостатки в обеспечении защиты ценной информации должны быть исправлены ответственным организатором совещания. После этого документы утверждаются руководителем, организующим совещание.

Одновременно с визированием подготовленных документов руководитель службы безопасности и ответственный организатор определяют место проведения совещания, порядок доступа участников в это помещение, порядок документирования хода совещания, а также порядок передачи участникам совещания оформленных решений и подписанных документов.

Конфиденциальное совещание проводится в специальном помещении и оборудованном средствами технической защиты информации. Доступ в такие помещения сотрудников предприятия и представителей других организаций разрешается только руководителем службы безопасности.

Перед началом конфиденциального совещания сотрудник службы безопасности обязан убедиться в отсутствии в помещении несанкционированно установленных аудио- и видеозаписывающих или передающих устройств и в качественной работе средств технической защиты на всех возможных каналах утечки информации. Помещение должно быть оборудовано кондиционером, так как открытие окон, дверей в ходе совещания не допускается. Окна закрываются светопроницаемыми шторами, входная дверь оборудуется сигналом, оповещающим о ее неплотном закрытии. В целях звукоизоляции целесообразно иметь двойную дверь или зашторивать двери звукопоглощающей тканью.

В помещении для проведения конфиденциальных совещаний не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения хода совещания. Документирование, аудио- и видеозапись конфиденциальных совещаний ведутся только по письменному указанию директором предприятия одним из сотрудников, готовивших совещание.

Доступ участников на конфиденциальное совещание осуществляет ответственный организатор под контролем сотрудника службы безопасности в соответствии с утвержденным списком и предъявляемыми участниками персональными документами. Перед началом обсуждения каждого вопроса состав присутствующих корректируется. Нахождение на совещании лиц, не имеющих отношения к обсуждаемому вопросу, не разрешается.

Обычно при открытии совещания организовавший его руководитель должен напомнить участникам о необходимости сохранения производственной и коммерческой тайны и уточнить, какие конкретные сведения являются конфиденциальными на данном совещании.

Участникам конфиденциального совещания, независимо от занимаемой должности и статуса на совещании, не разрешается:

- вносить на совещание фото-, и видеоаппаратуру, компьютеры, магнитофоны, диктофоны и радиотелефоны и другую бытовую аппаратуру и пользоваться ими;
- делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф ограничения доступа;
- обсуждать вопросы, вынесенные на совещание, в местах общего пользования;
- информировать о совещании любых лиц, не связанных с проведением данного совещания, в том числе сотрудников предприятия.

Участники совещания, нарушившие перечисленные правила, лишаются права дальнейшего присутствия на совещании.

По окончании конфиденциального совещания сотрудник службы безопасности осматривает помещение, запирает, опечатывает и сдает под охрану. Документы, принятые на совещании, оформляются, подписываются, при необходимости размножаются и передаются участникам совещания в соответствии с требованиями по работе с конфиденциальными документами предприятия. Все экземпляры этих документов должны иметь гриф ограничения доступа. Рассылать документы, содержащие строго конфиденциальную информацию, не разрешается.

На практике местом проведения переговоров часто становятся постоянно действующие и периодические торговые или торгово-промышленные выставки и ярмарки. Любая выставка является, с одной стороны, отличным источником полезной для бизнеса информации, объектом добросовестного маркетингового исследования рынка товаров, а с другой – опасным каналом несанкцио-

нированного получения конфиденциальных сведений, касающихся новых идей, технологий и продукции. Обобщенно источники ценных сведений в процессе выставочной деятельности включают в себя: экспозицию, персонал предприятия, участвующий в выставке, и рекламно-выставочные материалы. Утрата ценной информации происходит в результате общения специалистов родственных профессий, но разных фирм и наличия в выставочной экспозиции самого нового продукта. Проводимые вместе с выставочными мероприятиями пресс-конференции, семинары, презентации фирм и товаров создают дополнительную угрозу сохранности ценной информации.

Для обеспечения безопасности конфиденциальной информации в рекламно-выставочных материалах следует заблаговременно:

- проанализировать множество предполагаемых к изданию материалов с точки зрения возможности извлечения из них ценных конфиденциальных сведений;
- разбить информацию на части и распределить их между разными рекламно-выставочными материалами, предназначенными для массового посетителя и посетителей-специалистов;
- разбить информацию по видам и средствам рекламы – традиционным бумажным изданиям, электронной рекламе, Web-странице, рекламе в средствах массовой информации и др.

Вопросы.

1. Основные требования, предъявляемые к подготовке служебного совещания.
2. Организация обеспечения режима секретности при проведении служебного совещания.
3. Требования к помещениям проведения совещания.
4. Организация работ по защите информации при опубликовании открытых материалов.
5. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.
6. Допуск лиц к конфиденциальной информации.

Практическое занятие. Организация пропускного и внутриобъектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Требования к помещениям, в которых циркулирует защищаемая информация. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима.

Цель. Ознакомиться с порядком определения перечня предметов, запрещенных к проносу/провозу на территорию организации

Теоретические сведения

Пропускной режим устанавливается на предприятиях в целях недопущения бесконтрольного прохода на территорию, а также бесконтрольного вноса, выноса материальных ценностей, ввоза и вывоза материальных ценностей, технической и другой служебной документации.

Пропускной режим распространяется как на сотрудников предприятия, так и на посетителей и на автотранспорт.

Пропускной режим может устанавливаться как для прохода на территорию предприятия в целом, так и в отдельные зоны безопасности; под наблюдением непосредственно сотрудников охраны, либо через автоматизированные посты, оборудованные соответствующими техническими средствами.

Пропуск - документ, удостоверяющий право прохода на территорию и нахождение на этой территории.

Существуют 3 вида пропусков:

- постоянный;
- временный;
- разовый.

Постоянные пропуска оформляются на сотрудников, постоянно работающих на предприятии, и только после выхода соответствующего приказа.

При выдаче пропуска сотрудник обязательно знакомится под расписку с правилами внутреннего распорядка.

При утере пропуска проводится служебное расследование. На период проведения служебного расследования сотруднику может быть выдан временный, а по его результатам принято решение о списании старого пропуска и выдачи нового.

Временные пропуска выдаются при выполнении определенного вида работ (производственная необходимость) либо на период замещения времен-но отсутствующего сотрудника (длительная командировка, болезнь). Временные пропуска выдаются по заявкам руководителей структурных подразделений с обязательной визой заместителя директора по режиму (начальника Службы безопасности). Максимальный срок действия временного пропуска устанавливается 6 месяцев с возможностью дальнейшего продления еще на 6 месяцев, после чего временный пропуск оформляется заново.

Краткосрочные пропуска могут не иметь фотографии. В этом случае проход на территорию осуществляется при одновременном предъявлении паспорта.

Разовые пропуска оформляются на каждое лицо в отдельности только на данный день и время. Для получения разового пропуска необходимо иметь:

– предписание на выполнение конкретного вида работ;
– справку о допуске;
– паспорт или другое удостоверение личности.

Для участия в массовых мероприятиях (общих собраниях, конференциях и т. д.) допускается проход на территорию по спискам с предъявлением паспорта. При этом должен быть назначен ответственный за проведение мероприятия. Руководством предприятия принимаются меры по ограничению доступа участников на неоговоренные планом мероприятия территории.

Въезд и выезд автотранспорта на территорию предприятия осуществляется по пропускам на машину с конкретным номером.

Сотрудники, сопровождающие машину (например, грузчики, экспедиторы), должны проходить на территорию в установленном порядке, т.е. по пропускам.

Охрана обязана осуществлять досмотр ввозимого и вывозимого груза. На весь груз должно быть оформлено разрешение в виде материальных накладных.

Сотрудники МЧС, скорой помощи проезжают на собственной машине в сопровождении сотрудников службы безопасности.

Внос и вынос материальных ценностей и документов производится при наличии товарно-транспортной накладной или материального пропуска.

Материальный пропуск подписывается:

– руководителем или заместителем руководителя предприятия;
– начальником финансово-бухгалтерского отдела или его заместителем (главным бухгалтером).

Оформление на вынос или вывоз специальных изделий осуществляется в том же порядке, но с обязательной визой начальника Службы безопасности. Допускается ввоз и вывоз материальных ценностей на опломбированных машинах. В этом случае сотрудники службы безопасности проверяют только наличие пломб и разрешение на выезд.

Мусор, снег, старый лом, отходы производства вывозятся по специальным накладным, а погрузка осуществляется в присутствии специально назначенных лиц.

Внос или вынос несекретной документации (литературы) осуществляется после просмотра в Службе безопасности. Внос и вынос секретных документов производится в установленном порядке с разрешения заместителя руководителя предприятия (начальника службы безопасности).

Проход на территорию предприятий разрешается, как правило, с личными вещами небольшого размера. Работникам охраны разрешается в ряде случаев досмотр личных вещей (последнее должно быть особо оговорено Правилами внутреннего распорядка). При обнаружении подозрительных вещей должен составляется протокол и проводиться служебное расследование.

В связи с тем, что на большинстве режимных предприятий ограничен пронос личный вещей, то при входе, на нережимной территории, оборудуются специальные камеры хранения.

Для ведения переговоров с сотрудниками других предприятий рекомендуется оборудовать специальные изолированные комнаты переговоров, расположенные на нережимной территории предприятия.

Отдельно Правилами должен быть оговорен пронос на территорию предприятия (без соответствующего разрешения) личной кино- и фотосъе-мочной аппаратуры, звуко- и видеозаписывающей аппаратуры, множительной, копировальной техники, персональных ЭВМ и блоков к ним, мобильных телефонов.

Режимные, складские помещения, хранилища ценностей и носителей информации, архивы должны обладать надежными стенами и перекрытиями, иметь прочные двери и обладать охранной сигнализацией. Окна нижних этажей помещений, выходящих на неохраняемую территорию, а также окна режимных и складских помещений, выходящих на охраняемую территорию, должны иметь соответствующие решетки.

По окончании работы в помещениях, заблокированных сигнализацией, двери запираются и опечатываются. Ключи под расписку сдаются в охрану.

Включение сигнализации производится начальником охраны или его заместителем в присутствии сотрудника, сдающего помещение. О времени включения сигнализации делается отметка в соответствующем журнале. Получение ключей, вскрытие заблокированных помещений осуществляется лицами, работающими на данном предприятии, при предъявлении соответствующего пропуска и только в том случае, если эти лица включены в соответствующий список. Место хранения и порядок выдачи дубликатов ключей заранее оговариваются.

Уборка режимных помещений должна производиться в присутствии сотрудника, работающего в данном помещении. Во время уборки помещения все служебные документы должны быть убраны с рабочих мест.

Помещения, в которых ведутся секретные работы, должны быть постоянно закрыты на замок. В таких помещениях должны находиться только лица, которые имеют отношение к работе в данном помещении. Список лиц, допущенных к работе в режимном помещении, составляется руководителем подразделения, согласовывается со Службой безопасности и утверждается руководителем предприятия или его заместителем.

Режимные помещения аттестуются. Вид аттестации определяется степенью конфиденциальности информации, представленной в данном помещении. На случай пожара или других стихийных бедствий должны быть разработаны специальные инструкции, в которых определяется порядок вывода сотрудников, вскрытие помещений, спасение документов и изделий.

Задание. Разработать инструкцию Требования к помещениям, в которых циркулирует защищаемая информация. Ответить на контрольные вопросы.

Вопросы.

1. Определение границ контролируемых зон.
2. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации.
3. Кто дает разрешение на вывоз компьютерной техники?
4. Какие требования к помещениям в которых работают с конфиденциальной информацией?
5. Виды пропусков.

Практическое занятие. Организация и обеспечение режима секретности. Требования режима секретности при работе с секретными документами. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов. Формы допусков. Служебное расследование нарушений режима секретности. Организация работ по защите информации при опубликовании открытых материалов.

Цель занятия. Организация работы по защите государственной тайны

Порядок выполнения занятия

Ответить на вопросы вводного контроля:

– Какие нормативные документы регулируют порядок допуска к сведениям, составляющих государственную тайну?

– Сколько существует форм допуска к сведениям, составляющих государственную тайну?
– Необходимо ли письменное согласие на частное, временное ограничение прав?
– Каковы условия проведения проверочных мероприятий?

Принятие на себя гражданином или должностным лицом обязательств перед государством по нераспространению доверенных сведений, составляющих государственную тайну.

Письменное согласие гражданина или должностного лица на проведение в его отношении проверочных мероприятий полномочными органами.

Подготовить номенклатуру должностей работников, подлежащих оформлению на допуск к государственной тайне (форма № 3).

Составить предписание на выполнение задания (форма № 5).

Утв. постановлением Правительства РФ
от 6 февраля 2010 г. № 63
Форма 2

**Примерное содержание обязательств граждан
перед государством по соблюдению требований законодательства
Российской Федерации о государственной тайне**

Я _____ ,
(фамилия, имя, отчество)

оформляясь на должность в _____ ,
(наименование организации)

будучи поставлен(а) в известность о том, что по роду своей деятельности и обязанностям буду допущен(а) к государственной тайне, добровольно принимаю на себя обязательства, связанные с допуском к государственной тайне, на условиях, предусмотренных законодательством Российской Федерации о государственной тайне.

В соответствии с Законом Российской Федерации «О государственной тайне» и иными нормативными правовыми актами о государственной тайне, с которыми меня ознакомили, принимая на себя перед государством обязательства по неразглашению доверенных мне сведений, составляющих государственную тайну, даю согласие на частичные, временные ограничения моих прав, которые могут касаться:

права на выезд из Российской Федерации на срок до 5 лет со дня последнего ознакомления со сведениями особой важности и совершенно секретными сведениями;

права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих сведения, составляющие государственную тайну;

права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления (переоформления) допуска к государственной тайне.

Принимаю на себя обязательства:

соблюдать требования законодательства Российской Федерации о государственной тайне;

в случае принятия решения о временном ограничении моего права на выезд из Российской Федерации в 5-дневный срок передать имеющийся заграничный паспорт на хранение в

_____
(наименование организации)

до истечения установленного срока ограничения моих прав;

в полном объеме и своевременно информировать кадровое подразделение _____

_____
(наименование организации)

об изменениях в анкетных и автобиографических данных и о возникновении оснований для отказа мне в допуске к государственной тайне, предусмотренных Законом Российской Федерации «О государственной тайне»;

представлять в установленном порядке в кадровое подразделение _____

_____
(наименование организации)

документы об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом государственной власти, уполномоченным в области здравоохранения и социального развития;

в случае попытки посторонних лиц получить информацию секретного характера немедленно сообщить об этом в режимно-секретное подразделение

_____
(наименование организации)

или в органы Федеральной службы безопасности Российской Федерации.

Я предупрежден(а) о том, что в случае даже однократного нарушения мною принятых на себя обязательств, а также при возникновении обстоятельств, являющихся основанием для отказа мне в допуске к государственной тайне, мой допуск к государ-

ственной тайне может быть прекращен и я буду отстранен(а) от работы со сведениями, составляющими государственную тайну, а трудовой договор (контракт) со мной может быть расторгнут.

Утв. постановлением Правительства РФ
от 6 февраля 2010 г. № 63
Форма 1

КАРТОЧКА

1. _____
(фамилия, имя, отчество)

2. _____
(дата и место рождения)

_____

3. Сведения о наличии загранпаспорта _____

_____

4. Образование _____
(наименование учебного

_____
заведения, когда окончил)

5. Домашний адрес _____

_____

6. Дополнительные отметки _____

_____

_____

Место
для
фотографии
(4 см × 6 см)

_____
(учетный номер карточки по журналу)

М. П.

Фотография _____
(фамилия и инициалы)

и данные, указанные в карточке удостоверяются.

Руководитель режимно-секретного подразделения

_____
(подпись)

«____» _____ 20____ г.

_____

10. Сведения о нарушениях режима секретности и наличии оснований для отказа в допуске

_____

11. Родственники (муж (жена), в т.ч. бывшие, отец, мать, усыновители, усыновленные, полнородные и неполнородные (имеющие общих отца или мать) братья и сестры, дети старше 14 лет).

№ п/п	Фамилия, имя, отчество	Степень родства	Дата рождения	Примечание

7. Данные о проведении проверочных мероприятий органами безопасности.

Проверка
по _____ форме произведена.

_____
(подпись)

_____ «____» _____ 20____ г.

М. П.

Особые отметки

8. Распоряжение о допуске:

Допустить _____
(фамилия и инициалы)

к работам и документам по _____ форме.

Руководитель организации _____
(подпись)

«____» _____ 20____ г.

М. П.

Прекратить допуск _____
(фамилия и инициалы)

_____ Руководитель организации _____

(подпись)

_____

М. П. «____» _____ 20____ г.

Проверка

по _____ форме произведена. М. П.

_____ Допустить _____

(подпись) (фамилия и инициалы)

«____» _____ 20____ г. к работам и документам по _____ форме.

М. П. Руководитель организации _____

(подпись)

Особые отметки «____» _____ 20____ г.

М. П.

_____

Прекратить допуск _____

(фамилия и инициалы)

Руководитель организации _____

(подпись)

«____» _____ 20____ г.

9. Трудовая деятельность с момента оформления допуска:

№ п/п	Наименование организации, юридический адрес	Занимаемая должность (подразделение)	№ и дата приказа о приеме	№ и дата приказа об увольнении	Примечание

Пояснение. Заполнение карточки от руки не допускается.

Мне известно, что в соответствии с Законом Российской Федерации «О государственной тайне» в случае прекращения допуска к государственной тайне я не освобождаюсь от взятых обязательств по неразглашению сведений, составляющих государственную тайну.

Обязуюсь добросовестно выполнять свои обязательства, строго сохранять доверенные мне сведения, составляющие государственную тайну.

Я предупрежден(а), что за разглашение сведений, составляющих государственную тайну, или утрату носителей сведений, составляющих государственную тайну, а также за нарушение режима секретности буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____

(подпись) (инициалы, фамилия)

«____» _____ 20____ г.

Утв. постановлением Правительства РФ
от 6 февраля 2010 г. № 63
Форма 3

УТВЕРЖДАЮ

_____

«____» _____ 20____ г.

НОМЕНКЛАТУРА
должностей работников

_____ ,

(наименование организации)

подлежащих оформлению на допуск к государственной тайне

№ п/п	Подразделение	Количество работающих по штату	Должность	Обоснование необходимости допуска к государст-	Кол-во лиц, подлежащих оформлению на допуск к сведениям			Кол-во лиц, оформленных на допуск к сведениям			Примечание
					ОВ	СС	С	ОВ	СС	С	

				венной тайне							
1	2	3	4	5	6	7	8	9	10	11	12

Руководитель режимно-секретного подразделения

_____
(подпись)

«____» _____ 20____ г.

Пояснения:

1. Порядковые номера должностей указываются в возрастающей последовательности независимо от структурных подразделений (каждой должности соответствует свой порядковый номер).

2. В графе 3 проставляется общее количество работающих, предусмотренное штатным расписанием (отдельно по каждому подразделению и по каждой должности).

3. В графе 5 кратко отражаются функциональные обязанности и (или) характер выполняемых работ со ссылкой на пункт развернутого перечня сведений, подлежащих засекречиванию. В случае если пункт развернутого перечня предусматривает разные степени секретности, дополнительно указывается абзац (графа) данного пункта.

4. По графам 3, 6—11 подводится итог по каждому подразделению и в конце номенклатуры — по всей организации.

5. В дополнениях к номенклатуре должностей порядковые номера указываются в возрастающей последовательности, начиная с единицы, независимо от структурных подразделений.

Утв. постановлением Правительства РФ
от 6 февраля 2010 г. № 63
Форма 5

ПРЕДПИСАНИЕ № _____
на выполнение задания

Штамп организации «____» _____ 20____ г.

_____
(должность)

_____
(фамилия, имя, отчество)

командируется в _____
(наименование организации)

в целях _____
(указать конкретно)

Руководитель организации _____
(подпись)

М. П.
(печать организации)

Разрешаю _____
(с чем ознакомить, что конкретно предоставить)

«____» _____ 20____ г. _____ _____
(подпись) (инициалы, фамилия)

_____ допущен(а) к _____ сведениям.
(инициалы, фамилия командированного лица) (степень секретности)

Ему (ей) разрешен доступ в помещение _____
(№ или наименование помещения)

в сопровождении _____
(должность, фамилия и инициалы сопровождающего лица)

Руководитель режимно-
секретного подразделения _____ «____» _____ 20____ г.
(подпись)

СПРАВКА

_____ ознакомлен(а) _____
(фамилия, инициалы командированного лица) (указать, с какими работами,

_____
документами или изделиями, какова степень их секретности)

_____

_____ _____ _____
(должность лица, принявшего командированного) (фамилия, инициалы) (подпись)

Подпись ознакомившегося _____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20____ г.

Вопросы.

1. Что понимается под режимом секретности?
2. Что включает в себя режим секретности?
3. Что понимается под пропускным режимом?
4. Что понимается под внутриобъектовым режимом?
5. Перечислите особенности защиты информации при авариях и иных экстремальных ситуациях.
6. Перечислите особенности защиты информации при осуществлении международного научно-технического и экономического сотрудничества.
7. Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях.

Практическое занятие 5. Организация и обеспечение режима секретности. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве. Требования режима секретности при работе с секретными документами. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов. Формы допусков. Служебное расследование нарушений режима секретности. Организация работ по защите информации при опубликовании открытых материалов.

Цель занятия. Изучить правила разработки и ведения перечня сведений, составляющих конфиденциальный характер и выработка навыков выработки мероприятий, направленных на управление рисками,

Документ о порядке и методических указаниях по формированию Перечня сведений, составляющих конфиденциальный характер, должен разрабатываться в организации в виде отдельного положения, которое подписывается начальником службы безопасности (заместителем по режиму) или другим должностным лицом, в ведении которого находятся вопросы безопасности, а затем утверждается руководителем организации.

При введении в действие этого положения приказом отдельным пунктом в нем должны определяться должности или лица, которые наделяются полномочиями по отнесению сведений к составляющим служебную или коммерческую тайну в период формирования (разработки) Перечня и по их применению в последующем.

Положение по формированию Перечня обеспечивает единый подход к его созданию, обоснованность принимаемых решений о включении в него сведений за структурное подразделение в отдельности и за организацию в целом, а также проведение административного расследования в случае несанкционированного распространения (разглашения, передачи, утечки, хищения) сведений, составляющих конфиденциальный характер и наказание лиц, виновных в этом, согласно Уголовному или Гражданскому Кодексу РФ.

В Перечень включаются все сведения (данные, информация, документы и их носители), являющиеся собственностью организации. В ходе подготовки Перечня должностные лица организации должны провести анализ всех сторон ее деятельности с целью определения конкретных сведений, разглашение которых может нанести ущерб ее собственнику и владельцу.

Сведения, составляющие служебную или коммерческую тайну о деятельности организации, по степени (характеру) важности должны разделяться на сведения конфиденциального и коммерческого характера (отметка «Конфиденциально» или «Из офиса не выносить»), а также служебные сведения, имеющие гриф «Для служебного пользования».

При этом: а) Под сведениями (и их носителями) понимаются:

• данные, полученные в результате обработки информации с помощью технических средств (оргтехники);

• информация как часть данных, несущая в себе полезные сведения и используемая сотрудниками организации для работы в служебных целях;

• документы (носители), образующиеся в результате мыслительной деятельности сотрудников организации, включающие сведения любого происхождения, вида и назначения, но необходимые для нормального функционирования организации.

б) Сведения, включенные в Перечень, имеют ограничительный характер на использование (применение).

Ограничения, вводимые на использование сведений, составляющих служебную или коммерческую тайну, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при организации трудовой деятельности работников (персонала) ее подразделений, а также при их сотрудничестве с работниками других предприятий.

в) В совокупности под служебной или коммерческой тайной надо понимать сведения, не являющиеся государственными секретами, но которые связаны, прежде всего, с производственной, управленческой, финансовой или другой экономической деятельностью организации, разглашение (передача, утечка, хищение) которой может нанести ущерб ее интересам или интересам их владельцев.

г) Законодательной основой защиты служебной и коммерческой тайны является часть вторая Гражданского Кодекса РФ.

Для работы по составлению Перечня должен привлекаться широкий круг экспертов и должностных лиц отделов, служб организации с тем, чтобы ни одно из возможных направлений ее деятельности не было упущено при его разработке. Руководство работой по формированию Перечня, как правило, должно возлагаться на начальника службы безопасности (заместителя по режиму) организации. Для непосредственного формирования Перечня в организации должна создаваться ЭК, комплектуемая наиболее квалифицированными сотрудниками и специалистами из ее структурных подразделений. ЭК должна осуществлять анализ всех сторон деятельности организации в целом и подчиненных ему подразделений в отдельности, а также координировать вопросы, касающиеся их совместных действий по формированию Перечня, путем обобщения поступающих предложений.

Работа по формированию Перечня и определению сведений, составляющих служебную или коммерческую тайну, должна состоять из следующих этапов:

• составление предварительного перечня сведений, содержащих служебную или коммерческую тайну, для структурных подразделений;

• определение возможного ущерба, наступающего в результате несанкционированного распространения сведений, включаемых в Перечень;

• определение преимуществ открытого использования рассматриваемых сведений по сравнению с закрытым;

• определение затрат на защиту рассматриваемых сведений;

• принятие решения о включении сведений в окончательный вариант Перечня;

• составление обобщенного Перечня и рассмотрение его на заседании ЭК;

• оформление результатов работы по формированию Перечня.

Результаты работы ЭК должны оформляться в виде окончательного варианта обобщенного Перечня, подписанного начальником службы безопасности (заместителем по режиму) и представляемого председателем ЭК на утверждение руководителю организации. К окончательному варианту обобщенного Перечня могут прилагаться рабочие материалы с обоснованием необходимости включения в него тех или иных сведений. Такие материалы должны подписываться всеми членами ЭК.

Сведения, отнесенные к служебной или коммерческой тайне, должны включаться в обобщенный Перечень с указанием грифа конфиденциальности и сроков их засекречивания. Вместо указания срока засекречивания могут приводиться обстоятельства или события, при наступлении которых возникает необходимость изменения грифа конфиденциальности или полного открытия сведения, включенного в Перечень.

Решение об открытии (рассекречивании) такого сведения принимается руководителем организации или ЭК. При этом необходимо учитывать, что одинаковый гриф конфиденциальности и сроки засекречивания должны устанавливаться на все сведения в совокупности при указании через союз “и”, а также на все категории сведений в совокупности или в отдельности при указании через запятую и союзы “или”, “либо”, “а также”.

Результаты расширенного заседания ЭК должны протоколироваться секретарем комиссии, а протокол — утверждаться руководителем организации. Перечень вводится в действие приказом руководителя организации в виде приложения к нему.

Сотрудники организации, допускаемые по роду деятельности или функциональным обязанностям к сведениям, составляющим служебную или коммерческую тайну, должны под расписку ознакомиться с этим приказом или приложением. Порядок такого ознакомления возлагается на начальника службы безопасности организации. В заинтересованные организации, учреждения, а также подчиненные структурные подразделения высылаются выписки или копии этих сведений в части, их касающейся.

В Перечень могут быть включены сведения служебного, коммерческого или конфиденциального характера сторонних организаций. Степень конфиденциальности таких сведений должна устанавливаться по согласованию между организацией, разрабатывающей такой Перечень, и собственником таких сведений.

Контроль за обеспечением защиты служебной или коммерческой тайны и правильностью пользования Перечнем в практической деятельности должен возлагаться на начальника службы безопасности (заместителя по режиму) организации. Вопросы организации такого контроля, как правило, должны отражаться в годовом плане мероприятий по защите служебной или коммерческой тайны.

В последующем Перечень дифференцированно должен доводиться не реже 1 раза в год до всех сотрудников организации, которые используют в своей работе частично или в полном объеме сведения, информацию, данные или работают с документами “Для служебного пользования» и их носителями. Все лица, принимаемые на работу в организацию, должны пройти инструктаж и ознакомиться с памяткой о сохранении служебной или коммерческой тайны.

Памятка должна разрабатываться службой безопасности с учетом специфики организации. Гриф конфиденциальности самого Перечня устанавливается руководителем организации при его утверждении

Задание: 1.Найти в Интернет Перечни сведений, составляющих конфиденциальный характер. Сравнить их и выявить общие и обязательные моменты.

2.Разбиться на группы и разработать свой «Документ о порядке и методических указаниях по формированию Перечня сведений, составляющих конфиденциальный характер» по аналогии для любого предприятия.

3.Обсудить свой «Документ о порядке и методических указаниях по формированию Перечня сведений, составляющих конфиденциальный характер» с другими группами и исправить недочеты

4. Составление заключения служебной проверки (Приложение):

получение информации о нарушении информационной безопасности объекта;

сбор документов, раскрывающих причины нарушения информационной безопасности объекта;

выработка мероприятий, направленных на управление рисками;

предложения по принятию мер к нарушителям информационной безопасности объекта.

Вопросы.

1. Какие должности наделяются полномочиями по отнесению сведений к составляющим служебную или коммерческую тайну в период формирования и разработки Перечня?

2. Какие наказания предусмотрены Уголовным или Гражданским Кодексом РФ в случае несанкционированного распространения (разглашения, передачи, утечки, хищения) сведений, составляющих конфиденциальный характер?

3. Что понимается под ограничительным характером на использование (применение) сведений, включенные в Перечень?

4. Перечислите этапы работ по формированию Перечня и определению сведений, составляющих служебную или коммерческую тайну.

Приложение

Утверждаю

_____
(руководитель предприятия)

«___» _____ 200_ г.

Заключение

по факту _____

_____
(формулировка факта нарушения)

_____ рассмотрев материал
(должность, ФИО проводившего проверку)

служебной проверки по факту _____,
(формулировка нарушения)

установил:

_____
_____
_____
_____
_____
_____
_____
(описываются установленные факты нарушения информационной безопасности)

На основании изложенного,

полагал бы:

_____
_____
_____
_____

_____

(предлагаются меры по управлению рисками, меры по недопущению подобных случаев впредь и меры воздействия на нарушителей информационной безопасности объекта)

Должность, подпись составителя заключения.

Практическая работа № 6.

Тема: Разработка и ведение перечня сведений, составляющих конфиденциальный характер.

Цель: изучить правила разработки и ведения перечня сведений, составляющих конфиденциальный характер.

Документ о порядке и методических указаниях по формированию Перечня сведений, составляющих конфиденциальный характер, должен разрабатываться в организации в виде отдельного положения, которое подписывается начальником службы безопасности (заместителем по режиму) или другим должностным лицом, в ведении которого находятся вопросы безопасности, а затем утверждается руководителем организации.

При введении в действие этого положения приказом отдельным пунктом в нем должны определяться должности или лица, которые наделяются полномочиями по отнесению сведений к составляющим служебную или коммерческую тайну в период формирования (разработки) Перечня и по их применению в последующем.

Положение по формированию Перечня обеспечивает единый подход к его созданию, обоснованность принимаемых решений о включении в него сведений за структурное подразделение в отдельности и за организацию в целом, а также проведение административного расследования в случае несанкционированного распространения (разглашения, передачи, утечки, хищения) сведений, составляющих конфиденциальный характер и наказание лиц, виновных в этом, согласно Уголовному или Гражданскому Кодексу РФ.

В Перечень включаются все сведения (данные, информация, документы и их носители), являющиеся собственностью организации. В ходе подготовки Перечня должностные лица организации должны провести анализ всех сторон ее деятельности с целью определения конкретных сведений, разглашение которых может нанести ущерб ее собственнику и владельцу.

Сведения, составляющие служебную или коммерческую тайну о деятельности организации, по степени (характеру) важности должны разделяться на сведения конфиденциального и коммерческого характера (отметка «Конфиденциально» или «Из офиса не выносить»), а также служебные сведения, имеющие гриф «Для служебного пользования». При этом:

а) Под сведениями (и их носителями) понимаются:

• данные, полученные в результате обработки информации с помощью технических средств (оргтехники);

• информация как часть данных, несущая в себе полезные сведения и используемая сотрудниками организации для работы в служебных целях;

• документы (носители), образующиеся в результате мыслительной деятельности сотрудников организации, включающие сведения любого происхождения, вида и назначения, но необходимые для нормального функционирования организации.

б) Сведения, включенные в Перечень, имеют ограничительный характер на использование (применение). Ограничения, вводимые на использование сведений, составляющих служебную или коммерческую тайну, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при организации трудовой деятельности работников (персонала) ее подразделений, а также при их сотрудничестве с работниками других предприятий.

в) В совокупности под служебной или коммерческой тайной надо понимать сведения, не являющиеся государственными секретами, но которые связаны, прежде всего, с производственной, управленческой, финансовой или другой экономической деятельностью организации, разглаше-

ние (передача, утечка, хищение) которой может нанести ущерб ее интересам или интересам их владельцев.

г) Законодательной основой защиты служебной и коммерческой тайны является часть вторая Гражданского Кодекса РФ.

Для работы по составлению Перечня должен привлекаться широкий круг экспертов и должностных лиц отделов, служб организации с тем, чтобы ни одно из возможных направлений ее деятельности не было упущено при его разработке.

Руководство работой по формированию Перечня, как правило, должно возлагаться на начальника службы безопасности (заместителя по режиму) организации.

Для непосредственного формирования Перечня в организации должна создаваться ЭК, комплектуемая наиболее квалифицированными сотрудниками и специалистами из ее структурных подразделений. ЭК должна осуществлять анализ всех сторон деятельности организации в целом и подчиненных ему подразделений в отдельности, а также координировать вопросы, касающиеся их совместных действий по формированию Перечня, путем обобщения поступающих предложений.

Работа по формированию Перечня и определению сведений, составляющих служебную или коммерческую тайну, должна состоять из следующих этапов:

- составление предварительного перечня сведений, содержащих служебную или коммерческую тайну, для структурных подразделений;
- определение возможного ущерба, наступающего в результате несанкционированного распространения сведений, включаемых в Перечень;
- определение преимуществ открытого использования рассматриваемых сведений по сравнению с закрытым;
- определение затрат на защиту рассматриваемых сведений;
- принятие решения о включении сведений в окончательный вариант Перечня;
- составление обобщенного Перечня и рассмотрение его на заседании ЭК;
- оформление результатов работы по формированию Перечня.

Результаты работы ЭК должны оформляться в виде окончательного варианта обобщенного Перечня, подписанного начальником службы безопасности (заместителем по режиму) и представляемого председателем ЭК на утверждение руководителю организации. К окончательному варианту обобщенного Перечня могут прилагаться рабочие материалы с обоснованием необходимости включения в него тех или иных сведений. Такие материалы должны подписываться всеми членами ЭК.

Сведения, отнесенные к служебной или коммерческой тайне, должны включаться в обобщенный Перечень с указанием грифа конфиденциальности и сроков их засекречивания.

Вместо указания срока засекречивания могут приводиться обстоятельства или события, при наступлении которых возникает необходимость изменения грифа конфиденциальности или полного открытия сведения, включенного в Перечень.

Решение об открытии (рассекречивании) такого сведения принимается руководителем организации или ЭК. При этом необходимо учитывать, что одинаковый гриф конфиденциальности и сроки засекречивания должны устанавливаться на все сведения в совокупности при указании через союз “и”, а также на все категории сведений в совокупности или в отдельности при указании через запятую и союзы “или”, “либо”, “а также”.

Результаты расширенного заседания ЭК должны протоколироваться секретарем комиссии, а протокол — утверждаться руководителем организации. Перечень вводится в действие приказом руководителя организации в виде приложения к нему.

Сотрудники организации, допускаемые по роду деятельности или функциональным обязанностям к сведениям, составляющим служебную или коммерческую тайну, должны под расписку ознакомиться с этим приказом или приложением. Порядок такого ознакомления возлагается на начальника службы безопасности организации. В заинтересованные организации, учреждения, а также подчиненные структурные подразделения высылаются выписки или копии этих

сведений в части, их касающейся. В Перечень могут быть включены сведения служебного, коммерческого или конфиденциального характера сторонних организаций.

Степень конфиденциальности таких сведений должна устанавливаться по согласованию между организацией, разрабатывающей такой Перечень, и собственником таких сведений.

Контроль за обеспечением защиты служебной или коммерческой тайны и правильностью пользования Перечнем в практической деятельности должен возлагаться на начальника службы безопасности (заместителя по режиму) организации. Вопросы организации такого контроля, как правило, должны отражаться в годовом плане мероприятий по защите служебной или коммерческой тайны.

В последующем Перечень дифференцированно должен доводиться не реже 1 раза в год до всех сотрудников организации, которые используют в своей работе частично или в полном объеме сведения, информацию, данные или работают с документами "Для служебного пользования» и их носителями. Все лица, принимаемые на работу в организацию, должны пройти инструктаж и ознакомиться с памяткой о сохранении служебной или коммерческой тайны. Памятка должна разрабатываться службой безопасности с учетом специфики организации.

Гриф конфиденциальности самого Перечня устанавливается руководителем организации при его утверждении.

Задание:

1.Найти в Интернет Перечни сведений, составляющих конфиденциальный характер.

2.Сравнить их и выявить общие и обязательные моменты.

3.Разбиться на группы и разработать свой «Документ о порядке и методических указаниях по формированию Перечня сведений, составляющих конфиденциальный характер» по аналогии для любого предприятия.

4.Обсудить свой «Документ о порядке и методических указаниях по формированию Перечня сведений, составляющих конфиденциальный характер» с другими группами и исправить недочеты.

Вопросы для самоконтроля:

1. Какие должности наделяются полномочиями по отнесению сведений к составляющим служебную или коммерческую тайну в период формирования и разработки Перечня?

2. Какие наказания предусмотрены Уголовным или Гражданским Кодексом РФ в случае несанкционированного распространения (разглашения, передачи, утечки, хищения) сведений, составляющих конфиденциальный характер?

3. Что понимается под ограничительным характером на использование (применение) сведений, включенные в Перечень?

4. Перечислите этапы работ по формированию Перечня и определению сведений, составляющих служебную или коммерческую тайну.

Практическая работа № 7.

Тема: Проверка наличия конфиденциальных дел и носителей информации.

Цель: Ознакомить с особенностями проверки наличия конфиденциальных документов, дел и носителей информации.

Обеспечение сохранности материальных носителей информации с грифом «коммерческая тайна»:

- За сохранность документа с грифом «коммерческая тайна» отвечает сотрудник, которому данный документ выдан под расписку для работы или хранения.
- В структурных подразделениях материальные носители информации, составляющей коммерческую тайну, выдаются исполнителям и принимаются от них ответственными за конфиденциальное делопроизводство. При получении документа исполнитель должен сверить регистрационный номер документа с учетным номером и экземпляром в журнале, проверить количество листов и после этого поставить в карточке учета выдачи документа (дела) подпись и дату. При возврате документа исполнителем, ответственный производит аналогичную сверку, как и при вы-

даче документа, и в присутствии исполнителя в соответствующей графе карточки учета выдачи документа (дела) ставит свою роспись и дату возврата документа.

• Передача материальных носителей информации между структурными подразделениями производится через ответственных за конфиденциальное делопроизводство.

• Запрещается выносить материальные носители информации, составляющей коммерческую тайну, из здания для работы с ними на дому, в гостинице и т. д.

• Сотрудникам, убывающим в командировку, материальные носители информации, составляющей коммерческую тайну, выдаются на основании письменного указания руководителя структурного подразделения в определенном порядке. Данные сотрудники несут персональную ответственность за соблюдение в отношении полученных материальных носителей информации режима коммерческой тайны и их сохранность с момента расписки в их получении и до момента сдачи их ответственному за конфиденциальное делопроизводство.

• Материальные носители информации с грифом «коммерческая тайна» должны храниться в надежно запираемых металлических шкафах (сейфах), оснащенных устройствами, исключающими их несанкционированное вскрытие (механические и электронные кодовые замки, устройства для опечатывания и т.д.).

• В помещениях, предназначенных для хранения материальных носителей информации, составляющей коммерческую тайну, должна быть обеспечена возможность их эвакуации в случае возникновения пожара и стихийных бедствий. Данные помещения должны быть оснащены средствами наблюдения и пожаротушения, охранной и пожарной сигнализацией.

Проверки соблюдения режима коммерческой тайны в подразделениях могут быть плановыми и внеплановыми. Плановым проверкам подвергаются все структурные подразделения (управления, самостоятельные отделы) один раз в год согласно «Плана-графика проведения проверок режима коммерческой тайны в ОАО «Амуроблгаз»», согласованного с начальниками структурных подразделений и утвержденного Генеральным директором. Внеплановые проверки могут проводиться в любой рабочий день в течение календарного года согласно «Предписания на проведение проверки режима коммерческой тайны», подписанного начальником службы безопасности.

Проверка архива Общества проводится не реже одного раза в три года комиссией, назначаемой приказом Генерального директора. Для проведения проверки советником генерального директора по безопасности назначается комиссия в составе сотрудников Управления безопасности и одного из членов Комиссии по проверке сохранности документов, дел и других материальных носителей информации, составляющей коммерческую тайну, не являющегося сотрудником проверяемого структурного подразделения, согласно графику очередности. Комиссия по проверке сохранности документов, дел и других материальных носителей информации, составляющей коммерческую тайну, в структурных подразделениях назначается приказом Генерального директора. При проведении проверки подразделения член указанной Комиссии не должен являться сотрудником проверяемого подразделения.

Плановая проверка включает в себя:

• проверку наличия материальных носителей информации с грифом «коммерческая тайна», зарегистрированных в структурном подразделении;

• проверку обоснованности присвоения материальным носителям информации грифа «коммерческая тайна»;

• проверку правильности ведения конфиденциального делопроизводства и наличия необходимых нормативных и учетных документов;

• проверку соблюдения сотрудниками структурных подразделения требований установленного режима коммерческой тайны;

• проверку знания сотрудниками структурного подразделения положений настоящей Инструкции и Перечня, регламентирующих порядок работы с КИ;

• проверку соблюдения порядка хранения материальных носителей информации с грифом «коммерческая тайна», зарегистрированных в структурном подразделении.

По результатам проверки составляется «Акт проведения проверки соблюдения режима коммерческой тайны» в произвольной форме. В акте отражается подробный перечень обнаруженных недостатков по всем проверяемым вопросам. Акт подписывается всеми членами комиссии, предоставляется руководству проверяемого структурного подразделения для ознакомления и утверждается руководством. Не позднее пяти рабочих дней с момента окончания работы комиссии руководитель проверяемого структурного подразделения представляет советнику генерального директора по безопасности план устранения недостатков с указанием сроков их устранения. По результатам проверки советником генерального директора безопасности составляется служебная записка на имя Генерального директора, к которой прилагаются «Акт проведения проверки…» и план устранения недостатков. Недостатки должны быть устранены в срок не позднее одного месяца с момента принятия Генеральным директором решения по результатам проверки.

Проведение служебных расследований по фактам разглашения или утраты информации, составляющей коммерческую тайну:

• Обо всех случаях разглашения или утраты информации, составляющей коммерческую тайну и обстоятельствах, которые могут к таковым привести сотрудник обязан немедленно докладывать руководителю своего структурного подразделения. Руководитель безотлагательно информирует о происшествии начальника службы безопасности для принятия совместных с данным управлением мер с целью предотвращения неблагоприятного развития ситуации. Руководители этих подразделений так же незамедлительно докладывают о происшествии лично Генеральному директору и составляют служебную записку на его имя, содержащую полную информацию о происшествии и перечень планируемых и проведенных мероприятий по предотвращению негативных последствий данного происшествия.

• На основании приказа Генерального директора начальнику службы безопасности проводится служебное расследование, результаты которого докладываются Генеральному директору начальником службы безопасности лично. Дальнейшие мероприятия проводятся в соответствии с решением Генерального директора, принятого по результатам служебного расследования, в порядке, определенном законодательством РФ.

• Для оказания помощи в проведении служебного расследования по фактам разглашения или утраты информации, составляющей коммерческую тайну и мероприятий по предотвращению негативных последствий данного происшествия начальник Управления безопасности вправе привлекать любого специалиста по согласованию с руководителем структурного подразделения.

Задание:

1. Рассмотреть общие правила проведения плановых и неплановых проверок.
2. Обсудить, как человеческий фактор может сказаться на хранении конфиденциальных документов.
3. Определить угрозы конфиденциальных документов в процессе хранения.
4. Обсудить, порядок проведения служебных расследований по фактам разглашения или утраты информации, составляющей коммерческую тайну.

Вопросы для самоконтроля:

1. Для чего проводится плановая проверка в подразделениях?
2. С какой целью проводится внеплановая проверка?
3. В чем заключается проверка архива конфиденциальных документов?
4. Какие особенности имеет заполнение «Акта проведения проверки…»?

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ СТУДЕНТОВ

Самостоятельная работа является одним из видов учебной деятельности обучающихся, способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Самостоятельная работа проводится с целью:

– систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
– углубления и расширения теоретических знаний;
– формирования умений использовать специальную литературу;
– развития познавательных способностей и активности обучающихся: творческой инициативы, ответственности и организованности;
– формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
– развития исследовательских умений.

Аудиторная самостоятельная работа по учебной дисциплине на учебных занятиях под непосредственным руководством преподавателя и по его заданию. Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференцированный характер, учитывать специфику изучаемой учебной дисциплины, индивидуальные особенности обучающегося.

Контроль самостоятельной работы и оценка ее результатов организуется как единство двух форм:
- самоконтроль и самооценка обучающегося;
- контроль и оценка со стороны преподавателя.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Основными видами аудиторной самостоятельной работы являются:
– выполнение лабораторных и практических работ по инструкциям; работа с литературой и другими источниками информации, в том числе электронными;
– само- и взаимопроверка выполненных заданий;
– решение проблемных и ситуационных задач.

Выполнение лабораторных и практических работ осуществляется на лабораторных и практических занятиях в соответствии с графиком учебного процесса. Для обеспечения самостоятельной работы преподавателями разрабатываются методические указания по выполнению лабораторной/практической работы.

Работа с литературой, другими источниками информации, в т.ч. электронными может реализовываться на семинарских и практических занятиях. Данные источники информации могут быть представлены на бумажном и/или электронном носителях, в том числе, в сети Internet. Преподаватель формулирует цель работы с данным источником информации, определяет время на проработку документа и форму отчетности.

Само и взаимопроверка выполненных заданий чаще используется на семинарском, практическом занятии и имеет своей целью приобретение таких навыков как наблюдение, анализ ответов сокурсников, сверка собственных результатов с эталонами.

Решение проблемных и ситуационных задач используется на лекционном, семинарском, практическом и других видах занятий. Проблемная/ситуационная задача должна иметь четкую формулировку, к ней должны быть поставлены вопросы, ответы на которые необходимо найти и обосновать. Критерии оценки правильности решения проблемной/ситуационной задачи должны быть известны всем обучающимся.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия.

При предъявлении видов заданий на внеаудиторную самостоятельную работу рекомендуется использовать дифференцированный подход к уровню подготовленности обучающегося. Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит консультацию с определением цели задания, его содержания, сроков выполнения, ориентировочного объема работы, основных требований к результатам работы, критериев оценки, форм контроля и перечня ли-

тературы. В процессе консультации преподаватель предупреждает о возможных типичных ошибках, встречающихся при выполнении задания.

Ежедневно обучающийся должен уделять выполнению внеаудиторной самостоятельной работы в среднем не менее 3 часов.

При выполнении внеаудиторной самостоятельной работы обучающийся имеет право обращаться к преподавателю за консультацией с целью уточнения задания, формы контроля выполненного задания.

Контроль результатов внеаудиторной самостоятельной работы студентов может проводиться в письменной, устной или смешанной форме с представлением продукта деятельности обучающегося. В качестве форм и методов контроля внеаудиторной самостоятельной работы могут быть использованы зачеты, тестирование, самоотчеты, контрольные работы, защита творческих работ и др.

Итоговый контроль – проводятся на основании перечней вопросов, представленных в рабочей программе. Подготовка к нему заключается в изучении и тщательной проработке студентом конспектов по всем видов занятий в соответствии с перечнем вопросов, представленном в рабочей программе дисциплины. Подготовку к контролю требуется начинать с просмотра перечня всех вопросов с целью оценки требуемого объема учебного материала, логики и структуры построения курса. С учетом накопленных за семестр знаний студент должен запланировать распределение времени на подготовку. Желательно зарезервировать время для повторения материала. Работа над каждым из вопросов рекомендуется прочитать конспект лекции, дополнительно прочитать рекомендованный учебник, если материал трудно усваивается.

ЛИТЕРАТУРА

1. Аверченков В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 c.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks»

2. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 186 c.— Режим доступа: http://www.iprbookshop.ru/7008.— ЭБС «IPRbooks»

3. Аверченков В.И. Системы организационного управления [Электронный ресурс]: учебное пособие/ Аверченков В.И., Ерохин В.В.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 208 c.— Режим доступа: http://www.iprbookshop.ru/7013.— ЭБС «IPRbooks»

4. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c.— Режим доступа: http://www.iprbookshop.ru/52160.— ЭБС «IPRbooks»

5. Новиков С.Н. Методы защиты информации [Электронный ресурс]: учебное пособие/ Новиков С.Н., Солонская О.И.— Электрон. текстовые данные.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009.— 121 c.— Режим доступа: http://www.iprbookshop.ru/54767.— ЭБС «IPRbooks»

6. Качановский Ю.П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс]: методические указания к проведению лабораторной работы по курсу «Информатика»/ Качановский Ю.П., Широков А.С.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 24 c.— Режим доступа: http://www.iprbookshop.ru/55120.— ЭБС «IPRbooks»

7. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государ-

ственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.— ЭБС «IPRbooks»

8. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

9. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.— ЭБС «IPRbooks»

СОДЕРЖАНИЕ