МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Часть 1: Организационное обеспечение информационной безопасности

Методические материалы

Рекомендованы учебно-методической комиссией специальности 10.05.03 Информационная безопасность автоматизированных систем в качестве электронного издания для использования в образовательном процессе

Кемерово 2018

Рецензенты

Стенин Д. В. – кандидат технических наук, доцент директор ИИТМА

Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна
Чичерин Иван Владимирович
Организационное и правовое обеспечение информационной безопасности. Часть 1: Организационное обеспечение информационной безопасности: методические материалы [Электронный ресурс] для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Электрон. издан. – Кемерово, 2018.

1. Организационное обеспечение информационной безопасности.
1.1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности

Заключая рассмотрение правовых проблем информационной безопасности, отметим, что информационную безопасность можно рассматривать как аспект или ракурс изучения и формирования системы информационного права, подготовки и совершенствования норм и нормативных правовых актов этой отрасли.

Используя результаты исследования в области информационной безопасности, законодатель и исследователь отрасли информационного права получают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Тем самым существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере. В этой связи структура правового регулирования отношений в области информационной безопасности как бы повторяет структуру самого информационного законодательства, акцентируя внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности. В итоге можно построить некоторую модель основных направлений защиты объектов информационной сферы и институтов информационного законодательства, с помощью нормативных предписаний которых решается проблема правового обеспечения защиты их информационной безопасности.

Основные направления защиты информационной сферы		
Защита интересов личности, общества, государства от воздействия вредной, опасной, недоброкачественной информации	Защита информации, информационных ресурсов и информационных систем от неправомерного воздействия посторонних лиц	Защита информационных прав и свобод
Институт массовой информации Институт документированной информации Нормы УК РФ Нормы КоАП РСФСР	Институт документированной информации Институт государственной тайны Институт коммерческой тайны Институт персональных данных Другие виды тайн Нормы УК РФ Нормы КоАП РСФСР Нормы ГК РФ	Институты интеллектуальной собственности Институт документированной информации Нормы УК РФ Нормы КоАП РСФСР Нормы ГК РФ

Правовое регулирование информационной безопасности формируется на базе информационных правоотношений, охватывающих все; направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений. Объекты правоотношений в области информационной безопасности – это духов-

ность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства. Субъектами правоотношений в области информационной безопасности выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане. Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений. Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности.

Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.

Ответственность за правонарушения в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной информации и дезинформации; защиты личности в условиях информатизации; защиты информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения. Правовые механизмы защиты жизненно важных интересов личности, общества, государства должны разрабатываться и внедряться в каждой из областей информационной сферы.

1. Область поиска, получения и потребления информации. Объекты правоотношений: духовность и нравственность гражданина, общества, государства (от воздействия недостоверной, ложной, вредной информации); информационные права и свободы человека и гражданина (право на получение и использование информации); честь и достоинство гражданина (в связи с созданием и распространением недостоверной информации или несанкционированным распространением личной информации о нем). Субъекты правоотношений: человек и гражданин, потребитель информации, редакция.

2. Область создания (производство) исходной и производной информации. Объекты правоотношений: информация как интеллектуальная собственность; документированная информация как интеллектуальная и вещная собственность. Субъекты правоотношений: человек и гражданин, авторы, пользователи исключительных прав, издатели, потребители информации, органы государственной власти и местного самоуправления, органы и системы обеспечения защиты объектов информационной безопасности.

3. Область формирования информационных ресурсов, подготовки и предоставления пользователям информационных продуктов, информационных услуг. Объекты правоотношений: право авторства и собственности на информационные ресурсы; информационные ресурсы на всех видах носителей, в том числе содержащие информацию ограниченного доступа. Субъекты правоотношений: человек и гражданин, автор, пользователь, потребитель, участники самостоятельного оборота информации.

4. Область создания и применения информационных систем, технологий и средств их обеспечения. Объекты правоотношений: автоматизированные информационные системы, базы и банки данных, другие информационные технологии, средства обеспечения этих объектов.

При этом, прежде всего, должны защищаться:

• права авторов и собственников информационных систем и технологий, средств их обеспечения;

• машинные носители с информацией, например, средствами электронной цифровой подписи; базы данных (знаний) в составе автоматизированных информационных систем и их сетей от несанкционированного доступа;

• программные средства в составе ЭВМ, их сетей, информационные системы и их сети от несанкционированного доступа;

• информационные технологии и средства их обеспечения. Субъекты правоотношений: создатели, производители, заказчики, исполнители.

Доктрина информационной безопасности России

Базовым документом по информационной безопасности в России является утвержденная Президентом **Доктрина информационной безопасности** Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина понимает под информационной безопасностью Российской Федерации состояние защищенности национальных интересов России в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности: реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающей личную безопасность.

Интересы общества: обеспечение интересов личности, упрочение демократии, создание правового социального государства, достижение и поддержание общественного согласия, духовное обновление России.

***Интересы государства*:** создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и со-

циальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Доктриной выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы национальным интересам Российской Федерации в данных сферах признаются Доктриной угрозами информационной безопасности:

1. *Соблюдение конституционных прав и свобод человека и гражданина* в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

2. *Информационное обеспечение государственной политики* Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

3. *Развитие современных информационных технологий, отечественной индустрии информации*, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

4. *Защита* информационных ресурсов *от несанкционированного доступа*, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

Направления регулирования в сфере информационной безопасности

Законодательство России в сфере информационной безопасности развивается по следующим направлениям:

- закрепление общих положений о доступе к информации, о конфиденциальности и защите информации. Базовым актом здесь является Федеральный закон «Об информации, информационных технологиях и защите информации»;
- определение правового режима отдельных видов информации:
- персональных данных – Федеральный закон «О персональных данных»
- семейной тайны и тайны личной жизни – Гражданский и Семейный кодексы
- государственной тайны – Закон РФ «О государственной тайне»
- коммерческой тайны – Гражданский кодекс РФ и Федеральный закон «О коммерческой тайне»
- профессиональных, процессуальных тайн – процессуальными кодексами и законами о соответствующих видах деятельности (об адвокатуре, нотариате, охране здоровья граждан и т. п.);
- административное регулирование деятельности по защите информации, в том числе связанной с оборотом криптографических средств;
- определение порядка осуществления оперативно-розыскных мероприятий в информационной сфере;
- борьба с преступлениями в сфере информационной безопасности путем закрепления соответствующих составов преступлений в Уголовном кодексе РФ.

Ограничение доступа к информации, конфиденциальность и защита информации

Правовой режим информации в России определяется Федеральным законом «Об информации, информационных технологиях и защите информации». Данный закон классифицирует информацию по двум основаниям.

Информация в зависимости от порядка ее **предоставления или распространения** подразделяется законом на:

1) информацию, свободно распространяемую;
2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает, что информация в зависимости от категории **доступа** к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). На практике, конечно же, есть и третья категория информации: доступ к которой не ограничен федеральным законом, однако обладатель которой принимает меры по обеспечению ее конфиденциальности. В то же время, в законе установлена формальная презумпция общедоступности информации: информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Закон не выделяет отдельной категории **конфиденциальной информации**. Конфиденциальность информации понимается лишь как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. В то же время, закон предусматривает, что обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Таким образом, базовая категория «информация ограниченного доступа» входит в более широкую категорию конфиденциальной информации (информации, в отношении которой установлено требование о соблюдении ее конфиденциальности).

1.2. Правовой режим защиты государственной тайны и информации ограниченного доступа

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Правовую основу института государственной тайны составляют законы РФ «О безопасности», «О государственной тайне», Федеральный закон «Об информации, информатизации и защите информации», указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ, регулирующие отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В области государственной тайны применяются следующие понятия:

государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности российской Федерации»;

носители сведений, составляющих государственную тайну, – материальные объекты, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну;

гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

отнесение сведений к государственной тайне и их засекречивание – введение в предусмотренном законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям;

рассекречивание сведений и их носителей – снятие ранее введенных в предусмотренном законом ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

К органам защиты государственной тайны относятся:

- Межведомственная комиссия по защите государственной тайны;

- органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах);

- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Для государственной тайны устанавливается особый правовой режим – ***режим государственной тайны***, суть которого заключается в жестком ограничении доступа к такой информации, надежной защите ее от несанкционированного доступа и четком определении круга лиц, которым предоставляется доступ к такой информации.

режим государственной тайны определяет:

1) информацию, которая относится к государственной тайне и информацию, которая не может быть отнесена к ней, а также порядок отнесения информации к государственной тайне и степень секретности этих сведений;

2) особый порядок допуска (или доступа) к государственной тайне;

3) порядок рассекречивания государственной тайны;

4) порядок распоряжения сведениями, составляющими государственную тайну;

- порядок обеспечения защиты государственной тайны; ответственность за нарушения режима государственной тайны.

1. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне» в соответствии с принципами законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне предполагает соответствие засекречиваемых сведений требованиям законодательства РФ о государственной тайне.

Обоснованность отнесения сведений к государственной тайне заключается в установлении целесообразности их засекречивания исходя из баланса жизненно важных интересов государства, общества и граждан.

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

Государственную тайну составляют:

• *сведения в военной области* (например, о содержании планов строительства Вооруженных Сил РФ, документов боевого управления, о направлениях развития вооружения и военной техники, о боевых возможностях образцов вооружения и военной техники, о дислокации, организационной структуре, вооружении и численности войск);

• *сведения в области экономики, науки и техники* (например, о возможностях промышленных предприятий по изготовлению и ремонту вооружения и военной техники, о запасах стратегических видов сырья и материалов, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства, о достижениях науки и техники, работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства);

• *сведения в области внешней политики и экономики* (о внешнеполитической, внешнеэкономической деятельности Российской Федерации, финансовой политике в отношении иностранных государств, преждевременное распространение которых может нанести ущерб безопасности государства);

• *сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности*(например, о силах, средствах, источниках, методах, и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, о лицах, сотрудничающих с органами, осуществляющими такого рода деятельность, о системе шифрованной или кодированной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах защиты секретной информации).

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

• о правовом статусе и деятельности органов государственной власти, органов местного самоуправления, организаций, общественных объединений;

• 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 их должностными лицами.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения таких сведений. Устанавливаются три *степени секретности* сведений, составляющих государственную тайну, и для каждой из них соответствующие *грифы секретности:* «особой важности», «со-

вершенно секретно» и «секретно». Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

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

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

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с Федеральным законом «О государственной тайне», которые несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений действует *межведомственная комиссия по защите государственной тайны*, которая формирует по предложениям органов государственной власти и в соответствии с «Перечнем сведений, *составляющих* государственную тайну», «Перечень сведений, *отнесенных* к государственной тайне». Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

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

• о степени секретности содержащихся в носителе сведений;

• об органе государственной власти (предприятии, учреждении организации), осуществивших засекречивание носителя;

• о регистрационном номере;

• о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

1.3. Правовая охрана результатов интеллектуальной деятельности

Результаты интеллектуальной деятельности

Результаты интеллектуальной деятельности – продукт научной или научно-технической деятельности, содержащий новые знания или решения и зафиксированный на любом информационном носителе.

Интеллектуальная собственность

Интеллектуальная собственность – результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана, в т. ч. произведения науки, литературы и искусства, изобретения, полезные модели, промышленные образцы, программы для ЭВМ, базы данных, топологии интегральных микросхем, секреты производства (ноу-хау), фирменные наименования, товарные знаки и знаки обслуживания.

Интеллектуальные права

Интеллектуальные права – права на интеллектуальную собственность, включающие исключительное право, являющееся имущественным, а в случаях, предусмотренных Гражданским кодексом Российской Федерации, также личные неимущественные права и иные права (право следования, права доступа и другие).

Исключительное право

Исключительное право – гражданин или юридическое лицо, обладающие исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации (правообладатель), вправе использовать такой результат или такое средство по своему усмотрению любым не противоречащим закону способом. Правообладатель может распоряжаться исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации, если действующим законодательством не предусмотрено иное. Правообладатель может по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной деятельности или средства индивидуализации. Отсутствие запрета не считается согласием (разрешением). Другие лица не могут использовать соответствующие результат интеллектуальной деятельности или средство индивидуализации без согласия правообладателя, за исключением случаев, предусмотренных и действующим законодательством. Использование результата интеллектуальной деятельности или средства индивидуализации, если такое использование осуществляется без согласия правообладателя, является незаконным и влечет ответственность, установленную действующим законодательством, за исключением случаев, когда использование результата интеллектуальной деятельности или средства индивидуализации лицами иными, чем правообладатель, без его согласия допускается действующим законодательством.

Направление деятельности

Основными направлениями деятельности, связанными с охранной интеллектуальной собственности в Концерне, являются:

- организация работ по управлению интеллектуальной собственностью Концерна;
- координация деятельности Концерна в области управления и защиты интеллектуальной собственности;
- методическая помощь, связанная с управлением интеллектуальной собственностью всем предприятиям, входящим в интегрированную структуру Концерна.

Проведение единой политики в Концерне в области управления интеллектуальной собственностью организуется генеральным директором через Правление с использованием ресурсов управления по инновациям в лице отдела интеллектуальной собственности и трансфера технологий.

В рамках деятельности Концерна отдел интеллектуальной собственности и трансфера технологий решает следующие задачи:

- разработка и осуществление политики Концерна в области интеллектуальной собственности, направленной на развитие научно-производственной и инновационной деятельности;

- формирование корпоративной системы экономических, правовых и административных механизмов и процедур, обеспечивающих создание, защиту и использование объектов интеллектуальной собственности Концерна;
- обеспечение прав предприятий Концерна на объекты интеллектуальной собственности, создаваемые в результате их деятельности, продвижение и передача этих объектов в сферу реального производства;
- гражданско-правовая и административная защита прав и законных интересов предприятий и их работников в области интеллектуальной собственности;
- создание механизмов для обеспечения внутрикорпоративного и внешнего трансфера технологий;
- создание условий для трансфера технологий.

Правовая охрана результатов интеллектуальной деятельности

Интеллектуальная собственность охраняется законом (пункт 2 статьи 1225 Гражданского Кодекса РФ).

В соответствии с действующим законодательством результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

1) произведения науки, литературы и искусства;
2) программы для электронных вычислительных машин (программы для ЭВМ);
3) базы данных;
4) исполнения;
5) фонограммы;
6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
7) изобретения;
8) полезные модели;
9) промышленные образцы;
10) селекционные достижения;
11) топологии интегральных микросхем;
12) секреты производства (ноу-хау);
13) фирменные наименования;
14) товарные знаки и знаки обслуживания;
15) наименования мест происхождения товаров;
16) коммерческие обозначения.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей.

Действие исключительных прав на изобретения, полезные модели и промышленные образцы на территории Российской Федерации: На территории Российской Федерации признаются исключительные права на изобретения, полезные модели и промышленные образцы, удостоверенные патентами, выданными федеральным органом исполнительной власти по интеллектуальной соб-

ственности, или патентами, имеющими силу на территории Российской Федерации в соответствии с международными договорами Российской Федерации.

Патент на изобретение, полезную модель или промышленный образец

1. Патент на изобретение, полезную модель или промышленный образец удостоверяет приоритет изобретения, полезной модели или промышленного образца, авторство и исключительное право на изобретение, полезную модель или промышленный образец.

2. Охрана интеллектуальных прав на изобретение или полезную модель предоставляется на основании патента в объеме, определяемом содержащейся в патенте формулой изобретения или соответственно полезной модели. Для толкования формулы изобретения и формулы полезной модели могут использоваться описание и чертежи (пункт 2 статьи 1375 и пункт 2 статьи 1376 Гражданского Кодекса РФ).

3. Охрана интеллектуальных прав на промышленный образец предоставляется на основании патента в объёме, определяемом совокупностью его существенных признаков, нашедших отражение на изображениях изделия и приведённых в перечне существенных признаков промышленного образца (пункт 2 статьи 1377 Гражданского Кодекса РФ).

Товарный знак и знак обслуживания

1. На товарный знак, то есть на обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей, признается исключительное право, удостоверяемое свидетельством на товарный знак.

2. Свидетельство на товарный знак удостоверяет приоритет товарного знака и исключительное право на товарный знак в отношении товаров, указанных в свидетельстве.

3. На территории Российской Федерации действует исключительное право на товарный знак, зарегистрированный федеральным органом исполнительной власти по интеллектуальной собственности, а также в других случаях, предусмотренных международным договором Российской Федерации.

Трансфер технологий

Трансфер технологий – основная форма продвижения инноваций.

Трансфер технологий – это взаимодействие между двумя или более партнёрами, где хотя бы один партнёр передаёт свою технологию через ноу-хау, патенты и техническое содействие другому партнёру, который желает внедрить и использовать его для конкретной цели.

Обе стороны должны получить от трансфера технологий пользу на взаимовыгодной основе. Получатель технологии может, например, получить ноу-хау и технологическое преимущество перед конкурентами, а владелец технологии – финансовое преимущество и разработать другие технологические решения для повышения конкурентоспособности, снижения себестоимости или увеличения прибыли.

Трансфер технологий включает в себя:

- передачу патентов на изобретения;
- передачу технологической документации;

- передачу ноу-хау;
- передачу технологических сведений, сопутствующих приобретению или аренде (лизингу) оборудования и машин;
- проведение совместных разработок и исследований;
- организацию совместного производства;
- организацию совместного предприятия.

1.4. Преступления в сфере компьютерной информации

Преступления в сфере компьютерной информации – это предусмотренные статьями [272–274] гл. 28 УК общественно опасные деяния (действия или бездействие), осуществляемые умышленно или по неосторожности, направленные против безопасности компьютерной информации и причиняющие либо способные причинить вред охраняемым законом благам (отношениям собственности, правам личности и т. д.).

Уголовное законодательство России впервые предусмотрело данный вид преступных посягательств на общественную безопасность в УК России 1996 г. Глава 28 этого Кодекса «Преступления в сфере компьютерной информации» состоит из трех статей: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Федеральным законом от 07.12.2011 № 420-ФЗ названные статьи представлены в новой редакции.

Общественная опасность данных преступлений заключается в подрыве компьютерной безопасности общества, информационной безопасности пользователей ЭВМ.

Основной ***объект*** преступных посягательств – безопасность компьютерной информации. Дополнительные объекты – право на информацию ее собственников и владельцев, интересы собственности. Факультативные объекты – личность, ее конституционные права, государственная безопасность.

Предмет посягательств – компьютерная информация на соответствующем электронном носителе.

Объективная сторона составов преступлений выражается деянием, как правило, в форме действия. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в некоторых случаях может быть выражено в бездействии.

По законодательной конструкции составы преступлений являются, как правило, материальными. Преступления окончены (составами) в момент наступления соответствующих материальных общественно опасных последствий: уничтожения, блокирования, модификации, копирования информации (см. ч. 1 ст. 272 УК) или крупного ущерба (см. ч. 2 ст. 272 УК), либо тяжких последствий (см. ч. 4 ст. 272 УК), уничтожения, блокирования, модификации, копирования компьютерной информации (первичное последствие), если этим причинен крупный ущерб или

наступили тяжкие последствия (вторичное последствие) (см. ст. 274 УК). Формально-материальные составы закреплены в ч. 2 и 3 ст. 273 УК.

Состав преступления, предусмотренный ч. 1 ст. 273 УК, имеет формальную конструкцию. Преступление окончено (составом) в момент создания, распространения или использования компьютерной программы либо иной компьютерной информации определенного характера.

Субъект преступных посягательств – физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. Субъект посягательства, предусмотренного ст. 274 УК, наделен дополнительным признаком – доступом к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию. По ч. 3 ст. 272 и ч. 2 ст. 273 УК специальным субъектом может быть виновное лицо по групповому или служебно-профессиональному признакам.

Субъективная сторона составов преступлений характеризуется виной, как правило, в форме умысла. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (см. ст. 274 УК) может произойти и по неосторожности.

На квалификацию деяний по ч. 2 ст. 272 и ч. 2 ст. 273 УК может оказать влияние мотив посягательства – корыстная заинтересованность. Совершение данных преступлений возможно и но иным мотивам (хулиганство, интерес, самоутверждение и т. д.), для достижения определенных целей (удовлетворение интереса, сокрытие совершения другого преступления и пр.), которые не влияют на квалификацию содеянного, но могут быть учтены судом при назначении меры уголовно-правового воздействия на виновного.

Неправомерный доступ к компьютерной информации – это предусмотренное ст. 272 УК умышленное общественно опасное активное поведение, посягающее на безопасность компьютерной информации и причиняющее вред по меньшей мере собственнику или пользователю этой информации.

Общественная опасность преступления заключается в подрыве информационной безопасности общества.

В общем массиве регистрируемой преступности и наказуемости в России неправомерный доступ к компьютерной информации до 2003 г. практически отсутствовал. Так, в 1997–2002 гг. в России по ст. 272 УК осуждено всего 234 человека. Однако в 2003 г. наблюдалось существенное увеличение количества осужденных по данной статье (166 человек). В 2004 г. осужден 121 человек; в 2005 г. – 156 человек; в 2006 г. – 182 человека; в 2007 г. – 147 человек, а в 2008 г. – 318 человек, в 2009 г. – 725 человек, в 2010 г. – 280 человек, а в 2011 г. – 229 человек.

Статья 272 УК состоит из четырех частей, отражающих основной (см. ч. 1), квалифицированный (см. ч. 2) и особо квалифицированные (см. ч. 3, 4) составы преступления и выражающих умышленные деяния, относящиеся к категории преступлений небольшой (см. ч. 1), средней (см. ч. 2 и 3) тяжести, а также тяжких

преступлений (см. ч. 4). В двух присоединенных к статье примечаниях определены понятия «компьютерная информация» (1) и «крупный ущерб» (2).

Деяние, отягощенное квалифицирующими обстоятельствами, ответственность за которое предусмотрена ч. 2 статьи, следовало бы отнести к категории преступлений средней тяжести, а состав преступления именовать квалифицированным. Однако санкция нормы, закрепленная в ч. 2, обращает на себя внимание недостаточно качественной юридической конструкцией, о которой свидетельствуют слова «либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок». Согласно букве закона речь идет о возможности назначения наказания в виде лишения свободы на срок до шести месяцев. Вместе с тем системное (см. ч. 1 и 2 статьи) и логическое толкование данной части нормы позволяет утверждать, что слова «либо лишением свободы на тот же срок» должны следовать за выражением «либо принудительными работами на срок до четырех лет» [слова «либо арестом на срок до шести месяцев» надобно из текста исключить] или должны быть изменены на слова «либо лишением свободы на срок до четырех лет».

Безалаберность законодателя в формулировании указанной части нормы неизбежно приведет правоприменителя к вопросу о подсудности содеянного. Может ли мировой судья разбирать дело о квалифицированном неправомерном доступе к компьютерной информации или это прерогатива федерального суда? Если следовать букве закона (ч. 2 ст. 272 УК) и обратиться к ст. 31 УПК, то напрашивается отрицательный ответ «не может», а если обратиться к ст. 3 Федерального закона от 17.12.1998 № 188-ФЗ «О мировых судьях в Российской Федерации», то явствует положительный ответ «может». Таким образом, требуется безотлагательное вмешательство органов, обладающих правом законодательной инициативы, в исправление ошибки, допущенной законодателем. До исправления этой ошибки правоприменителю необходимо руководствоваться требованием ст. 31 УПК.

Основным ***объектом*** преступного посягательства является информационная безопасность общества. Дополнительные объекты – право на конфиденциальность компьютерной информации, интересы ее собственников и пользователей. Факультативные объекты – иные охраняемые законом интересы пользователей средствами доступа к компьютерной информации.

Предмет посягательства – информация в компьютерных файлах, программах или базах данных, причем не любая, а только охраняемая законом, т. е. доступ к которой (возможность ознакомления, копирования, изменения, уничтожения) ограничен. Данная информация должна содержаться исключительно на электронных носителях.

Объективная сторона составов преступления выражается деянием в форме действия, заключающегося в неправомерном доступе к охраняемой законом компьютерной информации.

Неправомерный доступ к компьютерной информации – это проникновение к охраняемой законом компьютерной информации лица, не имеющего права на вызов таковой, ознакомление с нею и распоряжение ею посредством использова-

ния электронной техники. Неправомерный доступ не должен быть сопряжен с неправомерным завладением средства доступа к информации.

Квалификация содеянного по ст. 272 УК возможна при наступлении соответствующих материальных общественно опасных последствий: уничтожения компьютерной информации, ее блокирования, модификации либо копирования. Таким образом, по законодательной конструкции составы преступления являются материальными. Преступление окончено (составами) не в момент обращения пользователя к средству доставки информации голосом, нажатием клавиши или иным образом, а в момент наступления хотя бы одного из перечисленных последствий.

Уничтожение компьютерной информации – это ликвидация всей информации или ее основных частей, признаков. Способы уничтожения информации:

а) стирание в памяти электронного средства;

б) перенесение информации на другой носитель без сохранения его на прежнем носителе;

в) повреждение электронного носителя, приведшее к полной или частичной утрате информации (оно не должно быть связано с внешним воздействием: механическим, магнитным и пр.), и т. д. Информация считается уничтоженной и в том случае, если утраченную информацию в дальнейшем можно восстановить с помощью программных средств, но нельзя воспроизвести в первоначальном виде на электронном носителе.

Блокирование компьютерной информации – это искусственное (полное или частичное) прекращение доступа пользователя к информации в течение значимого периода, не связанное с ее уничтожением. Значимость указанного промежутка времени определяется фактом нарушения деятельности пользователя, невозможностью выполнения работы с информацией.

Модификация компьютерной информации – это внесение в информацию каких-либо изменений (замены, дополнения, перестановки частей первоначальной информации), искажающих ее и не связанных с адаптацией компьютерной программы.

Копирование компьютерной информации – это получение вопреки установленному законодательством запрету дополнительных аналогичных оригиналу экземпляров компьютерной информации на любые материальные носители.

Некоторые авторы необоснованно сужают понятие «копирование информации», определяя его как «запись компьютерной информации на машинный носитель, в ЭВМ или распечатывание этой информации на средствах ЭВМ». Другие авторы в связи с этим задают резонный вопрос: если под копированием следует понимать перенос информации с машинного носителя только на аналогичный носитель, и не считать таковым фотографирование с экрана дисплея, то как расценивать, в частности, фотографирование экрана на цифровую камеру, т. е. получение того же самого машинного носителя? Думается, что копирование возможно любым способом, обеспечивающим идентичность оригинальной информации, – переписыванием на дискету, на лист бумаги, фотографированием информации с экрана дисплея. Главное, чтобы это было сопряжено с неправомерным доступом к компьютерной информации.

Посредством неправомерного доступа к компьютерной информации возможно совершение, например, таких преступлений, как нарушение неприкосновенности частной жизни (см. ст. 137 УК), тайны сообщений (см. ст. 138 УК), авторских/смежных прав (см. ст. 146 УК), изобретательских/патентных прав (см. ст. 147 УК), хищения (см. ст. 158, 159 УК), незаконное получение кредита (см. ст. 176 УК), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (см. ст. 183 УК), уклонение от уплаты налогов/сборов с организации (см. ст. 199 УК), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (см. ст. 237 УК), создание, использование рі распространение вредоносных компьютерных программ (см. ст. 273 УК), преступления против основ конституционного строя и безопасности государства (см. ст. 275, 276, 281 УК). В указанных случаях квалификация совершенных преступных деяний должна осуществляться по какой-либо из перечисленных статей и по ст. 272 УК.

Способ посягательства может иметь значение для квалификации деяния как преступления, если речь идет о ч. 3 ст. 272 УК.

Попытки лица преодолеть систему защиты информации: физически (например, отключить сигнализацию, тайно проникнуть внутрь охраняемой территории) или интеллектуально (например, подобрать код доступа к компьютерной информации) должны расцениваться как покушение на неправомерный доступ к компьютерной информации и квалифицироваться по ст. 272 УК со ссылкой на ч. 3 ст. 30 УК. Если же в результате действий лица по преодолению системы защиты наступили указанные в ч. 1 ст. 272 УК материальные общественно опасные последствия, то преступное поведение следует квалифицировать по данной статье без ссылки на ст. 30 УК.

Субъект преступного посягательства, как правило, общий, т.е. физическое вменяемое лицо, достигшее к моменту его совершения 16-летнего возраста. В некоторых случаях субъект наделен дополнительным признаком: а) является участником преступной группы; б) использует для совершения преступления свое служебное положение (см. ч. 3).

Субъективная сторона составов преступления характеризуется виной в форме умысла. Об умысле могут свидетельствовать и действия виновного по преодолению препятствий при осуществлении неправомерного доступа к компьютерной информации, например взламывание пароля.

Мотивы совершения преступления могут быть любыми: «спортивный интерес», проверка своего уровня квалификации, любопытство, совершение другого преступления, корыстная заинтересованность и пр. Только последний из названных мотивов может повлиять на квалификацию содеянного по ч. 2 ст. 272 УК.

Квалифицирующие признаки закреплены в ч. 2 ст. 272 УК. Предусмотрена более суровая уголовная ответственность, если содеянное повлекло крупный ущерб (см. примечание 2 к статье) или осуществлено из корыстной заинтересованности. Корыстная заинтересованность означает стремление виновного лица посредством неправомерного доступа к компьютерной информации получить выгоду имущественного характера для себя или других лиц.

Особо квалифицирующие признаки закреплены в ч. 3 и 4 ст. 272 УК: группа лиц, действующих по предварительному сговору (см. ч. 2 ст. 35 УК); организованная группа (см. ч. 3 ст. 35 УК); использование лицом своего служебного положения (т.е. виновное лицо для совершения преступления воспользовалось полномочиями, предоставленными ему по должности, службе, договору, что облегчило доступ к охраняемой законом информации); тяжкие последствия или угроза наступления таковых.

К тяжким последствиям можно отнести возникновение катастрофы, нарушение производственной или иной деятельности организации/учреждения на длительное время, осложнение межгосударственных отношений, рост социальной напряженности, совершение аварии, повлекшей причинение тяжкого вреда здоровью или наступление смерти хотя бы одного человека, причинение вреда средней тяжести здоровью нескольких лиц, утрату ценной дорогостоящей техники, уникальной информации или наступление иного материального ущерба в особо крупном размере, в том числе связанного с восстановлением нарушенной работы информационной системы и т. д. Угроза наступления тяжких последствий означает подкрепленную фактическими данными реальную возможность наступления таковых.

Если лицо, допущенное к работе с охраняемой законом компьютерной информацией, каким-либо образом способствует неправомерному доступу к этой информации другого лица (например, путем передачи ему пароля программы), то при наступлении хотя бы одного из указанных последствий действия данного лица надлежит квалифицировать по ч. 3 ст. 272 УК со ссылкой на ч. 5 ст. 33 УК.

Различия между неправомерным доступом к компьютерной информации и нарушением авторских или смежных прав

Неправомерный доступ к компьютерной информации (ст. 272 УК)	***Нарушение авторских или смежных прав (ст. 146 УК)***
Основной объект посягательства	
Информационная безопасность общества	Право на интеллектуальную собственность (в том числе на базы данных, компьютерные программы и т. д.)
Предмет посягательства	
Информация в компьютерных файлах, программах или базах данных на соответствующем электронном носителе	Объекты авторского права или смежных прав
Объективная сторона состава преступления	

Неправомерный доступ к компьютерной информации (ст. 272 УК)	***Нарушение авторских или смежных прав (ст. 146 УК)***
Неправомерный доступ к охраняемой законом компьютерной информации	Присвоение авторства (плагиат), незаконное использование объектов авторского права или смежных прав, приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм
Состав преступления по законодательной конструкции	
«Материальный»	«Материальный» (ч. 1); «формальный» (ч. 2, 3)
Материальные общественно опасные последствия	
Уничтожение, блокирование, модификация, копирование компьютерной информации (ч. 1), крупный ущерб (ч. 2), тяжкие последствия (ч. 4)	Крупный ущерб автору или иному правообладателю (ч. 1)

1.5. Понятие организационной защиты информации

Организационная защита информации – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, и включает в себя организацию режима охраны, организацию работы с сотрудниками, с документами, организацию использования технических средств и работу по анализу угроз информационной безопасности.

Обеспечение защиты средств обработки информации и автоматизированных рабочих мест от несанкционированного доступа достигается системой разграничения доступа субъектов к объектам.

Данная система реализуется в программно-технических комплексах:

- в рамках операционной системы,
- систем управления базами данных или прикладных программ,
- в средствах реализации ЛВС,
- в использовании криптографических преобразований, методов контроля доступа.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз безопасности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или по крайней мере сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

Защита информации организационными средствами предполагает защиту без использования технических средств.

Иногда, задача решается простым удалением организационно-технических средств от границы контролируемой зоны на максимально возможное расстояние. Так же возможен вариант размещения, например, трансформаторной подстанции и контура заземления в пределах контролируемой зоны.

К организационно-техническим можно отнести:

- удаление вспомогательных технических средств, линии которых выходят за пределы контролируемой зоны,
- запрещение использования технических средств с паразитной генерацией для обработки информации,
- проведение специальных проверок технических средств на отсутствие закладочных устройств.

Необходимо помнить, что организационно-технические меры требуют выполнения комплекса мер, предписанных нормативными документами.

При разработке системы защиты информации (СЗИ) так же следует принимать во внимание то, что вся система состоит из более мелких систем.

К ним относится:

- подсистема управления доступом,
- подсистема регистрации и учета, криптографическая защита информации
- и подсистема обеспечения целостности.

Общие принципы организации защиты информации, применяемые при разработке СЗИ:

- непрерывность
- достаточность
- комплексность
- согласованность
- эффективность

Для реализации мер защиты конфиденциальной информации должны применяться сертифицированные в установленном порядке технические средства защиты информации.

К организационным мерам защиты можно отнести **организационно-технические** и **организационно-правовые мероприятия,** осуществляемые в

процессе создания и эксплуатации системы обработки и передачи данных фирмы или банка с целью обеспечения защиты информации.

Насколько важным являются организационные мероприятия в общем арсенале средств защиты, говорит уже хотя бы тот факт, что ни одна система обработки данных не может функционировать без участия обслуживающего персонала.

Кроме того, организационные мероприятия охватывают все структурные элементы системы защиты на всех этапах их жизненного цикла:

- строительство помещений,
- проектирование системы,
- монтаж и наладка оборудования,
- испытания и проверка в эксплуатации аппаратуры, оргтехники, средств обработки и передачи данных.

Сегодня фирмы, специализирующиеся на изготовлении технических средств для промышленного шпионажа, выпускают устройства, которые по своим параметрам не уступают оперативной технике, используемой спецслужбами.

Лучше вооружены сегодня те спецслужбы, у которых есть для этого необходимые денежные средства. Это обстоятельство необходимо учитывать при оценке потенциальных возможностей ваших конкурентов по ведению промышленного шпионажа. Первым шагом в создании эффективной системы защиты фирмы от технического проникновения конкурентов или злоумышленников должна стать оценка основных методов промышленного шпионажа, которыми могут воспользоваться ваши конкуренты, изучение характеристик, имеющихся у них на вооружении средств съема информации с отдельных помещений и технических средств фирмы.

Предварительный анализ уязвимости помещений и технических средств фирмы от промышленного шпионажа позволяет сделать вывод о наиболее

вероятных методах съема информации, которые может использовать конкурент. Такой анализ дает возможность службе безопасности фирмы выработать необходимые организационные, технические и специальные меры защиты объекта фирмы.

Организационные меры защиты базируются на законодательных и нормативных документах по безопасности информации.

Они должны охватывать все основные пути сохранения информационных ресурсов и включать:

- ограничение физического доступа к объектам обработки и хранения информации и реализацию режимных мер;
- ограничение возможности перехвата информации вследствие существования физических полей;
- ограничение доступа к информационным ресурсам и другим элементам системы обработки данных путем установления правил разграничения доступа, криптографическое закрытие каналов передачи данных, выявление и уничтожение

«закладок»;

- создание твердых копий важных с точки зрения утраты массивов данных;

- проведение профилактических и других мер от внедрения "вирусов".

По содержанию все множество организационных мероприятий можно условно разделить на следующие группы:

1. **Мероприятия, осуществляемые при создании системы обработки, накопления, хранения и передачи данных заключающиеся в учете требований защиты при:**

- разработке общего проекта системы и ее структурных элементов; строительстве или переоборудовании помещений;
- разработке математического, программного, информационного или лингвистического обеспечений;
- монтаже и наладке оборудования;
- испытаниях и приемке системы.

Особое значение на данном этапе придается определению действительных возможностей механизмов защиты, для чего целесообразно осуществить целый комплекс испытаний и проверок.

2) Мероприятия, осуществляемые в процессе эксплуатации систем обработки данных:

- организация пропускного режима;
- организация автоматизированной обработки информации;
- распределение реквизитов разграничения доступа (паролей, полномочий и т. д.);
- организация ведения протоколов; контроль выполнения требований служебных инструкций и т. п.

3. **Мероприятия общего характера:**

- учет требований защиты при подборе и подготовке кадров;
- организация проверок механизма защиты;
- планирование всех мероприятий по защите информации;
- обучение персонала; проведение занятий с привлечением ведущих организаций;
- участие в семинарах и конференциях по проблемам безопасности информации и т. п.

Концептуальные основы организационного обеспечения Информационной безопасности

Цели и задачи организационной защиты информации (зи)

Организационные меры ЗИ – комплекс мероприятий по ЗИ, направленный на регламентацию деятельности персонала в процессе обработки информации

Основные цели организационных мер защиты:

1) Обеспечение правильности функционирования механизмов защиты

2) Регламентация автоматизированной обработки информации

Основные направления организационной защиты на объекте:

1) Защита от НСД (от не санкционированного доступа)

2) Защита информации от утечки по техническим каналам

3) Защита информации от незадекларированных возможностей (Например, от вредоносного программного обеспечения)

4) Защита информации от ИТР (от иностранных технических разведок)

6.2. Основные организационные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации

1) **Разовые мероприятия** – мероприятия, однократно проводимые и повторяемые только при полном пересмотре принятых решений

2) Эпизодические мероприятия

3) **Мероприятия, проводимые при осуществлении или возникновении определенных изменений в защищаемой системе или внешней среде**

4) **Периодически проводимые мероприятия**

5 Постоянно проводимые мероприятия

К разовым мероприятиям относятся:

1) Мероприятия по созданию научно-технической и методологической основы защиты системы, в том числе концепции и руководящие документы

2) Мероприятия, осуществляемые при проектировании, строительстве и оборудовании объектом проведение специальных проверок всех технических средств разработка и утверждение функциональных обязанностей должностных лиц мероприятия по разработке правил управления доступом к ресурсам системы организация пропускного режима на предприятии и в отдельных помещениях создание подразделений по защите информации

К эпизодическим мероприятиям относятся:

1) Мероприятия, осуществляемые при кадровых изменениях в составе персонала

2) Мероприятия, осуществляемые при ремонте и модификации оборудования, ПО и т. д.

К периодически проводимым мероприятиям относятся:

1) Распределение/разграничение реквизитов разграничения доступа (раздача паролей)

2) Анализ системных журналов и принятие мер по обнаруженным недостаткам и проблемам

3) Анализ состояния и оценка эффективности мер защиты информации

мероприятия по пересмотру состава и перестроению системы защиты и т. д.

К постоянно проводимым мероприятиям относятся:

1) Мероприятия по обеспечению достаточного уровня физической защиты всех элементов объекта (охрана, в том числе и противопожарная, сохранность съемных носителей)

2) Явный или скрытый контроль за работой персонала системы

3) контроль за реализацией выбранных мер защиты

постоянно осуществляемый анализ состояния системы защиты

Организационные средства

складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия).

Преимущества организационных средств:

- они позволяют решать множество разнородных проблем,
- просты в реализации,
- быстро реагируют на нежелательные действия в сети,
- имеют неограниченные возможности модификации и развития.

Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

1.6. Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним

В деле защиты информационной деятельности от различного вида угроз значительное место занимает персонал предприятия, который может стать как объектом, так и субъектом таких угроз. Этот процесс предполагает проведение превентивных и текущих мер, направленных на работу с кадрами. Важность работы с персоналом определяется тем, что в случае желания сотрудника разгласить сведения (в силу корыстных или других мотивов), являющиеся конфиденциальной информацией, воспрепятствовать этому не смогут никакие, даже дорогостоящие, средства защиты. Западные специалисты по обеспечению экономической безопасности считают, что сохранность конфиденциальной информации на 80% зависит от правильного подбора, расстановки и воспитания персонала. При приеме на работу проводится трехступенчатое анкетирование.

Анкетированное исследование – это инструмент социологического изучения социальных явлений в их конкретном состоянии с помощью методов, позволяющих производить количественные и качественные сборы, измерения, обобщения, анализ социологической информации. Социологический исследовательский проект – это система научно-исследовательских процедур, методов, методик поэтапного изучения социальных явлений на основе фактологических данных.

Программа – это изложение общей концепции исследовательского проекта, заключающей в себе поэтапное программирование и правила процедур научно-исследовательской деятельности. Программа выражает понимание и знание того:

- что надо делать;
- чем выполнять задуманное;
- как выполнять задуманное.

Функции программы:

- теоретико-методологическая, которая позволяет определить научную проблему и подготовить основы для ее решения;
- методологическая, которая позволяет наметить способы сбора данных и описания ожидаемых результатов;
- организационная, которая позволяет спланировать деятельность исследователя (коллектива) на всех этапах работы.

Анкетирование проводится совместно со специалистами службы отдела кадров и профессиональными психологами.

Вопросы могут быть расширены или видоизменены в связи с учетом специфики предприятия. В первую очередь вопросы подтверждают профессиональный и общеобразовательный уровень кандидата.

В анкету включены вопросы общего характера, позволяющие получить представление о человеке как о разносторонней личности, например: вопрос о занятиях спортом может говорить о состоянии здоровья кандидата. Также в анкету включен ряд вопросов-ловушек, предназначенных для проверки искренности и правдивости ответов анкетируемого лица.

Для выявления уровня интеллекта, сообразительности, определения морально-психологического уровня личности, ее возможных преступных наклонностей, умения хранить секреты в анкету включены психологические вопросы.

В случае необходимости получения более детальной информации о кандидате могут быть применены различные методики и тесты экспресс-диагностики характерологических особенностей личности.

Подбор, основанный на случайном обращении кандидатов непосредственно в фирму, может представлять угрозу ее экономической безопасности в будущем. После ознакомления с документами кандидата (личными документами, об образовании, прежней должности и стаже работы, характеристиками и рекомендациями), а последнего – с требованиями к нему и признания обоюдного соответствия производится собеседование работника кадровой службы фирмы с кандидатом. Кандидат заполняет анкету, отвечает на вопросы, в том числе вопросы профессиональных и психологических тестов. Следует отметить, что психологические качества кандидата не менее важны, чем профессиональные.

В случае успешного прохождения кандидатом проверки и признания его соответствующим должности осуществляется заключение (подписание) двух документов:

а) трудового договора (контракта). Контракт обязательно должен содержать пункт об обязанности работника не разглашать конфиденциальную информацию и соблюдать меры безопасности;

б) договора (обязательства) о неразглашении конфиденциальной информации, представляющего собой правовой документ, в котором кандидат на вакантную должность дает обещание не разглашать те сведения, которые ему будут известны в период его работы в фирме, а также об ответственности за их разглашение или несоблюдение правил безопасности (расторжение контракта и судебное разбирательство).

Непосредственная деятельность вновь принятого работника в целях проверки его соответствия занимаемой должности и соблюдения правил работы с конфиденциальной информацией должна начинаться с испытательного срока, в конце которого принимается окончательное решение о приеме кандидата на постоянную работу.

Основным источником утечки информации из организации является ее персонал. Человеческий фактор способен свести на нет любые самые изощренные механизмы безопасности. Это подтверждается многочисленными статистическими данными, свидетельствующими о том, что подавляющее большинство инцидентов без-

опасности связано с деятельностью сотрудников организации. Неудивительно, что работа с персоналом – главный механизм защиты. Ключевые принципы и правила управления персоналом с учетом требований информационной безопасности определены в Международном стандарте ISO/IEC 17799:2000 и сводятся к необходимости выполнения определенных требований безопасности, повышения осведомленности сотрудников и применения мер пресечения к нарушителям.

При работе с персоналом необходимо соблюдать следующие требования безопасности: ответственность за информационную безопасность должна быть включена в должностные обязанности сотрудников, включая ответственность за выполнение требований политики безопасности, за ресурсы, процессы и мероприятия по обеспечению безопасности. Должны проводиться соответствующие проверки сотрудников при приеме на работу, включая характеристики и рекомендации, полноту и точность резюме, образование и квалификацию, а также документы, удостоверяющие личность. Для критичных должностей должна проверяться также кредитная история кандидата.

Подписание соглашения о неразглашении конфиденциальной информации кандидатом должно быть обязательным условием приема на работу.

Требования информационной безопасности, предъявляемые к сотруднику, должны быть отражены в трудовых соглашениях. Там же должна быть прописана ответственность за нарушение безопасности.

Важную роль для обеспечения информационной безопасности играет осведомленность пользователей в вопросах безопасности и правилах безопасного поведения. Согласно ст. 139 Гражданского кодекса РФ обладатель конфиденциальной информации имеет право на правовую защиту от незаконного ее использования только при условии, что он принимает надлежащие меры к соблюдению ее конфиденциальности, поэтому правила политики безопасности и ответственность, предусмотренная за их нарушение, должны быть документированы и доведены до сведения всех сотрудников под роспись. Контроль осведомленности должен осуществляться на регулярной основе. Основную роль здесь играют PR-менеджеры организации.

Необходимо проводить обучение и контролировать знания пользователей по следующим вопросам:

- правила политики безопасности организации;
- правила выбора, смены и использования паролей;
- правила получения доступа к ресурсам информационной системы;
- правила обращения с конфиденциальной информацией;
- процедуры информирования об инцидентах, уязвимостях, ошибках и сбоях программного обеспечения и др.

В организации должен быть разработан соответствующий дисциплинарный процесс, проводимый в отношении нарушителей безопасности и предусматривающий расследование, ликвидацию последствий инцидентов и адекватные меры воздействия. При определении мер пресечения следует ориентироваться на положения действующего законодательства. Отношения между работником и работодателем и ответственность за нарушение информационной безопасности органи-

зации регулируются прежде всего Трудовым кодексом РФ. В определенных случаях возможно применение положений Кодекса об административных правонарушениях и Уголовного кодекса. Так, на основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности организации, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы за неоднократное грубое нарушение дисциплины. Согласно ст. 238 Трудового кодекса РФ все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный компании в результате нарушения ими правил политики безопасности. Сотрудник компании несет материальную ответственность как за прямой действительный ущерб, непосредственно причиненный им работодателю, так и за ущерб, возникший у работодателя в результате возмещения им ущерба иным лицам. Сотрудники несут материальную ответственность в пределах своего среднего месячного заработка (ст. 241 Трудового кодекса РФ). Согласно ст. 243 Трудового кодекса РФ за умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники компании несут материальную ответственность в полном размере причиненного ущерба.

Государственная доктрина в отношении лиц, допускаемых к работе с информацией, сводится к следующему: к работам и документам могут быть допущены только граждане России, которые по своим деловым, политическим и моральным качествам способны обеспечить сохранность доверенных им тайн. К работам и документам не допускаются лица, имеющие:

- психические заболевания;
- лица, которые понесли уголовную ответственность;
- лица, совершающие поступки, несовместимые с принципами нравственности и морали;
- лица, имеющие постоянный контакт с лицами (родственниками) за границей.

Те же принципы лежат в основе отбора персонала для работы с конфиденциальной информацией в организациях. Поэтому кандидатуры сотрудников, претендующих на работу с конфиденциальной информацией, проходят тщательный отбор.

Обычно при установлении квалификационных требований к должностям сотрудников, допущенных к работе с конфиденциальной информацией, упоминают необходимость наличия у специалиста высшего или среднего специального образования в области защиты информации.

При подборе персонала для работы с конфиденциальной информацией проводят следующие мероприятия:

1. Проведение аналитических мероприятий при приеме на работу.
2. Документирование добровольного согласия лица не разглашать конфиденциальную информацию и обеспечивать безопасность этой информации.
3. Инструктирование и обучение сотрудников практическим действиям по защите информации.
4. Контроль по защите сведений конфиденциального характера.

5. Стимулирование ответственности к сохранению конфиденциальной информации.

Профилактические кадровые мероприятия по защите информации:

1. Оформление письменного обязательства о неразглашении конфиденциальной информации, которая будет известна в результате трудовой деятельности.

2. Предупреждение увольняемых работников об ответственности за разглашение или незаконное использование информации, полученной в результате трудовой деятельности.

3. Проведение проверочных мероприятий в отношении лица, оформляемого на работу с конфиденциальной информацией.

Лица, допущенные к конфиденциальной информации, обязаны:

1. Строго охранять тайну конфиденциальной информации и пресекать действия других лиц, которые разглашают эту информацию.

2. Знакомиться только с той информацией, к которой они имеют отношение.

3. Знакомить представителей других организаций с конфиденциальной информацией только с письменного разрешения руководителя организации.

4. Сообщать в службу кадров о любых изменениях персональных данных.

Подразделения, имеющие дело с конфиденциальной информацией, должны комплектоваться специалистами, способными по своим деловым качествам решать возложенные на них задачи, иметь необходимые знания и опыт для работы с такой информацией.

Не рекомендуется зачислять на работу в такие подразделения лиц, временно работающих в фирме (организации). Если речь о государственном учреждении и охране государственной тайны, то это напрямую воспрещается.

Чтобы подробнее рассмотреть процедуры, проводимые при отборе персонала, следует определить принципы приема кандидатов. Отметим, что первые два принципа – получение резюме и его рассмотрение – хотя и относятся к этапу подбора, однако их исключение отрицательно скажется на целостности всего процесса.

Итак, в общем виде технологическая цепочка выглядит следующим образом:

- подбор предполагаемой кандидатуры (кандидатур) для приема на работу или перевода, получение резюме;

- изучение резюме руководством фирмы, структурного подразделения и секретарем-референтом (при отсутствии в фирме службы персонала или менеджера по персоналу);

- знакомство (предварительное собеседование) руководства фирмы, структурного подразделения и секретаря-референта с отобранными кандидатами, беседа с ними, уточнение отдельных положений резюме; ответы на вопросы о будущей работе (без сообщения конфиденциальных сведений); изучение полученных от кандидата рекомендательных писем;

- по итогам предварительного собеседования заполнение отобранными кандидатами, не работающими в фирме, и представление секретарю-референту заявления о приеме, автобиографии, личного листка по учету кадров, копий документов об образовании, наличии ученых степеней, ученых и почетных званий, передача секретарю-референту рекомендательных писем и, при наличии, характеристик;

- обновление материалов личного дела работающего в фирме сотрудника; получение представления о переводе на новую должность от руководителя структурного подразделения;

- изучение секретарем-референтом достоверности представленных кандидатами документов, собеседование по документам, при необходимости подтверждение тех или иных сведений представлением дополнительных документов;

- опрос секретарем-референтом авторитетных для фирмы лиц, лично знающих кандидата на должность, протоколирование опроса;

- собеседование экспертов-психологов с кандидатами на должность с целью определения их личных и моральных качеств, собеседование с кандидатами руководителя структурного подразделения с целью определения их профессиональных способностей; рассмотрение медицинской справки;

- при необходимости – тестирование или анкетирование кандидатов;

- по совокупности собранных материалов и их анализа принятие решения руководством фирмы об отборе единственного претендента и возможности предложить ему работу, связанную с владением тайной фирмы;

- заключительное собеседование с претендентом на должность, получение от него принципиального согласия на работу с конфиденциальной информацией;

- в случае согласия работника – подписание претендентом обязательства о неразглашении тайны фирмы, в частности сообщенных ему конфиденциальных сведений о характере информации, с которой он будет работать, о наличии системы защиты этой информации и тех ограничениях, которые придется учитывать работнику в служебной и неслужебной обстановке;

- беседа-инструктаж руководителя структурного подразделения, руководителя службы безопасности и секретаря-референта с претендентом на должность;

- ознакомление претендента с должностной инструкцией, рабочими технологическими инструкциями, инструкцией по обеспечению информационной безопасности фирмы и другими аналогичными материалами;

- составление проекта трудового договора, содержащего пункт об обязанности работника не разглашать конфиденциальные и ценные сведения фирмы и ответственность за разглашение;

- оформление и подписание трудового договора;

- составление и подписание приказа о приеме на работу (или переводе на другую работу) с испытательным сроком;

- заведение личного дела на вновь принятого работника и заполнение на него необходимых учетных форм, в том числе личной карточки по форме Т-2;

- внесение необходимых сведений в первичные учетные бухгалтерские документы;

- внесение соответствующей записи в трудовую книжку работника;

- изучение личных, моральных и профессиональных качеств работника в течение испытательного срока;

- обучение работника правилам работы с конфиденциальной информацией и документами, инструктажи, проверка знаний;

- анализ результатов работы сотрудника в течение испытательного срока, принятие решения о прекращении или продлении контракта и издание соответствующего приказа;

- оформление допуска сотрудника к конфиденциальной информации и документам фирмы в соответствии с его должностными обязанностями.

Особенностью технологической цепочки является то, что по итогам выполнения любой из процедур (до издания приказа о приеме или переводе) руководство фирмы или сам кандидат могут отказаться от дальнейшего продолжения процесса приема на работу. Следует отметить, что при подборе персонала для работы с ценной или конфиденциальной информацией следует в первую очередь обращать внимание на личные и моральные качества кандидатов на должность, их порядочность и лишь затем – на их профессиональные знания, умения и навыки.

Важно уже на первых этапах отбора отсечь те кандидатуры, которые по формальным признакам явно не соответствуют требованиям, предъявляемым к будущему сотруднику. Особое внимание специалисты по подбору персонала должны обращать на анализ достоверности и правильности оформления персональных документов: соответствие фамилий, имен и отчеств, других персональных данных, наличие в документах необходимых отметок и записей, идентичность фотокарточек и личности гражданина, соответствие формы бланка документа годам их использования, отсутствие подчисток, незаверенных исправлений, попыток замены листов, фотографий и т. п. Все печати должны соответствовать названиям тех организаций, которые выдали документ. Например: трудовая книжка должна соответствовать форме, установленной для того периода времени, когда она была выдана, или иметь надпись «дубликат», содержать запись об увольнении с последнего места работы, заверенную печатью и т. п.

При каких-то сомнениях кандидата просят представить дубликаты испорченных документов, заверить исправления. Документы, вызвавшие явное сомнение, возвращаются соискателю и одновременно ему отказывается в рассмотрении вопроса о приеме на работу. Только после тщательного анализа представленных документов с кандидатами на должность проводится собеседование.

1.7. Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников

Допуск (доступ) к государственной тайне.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

для принимающих такое решение предусматривает:

• принятие на себя обязательств перед государством по нераспространению соответствующих сведений;

• согласие на временные ограничения их прав (права выезда за границу на оговоренный срок, права на распространение или иное использование сведений, составляющих государственную тайну, права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне;

• определение видов, размеров и порядка предоставления льгот (обычно – надбавка к должностному окладу);

• ознакомление с нормами законодательства РФ об ответственности за нарушение режима государственной тайны,

• принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Объем и характер *проверочных мероприятий* зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

Взаимные обязательства администрации и оформляемого лица отражаются в трудовом договоре (контракте). Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут быть:

• признание его судом недееспособным или ограниченно дееспособным, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой (непогашенной) судимости за эти преступления;

• наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну;

• постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;

• выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;

• уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Прекращение допуска к государственной тайнене освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством РФ и возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны.

Руководители органов государственной власти, предприятий, учреждений и организаций несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся исключительно с теми сведениями и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

Допуск юридических лиц (предприятий, учреждений и организаций) к проведению работ, связанных с государственной тайной, осуществляется путем получения ими *лицензий* на проведение работ со сведениями соответствующей степени секретности. Лицензия на проведение указанных работ выдается на основа-

нии результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну.

Средства защиты информации должны иметь *сертификат*, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте РФ, Федеральную службу безопасности РФ, Министерство обороны РФ.

1.8. Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации.

О фактах утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам иных нарушений режима конфиденциальности (далее – утечка, утрата), работник контроля обязан немедленно поставить в известность руководителя акционерного общества и организаций по совместной работе по данной тематике. Принять срочные меры по исключению ущерба или свести их к минимуму.

Необходимые мероприятия по розыску утраченных носителей, а также по выявлению обстоятельств утечки сведений конфиденциального характера, и выявлению виновных в этом лиц в акционерном обществе проводятся подразделением режима и безопасности с привлечением (по необходимости) правоохранительных органов.

Для проведения служебного расследования руководитель акционерного общества не позднее чем на следующий день после обнаружения факта утечки, утраты, назначает приказом комиссию из компетентных, незаинтересованных в исходе дела лиц в составе не менее 3 человек (в том числе работника защиты информации), имеющих непосредственное отношение и допуск к данным сведениям и носителям, с освобождением их при необходимости от исполнения прямых служебных обязанностей.

В работе комиссии могут принимать непосредственное участие представители организаций по совместной работе по данной тематике.

Комиссия, проводящая служебное расследование, обязана:

- установить обстоятельства утечки, утраты (время, место, способ и др.);
- вести розыск утраченного носителя;
- установить лиц, виновных в создание условий и совершившие правонарушения;
- установить причины и условия, способствующие утечке, утрате и выработать рекомендации по их устранению.

Члены комиссии, проводящие служебное расследование, имеют право:

- проводить осмотр помещений, здания(й) местности, сейфов, столов, шкафов, спецпортфелей и т. д., где могут находиться утраченные носители;
- проверять полистно конфиденциальную документацию, журналы учёта конфиденциальных носителей, отражающие их поступление и движение, регистрационные карточки и т. п.;

- опрашивать работников, виновных в утечке, утрате, проверять их на лояльность к фирме, а также других работников общества, могущих оказать содействие в устранении обстоятельств утечки, утраты и получать от них письменные объяснения (показания);
- привлекать с разрешения руководителя акционерного общества других работников общества, незаинтересованных в исходе дела, для проведения отдельных действий служебного расследования.

Служебное расследование должно проводиться в минимально короткие сроки и не более месяца со дня обнаружения факта утечки, утраты.

В эти же сроки руководитель акционерного общества должен решить в установленном порядке вопрос о привлечении виновных лиц к ответственности.

В случаях, когда утраченные носители не обнаружены, розыск может быть прекращен, если исчерпаны все возможные меры розыска, внесена ясность в обстоятельства их утраты и установлены виновные в этом лица. О прекращении розыска составляется мотивированное заключение, которое утверждается руководителем организации, назначившим комиссию по проведению служебного расследования.

Результаты всех мероприятий, проводимых в процессе служебного расследования, документируются.

По окончании служебного расследования комиссия обязана представить руководителю организации на рассмотрение следующие документы:

- заключение о результатах проведенного служебного расследования;
- письменные объяснения лиц, которых опрашивали члены комиссии;
- акты проверок документации, изделий, помещений, сейфов и т. п.;
- другие документы, имеющие отношение к служебному расследованию.

Для определения степени (важности) конфиденциальности сведений, одновременно с комиссией по проведению служебного расследования создается комиссия специалистов по определению степени (важности) конфиденциальных сведений.

Такая комиссия назначается приказом руководителя общества в составе не менее трех человек, незаинтересованных в исходе дела, имеющих непосредственное отношение к сведениям и носителям, по которым дается заключение о степени их конфиденциальности.

В необходимых случаях руководитель общества для участия в работе комиссии может привлекать имеющих отношение к сведениям, носителям, по которым дается заключение, специалистов из обществ соисполнителей работ по согласованию с их руководителями.

Результаты работы комиссии специалистов по определению степени конфиденциальности, оформляются мотивированным заключением, которое в минимально короткий срок, но не позднее 10 дней со дня создания комиссии, представляется на утверждение руководителю общества.

В заключении специалистов указывается, содержатся ли в сведениях конфиденциальная информация на момент проведения экспертизы.

По результатам работы комиссии руководство общества принимает меры по ликвидации последствий утечки, утраты.

Снятие с учёта утраченных носителей сведений осуществляется на основании утвержденного руководителем организации акта о результатах служебного расследования факта утраты носителя.

Факт утраты информации выявляется в основном посредством анализа публикаций, рекламы, выставочных и других материалов фирм-конкурентов. В этом случае анализируются карточки учета осведомленности сотрудников в секретах фирмы и выявляется сотрудников, владеющих утраченной информацией. Анализ ведется в рамках служебного расследования.

Служебное расследование организуется по фактам разглашения или утечки информации, утраты документов и изделий, другим грубым нарушениям правил защиты информации. Расследование проводится специальной комиссией, формируемой приказом первого руководителя фирмы. Расследование предназначено для выяснения причин, всех обстоятельств и их последствий, связанных с конкретным фактом, установления круга виновных лиц, размера причиненного фирме ущерба. Все мероприятия обязательно документируются.

План проведения служебного расследования:

- определение возможных версий случившегося (утрата, хищение, уничтожение по неосторожности, умышленная передача сведений, неосторожное разглашение и т. д.);
- определение (планирование) конкретных мероприятий по проверке версий (осмотр помещений, полистная проверка документации, опрос сотрудников, взятие письменного объяснения у подозреваемого лица и т. д.);

назначение ответственных лиц за проведение каждого мероприятия;

- указание сроков проведения каждого мероприятия;
- определение порядка документирования;
- обобщение и анализ выполненных действий по всем мероприятиям;
- установление причин утраты информации, виновных лиц, размер ущерба для фирмы;
- передача материалов служебного расследования с заключительными выводами первому руководителю фирмы для принятия решения

Служебное расследование проводится в кратчайшие сроки. В ходе служебного расследования обычно анализируются следующие виды документов:

- письменные объяснения опрашиваемых лиц, составляемые в произвольной форме;
- акты проверки документации и помещений, где указываются фамилии лиц, проводивших проверку, их должности, объем и виды проведенного осмотра, результаты, указываются подписи этих лиц и дата;
- другие документы, относящиеся к расследованию (справки, заявления, планы, анонимные письма и т. д.).

По результатам анализа составляется заключение о результатах проведенного служебного расследования, в котором подробно описывается проведенная работа, указываются причины и условия случившегося, определяются виновные

лица, даются рекомендации по предотвращению в будущем подобных фактов. Вопрос о наказании виновных лиц ставится только после завершения служебного расследования, мера наказания определяется лично первым руководителем фирмы. При подтверждении факта передачи сотрудником информации постороннему лицу фирма должна обратиться в суд для рассмотрения вопроса о возмещении материального ущерба от кражи информации.

Следовательно, рекомендуемые направления и методы текущей работы с персоналом фирмы позволяют организовать эффективную систему заинтересованного участия сотрудников в обеспечении безопасности фирменных секретов, постоянного контроля работы персонала с конфиденциальной информацией и своевременного выявления попыток злоумышленника завладеть интеллектуальной собственностью фирмы.

1.9. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия

К помещениям, предназначенным для ведения работ с использованием сведений, составляющих государственную тайну, или для хранения их носителей, предъявляется ряд требований.

На практике данные требования, как правило, распространяются на служебные помещения и хранилища предприятия, в которых используются в работе или хранятся не только названные сведения, но и другие виды конфиденциальной информации (или ее носители). Это позволяет обеспечить сохранение конфиденциальности проводимых в указанных помещениях работ, а также надежную сохранность носителей конфиденциальной информации.

Требования к помещениям и хранилищам

Входные двери этих помещений оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время, в них также могут устанавливаться кодовые и электронные замки и автоматические турникеты.

Режимные помещения, в которых в нерабочее время хранятся носители конфиденциальной информации, оснащаются охранной сигнализацией, связанной с караульным помещением, пультом централизованного наблюдения за сигнализацией службы охраны и с дежурным по предприятию.

Режимные помещения, в которых имеются технические средства, разрабатываются, испытываются или эксплуатируются специальные изделия, имеющие охраняемые характеристики, оборудуются в соответствии с требованиями по противодействию иностранным техническим разведкам и технической защите информации.

Перед началом эксплуатации режимные помещения обследуются комиссией, назначаемой руководителем предприятия, и аттестуются на соответствие требованиям, предъявляемым к помещениям для проведения работ с конкретным видом конфиденциальной информации.

Результаты работы комиссии оформляются актом пригодности помещения для проведения конкретных видов работ, утверждаемым руководителем предпри-

ятия. Обследование и аттестация режимных помещений проводится не реже одного раза в 5 лет, а также после их ремонта или реконструкции.

В эти помещения допускается строго ограниченный круг сотрудников предприятия, имеющих прямое отношение к ведущимся в них работам. Вместе с тем, в них допускаются руководитель предприятия, его заместитель, руководитель службы безопасности, руководитель режимно-секретного подразделения и их заместители. Доступ других сотрудников предприятия в эти помещения в случае крайней служебной крайне важности должна быть разрешен заместителем руководителя предприятия, руководителем режимно-секретного подразделения или его заместителем.

Для осуществления приема и выдачи носителей конфиденциальной информации режимные помещения соответствующих структурных подразделений (режимно-секретного подразделения или службы безопасности) оборудуются специальными окнами, не выходящими в общий коридор, или выделяется часть рабочей комнаты, изолированная барьером.

Размер режимных помещений определяется исходя из функций этих помещений. Для ознакомления и работы с носителями конфиденциальной информации в помещениях службы безопасности (режимно-секретного подразделения) выделяются специальные комнаты (кабины).

В режимных помещениях службы безопасности (режимно-секретного подразделения) запрещается работать с документами, не имеющими непосредственного отношения к основной деятельности данной службы (подразделения), а также хранить посторонние предметы.

Для хранения носителей конфиденциальной информации помещения обеспечиваются необходимым количеством хранилищ, замки которых оборудуются приспособлениями для опечатывания. Хранилища и ключи от хранилищ учитываются в службе безопасности (режимно-секретном подразделении). Хранилища, а также входные двери помещений, в которых они находятся, оборудуются надежными замками с двумя экземплярами ключей от них, один из которых в опечатанном пенале (пакете) хранится у руководителя службы безопасности (режимно-секретного подразделения). Второй экземпляр ключей в опечатанном виде хранится у руководителя предприятия или у его заместителя.

В нерабочее время ключи от хранилищ и от входных дверей режимных помещений, в отдельных пеналах, опечатанных дежурным по службе безопасности (режимно-секретному подразделению), передаются на хранение службе охраны или дежурному по предприятию.

По окончании рабочего дня все хранилища и режимные помещения закрываются и опечатываются. Хранилища и входные двери помещений, в которых они находятся, опечатываются разными печатями. При опечатывании мастика (пластилин) или сургуч накладываются таким образом, чтобы исключить их снятие без повреждения оттиска печати.

Режимные помещения, в которых хранятся носители конфиденциальной информации, с опечатанными входными дверями и пеналы с ключами от них сдаются под охрану службе охраны или дежурному по предприятию с указанием

времени приема-сдачи и проставлением соответствующих отметок о включении и выключении охранной сигнализации.

1.10. Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов

Типовой шаблон положения:

1. Общие положения

1.1. Настоящий Порядок устанавливает организацию охраны, пропускного и внутриобьектового режимов в административных зданиях, расположенных по адресу: Юридический адрес/адрес регистрации.

1.2. Охрану административного здания осуществляет Частное охранное предприятие ххх (далее по тексту – подразделение охраны).

1.3. Требования Порядка направлены:

- на обеспечение охраны административных зданий, служебных помещений, служебной документации, материальных средств;
- на исключение бесконтрольного входа (выхода) лиц, вноса (выноса) имущества из административных зданий;
- на поддержание внутреннего порядка и обеспечение мер пожарной безопасности в административных зданиях.

1.4. Требования Порядка являются обязательными для работников предприятия, юридических и физических лиц. осуществляющих свою деятельность в административных зданиях.

1.5. Организация охраны и работы бюро пропусков, а также практическое осуществление пропускного и внутриобъектового режимов в административных зданиях осуществляется в соответствии с действующими нормативно-правовыми документами.

1.6. Физические и юридические лица, нарушившие требования пропускного и внутриобъектового режимов, несут ответственность в соответствии с законодательством Российской Федерации.

1.7. Выписки из Порядка для информации посетителей оформляются наглядно на контрольно-пропускном пункте (далее – КПП) и в бюро пропусков.

2. Порядок организации охраны зданий и помещений

2.1. Охрана административных зданий осуществляется путем дежурства (выставления постов) из числа сотрудников подразделения охраны на контрольно-пропускных пунктах, применения систем охранно-пожарной сигнализации и видеонаблюдения. патрулирования внутри и снаружи административных зданий.

2.2. Начальник подразделения охраны разрабатывает план охраны административных зданий и должностные инструкции для состава дежурной смены охраны, организует взаимодействие с территориальными органами внутренних дел и организациями по эксплуатации и хозяйственному обслуживанию административных зданий на случай действий при осложнении обстановки (пожар, напа-

дение и т.д.). План охраны административных зданий согласовывается с Руководителем предприятия, управляющего зданиями.

2.3. Служебные помещения, где хранятся документы ограниченного пользования и материальные ценности, помещения первого этажа оборудуются техническими средствами охраны.

2.4. С внешней стороны административных зданий, на КПП. а также в отдельных местах могут устанавливаться системы видеонаблюдения.

2.5. Порядок использования технических средств охраны и систем видеонаблюдения определяется отдельной инструкцией, утверждаемой начальником подразделения по охране административных зданий и согласуемой с Руководителем предприятия, управляющего зданиями.

2.6. Помещения в административных зданиях (согласно списку; составляемому руководством предприятия), где хранятся служебные документы ограниченного пользования, материальные ценности, после окончания рабочего дня опечатываются, ставятся на сигнализацию и сдаются под охрану дежурной смене.

2.7. Порядок сдачи (приема) помещений под охрану, а также порядок их вскрытия в случае пожара или стихийного бедствия определяется отдельными инструкциями, разработанными и утвержденными руководителем подразделения охраны и руководителем предприятия, обслуживающего здания. Ключи от этих помещений хранятся в опечатанных пеналах у старшего смены охраны.

2.8. При обнаружении на входных дверях нарушения оттисков печатей, срывов пломб и других признаков. указывающих на возможное проникновение в помещение, немедленно ставится в известность работник, за которым оно закреплено, организуется тщательная проверка и по результатам старшим смены охраны составляется акт осмотра помещения.

2.9. В предпраздничные и праздничные дни принимаются дополнительные меры по усилению охраны, обеспечению пропускного, внутриобъектового и противопожарного режимов в административных зданиях (могут выставляться дополнительные посты, меняться режим патрулирования, ограничиваться пропускной режим и т. д.).

3. Пропускной режим

3.1. Вход (выход) в административные здания работников и посетителей осуществляется через специально оборудованные в подъездах контрольно-пропускные пункты.

3.2. Все остальные входы в административные здания должны быть закрыты и опечатаны. Ключи от них хранятся в караульном помещении у старшего смены охраны.

3.3. Работники, сотрудники организаций, работающие в административных зданиях, допускаются в административные здания по пропускам (магнитным карточкам). Посетители допускаются в административные здания по разовым пропускам (специальным магнитным карточкам), при предъявлении документов, удостоверяющих личность.

3.4. Обо всех посетителях, допущенных в административные здания, сотрудником охраны производится запись в специальном журнале учета, который хранится на КПП.

3.5. Работники сотрудники организации, работающие в административных зданиях, допускаются в рабочие дни и часы, установленные служебным распорядком.

3.6. Посетители по разовым пропускам (специальным магнитным карточкам) допускаются в административные здания в рабочие дни с 9.00 до 17.00 часов. Ответственность за нахождение в зданиях посетителей во внерабочее время несет руководитель подразделения (организации), подавший заявку на оформление разового пропуска.

3.7. В выходные и праздничные дни, а также после 20.00 в рабочие дни все входы административного здания должны быть закрыты, за исключением основного входа, который закрывается в 22.00.

3.8. Внос (вынос) в административные здания крупногабаритных предметов (чемоданов, рюкзаков, коробок и т. д.) допускается через КПП. после предъявления содержимого для визуальной проверки контролеру КПП. В случае отказа предъявить ручную кладь для осмотра, проход посетителя в здание запрещается.

3.9. При попытке прохода в административные здания по служебным удостоверениям с истекшим сроком действия или неправильно оформленным, последние могут изыматься сотрудником подразделения охраны для передачи руководителям соответствующих предприятий с составлением протокола изъятия.

3.10. Пребывание посетителей в административных зданиях регламентируется временем, указанным в разовых пропусках и списках, которое может быть продлено в случае служебной необходимости по решению руководителя заинтересованного предприятия, о чем информируется старший смены охраны.

3.11. Посетители, допустившие нарушение установленного режима пребывания, задерживаются сотрудниками охраны до выяснения обстоятельств и причин произошедшего.

3.12. Списки работников и сотрудников организаций, работа которых связана с нахождением в административных зданиях в нерабочее время, выходные и праздничные дни утверждаются соответственно Руководителем предприятия, управляющего зданиями.

3.13. Внос продуктов (продукции) для организаций общественного питания в административные здания осуществляется в рабочие дни с 8.00 до 19.00. при наличии для данной организации письменного разрешения начальника охраны.

3.14. При этом рабочие, осуществляющие доставку продуктов внутри здания, должны иметь соответствующие пропуска.

3.15. Вносимые (выносимые) по материальным пропускам материальные ценности, стоящие на балансе, в (из) административных зданий подлежат проверке на их соответствие вышеуказанным пропускам.

3.16. Проведение общественных и культурно-массовых мероприятий в административных зданиях допускается только с разрешения руководителя предприятия с обязательным уведомлением подразделения охраны и назначением лиц.

осуществляющих контроль за соблюдением общественного порядка. Ответственные лица обязаны сообщать в подразделение охраны за сутки о планируемом времени начала и окончания проведения мероприятия.

3.17. Допуск в административные здания осуществляется по следующим документам:

3.17.1. По постоянным пропускам (магнитным карточкам):

- работников предприятий и учреждений, обслуживающих здания;
- работников сторонних организаций.

3.18. Допуск в административные здания по служебным удостоверениям (с отметкой о входе-выходе в журнале на КПП):

- руководителей министерств и ведомств, и их заместителей;
- депутатов всех уровней;
- руководителей органов государственной власти субъектов Российской Федерации и заместителей;
- работников органов законодательной, исполнительной и судебной власти Российской Федерации и работников прокуратуры;

3.19. По разовым пропускам или специальным магнитным карточкам лиц с предъявлением документов, удостоверяющих личность указанных в письменных заявках, подписанных руководителями предприятий, находящих в здании или лицами, имеющими право подписи таких заявок.

3.20. По спискам:

- лиц, приглашенных на совещания, конференции и другие мероприятия, проводимые в административных зданиях;
- иностранных граждан и членов делегаций в сопровождении работников, ответственных за организацию встречи.

3.21. По заявке-разрешению установленного образца:

- рабочих, выполняющих строительные и монтажные работы в административных зданиях, при предъявлении документа, удостоверяющего личность.

3.22. Проход к руководству посетителей, не вошедших в список, может осуществляться с разрешения (по телефону) из приемной руководителя, о чем уведомляются сотрудники подразделения охраны на КПП. Приглашенные лица обязаны предъявить документ, удостоверяющий их личность, а сотрудники подразделения охраны обязаны осуществить их допуск после регистрации в журнале на КПП.

3.23. В административные здания запрещается без специального разрешения руководства вносить кино-, фотосъемочную, звуко-, видеозаписывающую аппаратуру, а также огнестрельное, газовое и холодное оружие, взрывчатые, легковоспламеняющиеся и отравляющие вещества.

3.24. Документами, удостоверяющим личность, являются:

- паспорт гражданина Российской Федерации;
- удостоверение личности военнослужащего;
- служебное удостоверение, выданное федеральным органом исполнительной власти либо органом исполнительной власти субъекта Российской Федерации;
- военный билет военнослужащего;

- водительское удостоверение.

3.25. Разовый пропуск сдается по окончании посещения административного здания сотруднику подразделения охраны на КПП, через который посетитель входил в здание.

3.26. В разовом пропуске может быть произведена отметка об окончании времени посещения, заверенная подписью лица, принимающего посетителя.

3.27. Допуск на территорию административных зданий работников аварийных, пожарных служб и скорой помощи в случае чрезвычайных ситуаций осуществляется беспрепятственно при наличии удостоверения установленного образца у старшего группы, но с фиксацией общего количества человек, а при отсутствии удостоверения – в сопровождении сотрудников подразделения охраны или других специально выделенных лиц (дежурных служб по эксплуатации зданий). После ликвидации аварии (оказания помощи) их выпуск из административных зданий производится по служебным документам.

4. Внос (вынос) материальных ценностей в административные здания (из административных зданий)

4.1. Материальные пропуска на внос (вынос) материальных ценностей в (из) административные здания выписываются и выдаются заместителем руководителя предприятия, управляющей зданиями.

4.2. Образцы подписей должностных лиц, имеющих право подписи материальных пропусков, должны быть на контрольно-пропускных пятистах и у старшего смены охраны.

4.3. Вынос (внос) материальных ценностей разрешается только лицу, на имя которого выписан материальный пропуск.

4.4. Вынос (внос) материальных ценностей из административных зданий по устным распоряжениям должностных лиц категорически запрещается.

4.5. По материальноме пропуску могут быть вынесены указанные в нем материальные ценности в день выдачи пропуска только один раз, после чего он изымается на КПП. Ежемесячно один из старших смены охраны сдает материальные пропуска заместителю руководителя предприятия, управляющей зданиями, по специальному журналу под роспись.

4.6. Лица, нарушающие установленный порядок вноса (выноса) материальных ценностей в административные здания (из административных зданий), останавливаются, о чем немедленно докладывается старшему смены охраны для принятия решения.

4.7. По факту незаконного проноса материальных ценностей старший смены охраны информирует начальника и составляет акт.

5.1. Внутриобъектовый режим предусматривает:

- строгое соблюдение служебного распорядка всеми лицами, находящимися в административных зданиях;

- осуществление контроля за допуском в служебные помещения с целью исключения проникновения в них посторонних лиц;

- установление ответственности руководителей структурных подразделений, руководителей организаций, обслуживающих административные здания, за

сохранность имущества, состояние пожарной безопасности, соблюдение установленного режима работы и техники безопасности;

- оборудование охранно-пожарной сигнализацией выделенных помещений, спецхранилищ и комнат, где хранятся документы, издания и изделия, имеющие гриф секретности;

- установление порядка осмотра помещений по окончании рабочего дня и сдачи их под охрану;

- недопущение загромождения помещений и коридоров строительными и другими материалами, предметами, которые затрудняют движение людей и могут вызвать возгорание;

- определение безопасных участков в районе каждого административного здания на случай необходимости эвакуации людей, документов и имущества при пожаре, аварии и других стихийных бедствиях;

- определение и оборудование специальных мест для складирования излишней мебели и других материалов, а также курения;

- обеспечение мер пожарной безопасности при проведении ремонтных работ;

- проведение противопожарных мероприятий, исключающих возникновение пожаров в административных зданиях;

- своевременное уточнение плана и схемы эвакуации людей и имущества при пожаре и других стихийных бедствиях.

5.2. В административных зданиях запрещается:

- оставаться работникам в помещениях после окончания рабочего дня более одного часа без разрешения начальника отдела и сотрудникам организаций, расположенных в административные зданиях, без разрешения соответствующих руководителей организаций;

- оставлять открытыми окна и форточки по окончании рабочего дня;

- пользоваться на рабочих местах самодельными электрокипятильниками и другими нагревательными приборами;

- оставлять после окончания рабочего дня не выключенными освещение, компьютеры, ксероксы и другие электроприборы;

- курить в служебных помещениях и необорудованных для этого местах;

- засорять помещения, коридоры и места общего пользования пищевыми отходами, а также загромождать их посторонними вещами и предметами, затрудняющими проход людей;

- хранить в помещениях и комнатах легковоспламеняющиеся и горючие жидкости;

- оставлять незакрытыми рабочие помещения при выходе из них;

- находиться в административных зданиях в нетрезвом состоянии и состоянии наркотического опьянения;

- пользоваться радиотелефонами в служебных помещениях, где ограничено их применение;

- проживание каких бы то ни было лиц.

5.3. Начальники отделов организаций, расположенных в административных зданиях, в каждом служебном помещении назначают старшего, который обязан:

- повседневно контролировать выполнение работниками требований служебного распорядка и внутриобъектового режима;

- организовать соблюдение и подержание чистоты и порядка в рабочем помещении;

- знать места расположения первичных средств пожаротушения и уметь ими пользоваться;

- знать порядок вывода работников и очередность выноса из помещения и здания документов и имущества при пожаре и других бедствиях;

- по окончании рабочего дня осмотреть помещение, убедиться, закрыты ли окна и форточки, выключить освещение и электроприборы.

5.4. Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание е сторонних лиц, а также транспортных, технических и иных материальных средств.

5.5. Обработка ПДн в ИСПДн должна производиться в помещениях ограниченного доступа. Помещения ограниченного доступа должны располагаться в контролируемой зоне.

5.6. Лица, обнаружившие возгорание или пожар в помещениях административных зданий, обязаны немедленно сообщить об этом старшему смены охраны, а также в пожарную часть по телефону 01 и, по возможности, принимать меры по ликвидации возгорания или пожара первичными средствами пожаротушения.

5.7. Запасные экземпляры ключей от дверей всех помещений административных зданий хранятся у дежурного по эксплуатации зданий (коменданта) в специально оборудованном металлическом сейфе (шкафу), в опечатанных пеналах (конвертах).

5.8. Все ключи от основных и запасных выходов хранятся в служебном помещении у старшего смены охраны, обеспечивающего охрану административных зданий, в опечатанных пеналах.

5.9. Выдача этих ключей производится при пожаре, стихийных бедствиях и чрезвычайных ситуациях.

5.10. В предпраздничные дни все помещения (чердачные, подвальные, подсобные и складские, служебные комнаты и т. д.) административных зданий проверяются соответствующими комиссиями предприятия, управляющего зданиями с целью определения состояния пожарной безопасности и других вопросов, связанных с обеспечением внутриобъектового режима и охраны зданий.

5.11. О результатах осмотра помещений комиссия составляет акт, который утверждается Руководителем предприятия, управляющего зданиями.