ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Кафедра общенаучной подготовки

Основы организационно-правового обеспечения информационной безопасности сетей и систем

Методические указания по практическим занятиям

для студентов очной и заочной форм обучения
Направление подготовки – **11.03.02 «** Инфокоммуникационные технологии и системы связи»

Методические указания
Ростов-на-Дону
2019

Методические указания по практическим занятиям

по дисциплине

Основы организационно-правового обеспечения информационной безопасности сетей и систем

Составители: Жуковский Д.А., к. полит. наук., доцент кафедры «ОНП»

Рассмотрены и одобрены
на заседании кафедры Общенаучной подготовки
Протокол от 26.08.2019 г. № 1

УКАЗАНИЯ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Очная форма обучения

Практическое занятие 1

Законодательство РФ в области информационной безопасности

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту

силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 – право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в

процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Контрольные вопросы:

1. Какие общественные отношения являются предметом правового регулирования в информационной сфере?
2. Какова структура информационного законодательства РФ?
3. Какой закон установил принципы правового регулирования отношений, в информационной сфере?
4. Какие документы составляют правовую базу в информационной сфере?
5. На каком законе РФ основывается система защиты государственных секретов?

Практическое занятие 2

Правовые режимы защиты информации конфиденциального характера. Государственное регулирование деятельности в области защиты информации.

Коммерческая тайна - режим, позволяющий избежать неоправданных расходов, увеличить доходы, сохранить положение на рынке товаров, услуг или получить иную коммерческую выгоду.

Наиболее опасными формами проявления уязвимости конфиденциальной документированной информации являются потеря, хищение и разглашение - первые две одновременно могут привести и к утрате, и к утечке информации, вторая (хищение информации при сохранности носителя) и третья могут не обнаружиться, со

всеми вытекающими из этого последствиями. Поэтому необходимо уделять одинаковое внимание предотвращению как утраты защищаемой документированной информации, так и ее утечки, т.к. ущерб собственнику информации наносится в любом случае.

По данным мировой статистики, утрата 20% информации ведет к разорению 65% фирм и компаний. 1

Защита конфиденциальной документированной информации от утраты и утечки осуществляется в определенной мере конфиденциальным делопроизводством. Документирование конфиденциальной информации и организация работы с конфиденциальными документами должны производиться в условиях обеспечения их защиты, и вместе с тем многие вопросы защиты решаются в ходе и путем осуществления систематических операций по учету и обработке документов.

Сегодня, когда предприятия самостоятельно планируют и осуществляют свою деятельность, любые сведения, навыки и приёмы, неизвестные другим, могут дать значительные конкурентные преимущества. А утечка такой информации может привести к серьёзным потерям. В связи с этим особенно важное значение придается понятию - коммерческая тайна.

Коммерческая тайна - совокупность не являющихся государственной тайной сведений, представляющих ценность для субъекта предпринимательства, разглашение которых может нанести ему ущерб и, в отношении которых приняты надлежащие меры по сохранению конфиденциальности.

В соответствии с Законом «О коммерческой тайне» «коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

Информация, составляющая коммерческую тайну: научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в т.ч. составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим

лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны (ст. 3).

Нормы о коммерческой тайне содержатся более чем в 30 законодательных актах, среди которых порядок отнесения информации к конфиденциальной и виды конфиденциальной информации установлены Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» в соответствии с которым к конфиденциальной информации относятся:

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

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

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

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами;

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них и некоторые другие.

Но не вся информация субъекта хозяйствования может составлять коммерческую тайну. Так, в законе «О коммерческой тайне» представлен список сведений, не относящихся к коммерческой тайне. В частности это:

- сведения, содержащиеся в документах, подтверждающие право осуществлять коммерческую деятельность (в уставах, лицензиях и т.п.).

Документ, содержащий коммерческую тайну - это зафиксированная информация, составляющая коммерческую тайну, с реквизитами, позволяющими его идентифицировать;

- сведения о наличии на предприятии опасных факторов, влиянии предприятия на окружающую среду и граждан;

- о составе и численности работников, условиях труда, случаях профзаболеваний и производственного травматизма, о наличии вакансий, задолженности по выплате зарплаты и ряд других сведений.

Таким образом, коммерческая тайна является одним из видов конфиденциальной информации.

За разглашение коммерческой тайны предусматривается административная или уголовная ответственность. Согласно Закону «О коммерческой тайне» привлечь к ответственности в судебном порядке за разглашение коммерческой тайны и (или) использование коммерческой тайны в личных, предпринимательских, иных целях не связанных с выполнением трудовых обязанностей, возможно только в случае установления работодателем режима коммерческой тайны. При этом, если на предприятии или в организации положение о коммерческой тайне не введено, то, согласно закону, нет и информации, составляющей коммерческую тайну.

Первым шагом по реализации мер защиты коммерческой тайны, является принятие на предприятии «Положения (Инструкции) по обеспечению сохранности коммерческой тайны», в которых определяются:

- состав и объем сведений, составляющих коммерческую тайну;

- порядок присвоения грифа «Секрет предприятия» сведениям, работам и изделиям и его снятия;

- процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

- порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

- организация контроля за порядком использования сведений, составляющих коммерческую тайну;

- процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-

либо совместных действий;

- порядок применения предусмотренных законодательством мер дисциплинарного и материального воздействия на работников, разгласивших коммерческую тайну;

- возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

Руководство по введению режима коммерческой тайны.

Для того чтобы ввести в организации режим коммерческой тайны, необходимо разработать определенный пакет документов и провести ряд организационных мероприятий.

Во-первых, сначала следует четко определить в виде перечня совокупность сведений конфиденциального характера, которые будут составлять коммерческую тайну организации.

Во-вторых, определяются способы защиты информации, лица, ответственные за её сохранность, формы ответственности за разглашение.

Необходимо создание «Положения о коммерческой тайне», которое утверждается приказом, в котором отображается каким образом будет осуществляться защита коммерческой тайны, как будут маркироваться ее носители, кто будет иметь право с ними работать, как это будет учитываться, на кого будет возложена функция контроля, какова будет ответственность за разглашение коммерческой тайны и т. д.

В-третьих, осуществить регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров:

- организовать подписание всеми работниками, имеющими доступ к коммерческой тайне, «Обязательства о соблюдении коммерческой тайны», а им, в свою очередь, должны быть обеспечены все необходимые условия для надежного хранения важной информации;

- внести соответствующие пункты в Должностные инструкции, Положения об отделах (структурных подразделениях) и иную организационнораспорядительную

документацию компании.

- в Договоры с контрагентами необходимо внести пункт о том, что все сведения, связанные с договором и его исполнением, являются конфиденциальными и составляют коммерческую тайну организации.

Все сведения, связанные с договором подлежат передаче и разглашению третьим лицам за (исключением государственных (муниципальных) контрольно-надзорных, судебных и других органов) только по обоюдному соглашению сторон.

В-четвертых, необходимо обеспечить ознакомление под роспись всех сотрудников организации (работающих в настоящее время и вновь принимаемых) с разработанными и вводимыми документами и взять у каждого письменное обязательство по сохранению конфиденциальности составляющих коммерческую тайну сведений, которые стали известны в процессе работы в организации.

В этом же документе указать обязанность по неразглашению коммерческой тайны как во время работы в организации, так и в течение определенного времени после увольнения.

В пятых, ограничить доступ к информации, составляющей коммерческую тайну, путём установления порядка обращения с этой информацией и контроля за соблюдением такого порядка:

- утвердить «Приказ о доступе к коммерческой тайне» в отношении всех работников;

- при увольнении работников утверждать «Приказ о прекращении доступа к коммерческой тайне».

В шестых, вести учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена.

Для этого необходимо заполнять «Табель учёта лиц, имеющих допуск к коммерческой тайне» - вносить информацию по приказам о доступе и приказам о прекращении доступа к коммерческой тайне в случае увольнения либо при переводе на должность, не предполагающую доступ к коммерческой тайне, либо при изменении должностных обязанностей, которое не предполагает доступ к коммерческой тайне; либо в случае допуска сотрудников к информации, составляющей коммерческую

тайну.

И наконец, наносить на материальные носители, содержащие информацию, составляющую коммерческую тайну, гриф «Коммерческая тайна».

Включать в состав реквизитов документов, содержащих такую информацию, гриф «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем).

При этом, следует создать работникам все необходимые условия для соблюдения установленного компанией режима коммерческой тайны. Как правило, такими условиями являются создание возможности хранить документы, содержащие конфиденциальные сведения в запираемом месте, обеспечение доступа к персональному компьютеру, локальной сети и сети Интернет по персональному логину и паролю и т. д.

Весьма желательно сразу после введения режима коммерческой тайны, а также в дальнейшем проводить с работниками обучающие мероприятия, в процессе которых рассказывать и объяснять, зачем нужен режим коммерческой тайны, в чем он состоит и т.д.

Практика показывает, что защита конфиденциальных сведений, составляющих коммерческую тайну, равно как и интересов фирмы в целом, наилучшим образом осуществляется, когда каждый работник четко понимает требования, содержащиеся в организационно-распорядительных документах компании, и осознает важность их выполнения. В подобном случае можно говорить о наличии в коллективе высокой деловой и правовой культуры, корпоративного режима конфиденциальности и быть уверенным, что интересы фирмы защищены наилучшим образом.

Одним из основополагающих элементов системы мер по обеспечению безопасности информации, составляющей коммерческую тайну предприятия, является выделение документов, содержащих охраняемые сведения, из общего информационного потока. Выделение таких документов осуществляется присвоением им грифа «Коммерческая тайна».

Проставление грифа «Коммерческая тайна» является меткой, которая включает систему защиты охраняемой информации. Поэтому, если система защиты информации функционирует надежно, своевременность установления грифа «Коммерческая тайна» охраняемой информации имеет принципиально важное значение для ее защиты.

Вместе с тем, в соответствии с общепринятым понятием коммерческой тайны, важным является и то обстоятельство, которое позволяет ограничительный гриф по истечении надобности оперативно снимать.

Предлагаемый порядок установления и снятия грифа «Коммерческая тайна» не окажет должного влияния на защиту охраняемой информации вне связи с другими элементами системы.

Порядок установления и снятия грифа «Коммерческая тайна» для различных предприятий, фирм может различаться. Однако, во всех случаях он должен предусматривать следующие аспекты:

- кто, когда и как устанавливает гриф «Коммерческая тайна» документу и изделие;

- кто, когда и как этот гриф снимает;

- права, обязанности и ответственность должностных лиц, устанавливающих и снимающих ограничительный гриф;

- контроль за этой сферой деятельности.

При необходимости, можно вводить ограничительные пометки психологического характера. Например, на определенные категории документов, содержащих охраняемые сведения, можно прикреплять ярко выполненные таблички: «На столе не оставлять», «Хранить в сейфе».

На документах гриф «Коммерческая тайна» проставляется на первом (титульном) листе и на обложке в правом углу в соответствии с ГОСТ 6.3990.

Если документы с грифом «Коммерческая тайна» направляются с сопроводительным письмом, то на нем этот гриф также проставляется.

Следует помнить, что научно-техническую, проектно-технологическую и другую документацию, содержащую сведения, составляющие коммерческую тайну,

необходимо оформлять таким образом, чтобы сведения, составляющие коммерческую тайну, были максимально локализованы (например, собраны в отдельном томе или разделе документации). Это позволит уменьшить объем документов, что является одним из важных условий обеспечения надлежащей защиты охраняемых сведений.

Снятие грифа «Коммерческая тайна» с документа осуществляет должностное лицо, подписавшее (утвердившее) этот документ или техническую документацию на изделие, или руководитель предприятия. Основанием для снятия являются:

- требования заказчика;

- соответствующая корректировка «Перечня сведений, составляющих коммерческую тайну» предприятия;

- гриф «Коммерческая тайна» был установлен неправильно;

- истечение установленного срока действия грифа.

О снятии грифа «Коммерческая тайна» соответствующее должностное лицо делает отметку на самом документе и в технической (сопроводительной) документации на изделие путем зачеркивания грифа с проставлением своей подписи и даты.

Лица, осуществляющие учет документов с грифом «Коммерческая тайна», делают необходимые отметки в соответствующих учетных документах (формах) с указанием фамилии лица, снявшего гриф, и даты снятия.

О снятии грифа «Коммерческая тайна» предприятие, устанавливавшее гриф, извещает все предприятия, связанные договорными обязательствами с предприятием-разработчиком в части охраны коммерческой тайны.

Извещение является основанием для снятия грифа «Коммерческая тайна» с полученных документов. Выполняют эту операцию лица, осуществляющие учет документов с грифом «Коммерческая тайна».

Одним из инструментов по охране коммерческой тайны является Договор (Соглашение), которым уделяется самое серьезное внимание, поскольку в случае разглашения работником информации, составляющей коммерческую тайну работодателя, такие соглашения составят юридическую основу для привлечения работника к ответственности и взыскания причиненного ущерба. Подобные соглашения могут

заключаться как в виде отдельного документа, так и в виде условия в трудовом договоре.

В трудовом договоре либо в его неотъемлемой части (обязательстве о неразглашении информации, составляющей коммерческую тайну) следует предусмотреть порядок ознакомления работника с действующими в организации положениями и инструкциями по обеспечению сохранности коммерческой тайны. Кроме того, следует определять объем информации, передаваемой каждому конкретному работнику, за которую он должен нести ответственность.

Соглашения о неразглашении заключаются и с контрагентами по различным гражданско-правовым договорам, связанным с раскрытием сторонами по договору различной секретной информации. Для отдельных видов договоров такое условие прямо предусмотрено ГК РФ.

Обязанности по обеспечению сохранности коммерческой тайны возложены на руководителя организации. В связи с этим в контракт, заключаемый с руководителем при его найме, назначении или избрании, целесообразно включить положения, обуславливающие порядок сохранения коммерческой тайны руководителем.

В качестве примера опыт решения проблемы защиты коммерческой тайны, в следующей главе рассмотрим порядок организации работы по обеспечению защиты информации, составляющей коммерческую тайну ОАО «ФСК ЕЭС».

Контрольные вопросы:

1. Какие методы защиты лежат в основе комплексной системы информационной безопасности любого объекта.
2. С принятием каких законов началось формирование законодательства в информационной сфере?
3. Признаки и объекты профессиональной тайны?
4. Какие сведения относятся к служебной тайне?
5. На каких правовых актах основана защита служебной и коммерческой информации на предприятии?

Практическое занятие 3

Правовая охрана результатов интеллектуальной деятельности. Преступления в сфере компьютерной информации.

Введение законодателем в Уголовный кодекс термина "компьютерная информация" является новшеством. Ранее в Российском законодательстве: регулирующем информационные правоотношения: определения информации как компьютерной не существовало. Вероятней всего: определение "компьютерная" применительно к информации возникло для отграничения данного объекта посягательства от информационных преступлений: предусмотренных другими разделами Уголовного кодекса РФ. Крылов предлагает следующее криминалистическое определение компьютерной информации как специального объекта преступного посягательства. Компьютерная информация есть сведения: знания или набор команд (программа): предназначенные для использования в ЭВМ или управления ею: находящиеся в ЭВМ или на машинных носителях — идентифицируемый элемент ин формационной системы: имеющей собственника: установившего правила ее использования.

Конфиденциальными в соответствии с законом являются: в частности: такие виды информации: как:

- содержащая государственную тайну (Закон РФ "О государственной тайне" ст.ст. 275: 276: 283: 284 УК РФ);

- передаваемая путем переписки: телефонных переговоров: почтовых телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ: ст. 138 УК РФ)* касающаяся тайны усыновления (ст. 155 УК РФ).

Понятие информационных ресурсов: весьма тесно связано с понятием информации под которыми понимаются отдельные документы и отдельные массивы документов: документы и массивы документов в информационных системах: в частности: в банках данных (ст. 2 Федерального закона "Об информации: информатизации и защите информации").

Компьютерное право

Термин "компьютерное право" возник в промышленно развитых странах в середине нашего столетия в связи с широким использованием средств вычислительной техники и других: связанных с ними технических средств: в различных сферах общественной деятельности и частной жизни и формированием отношений: возникающих в процессе производства и применения новых информационных технологий. В самостоятельную отрасль права оно не выделилось ни в одной стране мира и состоит из нормативно-правовых актов разного уровня: относящихся к различным отраслям права % государственному: административному: гражданскому: уголовному и т л. В России аналогичное законодательство чаше всего называется "законодательством в сфере информатизации" и охватывает: по разным оценкам: от 70 до 500 НПА (включая НПА: которыми предусматривается создание отраслевых или специализированные автоматизированных систем: и не включая НПА. регулирующие на общих основаниях хозяйственную деятельность субъектов на рынке новых информационных технологий).

Неправомерный доступ к компьютерной информации

В специальной литературе под неправомерным доступом к компьютерной информации понимается несанкционированное собственником информации ознакомление лица с данными: содержащимися на машинных носителях или в ЭВМ. В. С. Комиссаров: д. ю. н.: профессор: определяет под неправомерным доступом к компьютерной информации получение возможности виновным лицом на ознакомление с информацией или распоряжения ею по своему усмотрению: совершаемое без согласия собственника либо иного уполномоченного лица. Самостоятельной формой неправомерного доступа являются случаи введения в компьютерную систему: сеть или в определенный массив информации без согласия собственника этого массива или иного лица заведомо ложной информации: которая искажает смысл и направленность данного блока информации.

Уничтожение информации

Уничтожение информации — это приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние.

Блокирование информации

Блокирование информации — это создание недоступности: невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства: или выключения реакции какого-либо устройства ЭВМ при сохранении самой информации.

Модификация информации

Под модификацией понимается изменение первоначальной информации без согласия ее собственника или иного законного лица.

Копирование информации

Копирование информации — это снятие копии с оригинальной информации с сохранением ее не поврежденности и возможности использования по назначению.

Конституция РФ непосредственно не регулирует отношения в области производства и применения новых информационных технологий: но создает предпосылки для такого регулирования: закрепляя права граждан свободно искать: получать: передавать: производить и распространять информацию любым законным способом (ч 4 ст. 29): право граждан на охрану личной тайны (ч 1 ст 24 и другие): обязанности государства: в частности: по обеспечению возможности ознакомления гражданина с документами и материалами: непосредственно затрагивающими его права и свободы (ч 2 ст 24). Соответствующее законодательство формирует механизмы реализации этих норм.

Уголовно-правовая характеристика главы 28 УК РФ "Преступления в сфере компьютерной информации"

Общие признаки преступлений в сфере компьютерной информации Последствия неправомерного использования информации могут быть самыми разнообразными — это не только нарушение неприкосновенности интеллектуальной собственности: но и разглашение сведений о частной жизни граждан: имущественный ущерб в виде прямых убытков и неполученных доходов: потеря репутации фирмы: различные виды нарушений нормальной деятельности предприятия: отрасли и т. д. Поэтому совершенно оправданно то: что преступления данного вида помещены в раздел IX «Преступления против общественной безопасности и общественного порядка».

Таким образом: если исходить из учения о четырехзвенной структуре объекта преступления: общим объектом компьютерных преступлений будет выступать совокупность всех общественных отношений: охраняемых уголовным законом* родовым — общественная безопасность и общественный порядок* видовым

совокупность общественных отношений по правомерному и безопасному использованию информации* непосредственный объект трактуется: исходя из названий и диспозиций конкретных статей. Чаще всего непосредственный объект основного состава компьютерного преступления сформулирован альтернативно: в квалифицированных составах количество их: естественно: увеличивается.

Практически все анализируемые преступления относятся к преступлениям средней тяжести: т. е. их максимальная наказуемость в виде лишения свободы не превышает 5 лет. Исключением является лишь создание использование и распространение вредоносных программ для ЭВМ: повлекшее по неосторожности тяжкое последствие: которое наказывается лишением свободы на срок от 3 до 7 лет и поэтому относится к тяжким преступлениям. При характеристике объективной стороны рассматриваемых составов: отмечается: что большинство из них конструктивно сформулированы как материальные: поэтому предполагают не только совершение общественно опасного деяния: но и наступление общественно опасных последствий: а также установление причинной связи между этими двумя признаками. Однако в силу ч. 2 ст. 9 временем совершения каждого из этих преступлений будет признаваться время окончания именно деяния независимо от времени наступления последствий. Сами же общественно опасные деяния чаще всего выступают здесь в форме действий и лишь иногда — как бездействие. В одном случае такой признак объективной стороны состава преступления: как способ его совершения: сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных он: а также время: место: обстановка: орудия: средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств.

Из всех признаков субъективной стороны значение будет иметь только один — вина. При этом: исходя из ч. 2 ст. 24: для всех преступлений данного вида необ-

ходимо наличие вины в форме умысла: и лишь два квалифицированных состава предусматривают две ее формы: умысел по отношению к деянию и неосторожность в отношении наступивших общественно опасных последствий. Факультативные признаки субъективной стороны так же: как и в вопросе о стороне объективной: не будут иметь значения для квалификации преступления. Так: мотивами совершения таких деяний чаще всего бывают корысть либо хулиганские побуждения: но могут быть и соображения интереса: чувство мести* не исключено совершение их с целью скрыть другое преступление и т. д. Естественно: что особую трудность вызовет проблема отграничения неосторожного и невиновного причинения вреда: что связано с повышенной сложностью и скрытностью процессов: происходящих в сетях и системах ЭВМ.

Субъект нескольких составов является специальным. В остальных случаях им может стать: в принципе: любой человек: особенно если учесть всевозрастающую компьютерную грамотность населения. Ответственность за преступления против компьютерной безопасности наступает с 16 лет (ст. 20 УК).

Диспозиции статей 28-й главы описательные: зачастую — бланкетные или отсылочные. Так: для применения ряда их необходимо обратиться к ст. 35 УК: к нормативно-правовому акту об охране компьютерной информации: правилам эксплуатации ЭВМ и т. п.

Санкции — альтернативные: за исключением двух квалифицированных составов: где они — в силу тяжести последствий преступления — «урезаны» до относительно-определенных.]

Уголовно-правовой анализ ст. 272 гл. 28 УК РФ "Неправомерный доступ к компьютерной информации"

Эта статья: которая: как и последующие: состоит из 2 частей: содержит достаточно много признаков: обязательных для объекта: объективной и субъективной сторон состава преступления. Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ: их системы или сети. Предметом преступления будет компьютерная (машинная) информация: содержащаяся на машинном носителе: в ЭВМ: их

системе или сети: охраняемая законом: т. е. изъятая из открытого оборота на основании закона: иного нормативного правового акта: а также правил внутреннего распорядка: основанных на названных правовых актах.

Контрольные вопросы:

1. Виды материальных носителей сведений.
2. Определение и виды конкурентной разведки.
3. Какие сведения не могут составлять коммерческую тайну?
4. Какие грифы конфиденциальности может использовать предприятие для обозначения степени важности коммерческой информации?
5. Какие виды деятельности в области защиты информации подлежат лицензированию?

Практическое занятие 4

Основные понятия организации безопасности в области защиты информации

Законодательные и административные меры для регулирования вопросов защиты информации на государственном уровне применяются в большинстве научно-технических развитых странах мира. Компьютерные, преступления приобрели в странах с развитой информационно телекоммуникационной инфраструктурой такое широкое распространение, что для борьбы с ними в уголовное законодательство введены специальные статьи.

Первый закон о защите информации был принят в США в 1906 году. В период с 1967 года по настоящее время здесь принят целый ряд федеральных законов, создавших правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации с учётом интересов национальной безопасности страны. Это законы: «О свободе информации» (1967 год), «О секретности» (1974 год), «О праве на финансовую секретность» (1978 год), «О доступе к информации о деятельности ЦРУ» (1984 год), «О компьютерных злоупотреблениях и мошенничестве» (1986 год), «О безопасности компьютерных систем» (1987 год) и другие. В настоящее время в США имеется около 500 законода-

тельных актов по защите информации, ответственности за её разглашение и компьютерные преступления.

Система защиты информации в нашей стране до начала 90-х годов определялась существовавшей политической обстановкой и действовала в основном в интересах Специальных служб государства, Министерства обороны и Военно-промышленного комплекса. Цели защиты информации достигались главным образом за счёт реализации принципа «максимальной секретности», в соответствии, с которым доступ ко многим видам информации был просто ограничен. Никаких законодательных и иных государственных нормативных актов, определяющих защиту информационных прав негосударственных организаций и отдельных граждан, не существовало. Происходящие в стране процессы существенно затронули проблему организации системы защиты информации во всех её сферах - разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Прежние традиционные подходы в современных условиях уже не в состоянии обеспечить требуемый уровень безопасности государственно-значимой и частной конфиденциальной информации, циркулирующей в информационно - телекоммуникационных системах страны.

Нормы и требования российского законодательства включают в себя положения ряда нормативных актов Российской Федерации различного уровня. 19 февраля 1993 года Верховным Советом Российской Федерации был принят закон «О федеральных органах правительственной связи и информации» № 4524-1, который является первым собственно российским правовым нормативным актом. Он ввёл сертификацию деятельности в области защиты информации.

Новым шагом в деле правового обеспечения деятельности в области защиты информации явилось принятие Федеральным собранием России федерального закона «Об информации, информатизации и защите информации» от 20. 02. 95 г. №24-ФЗ. Данный закон впервые официально вводит понятие «конфиденциальной информации», которая рассматривается как документированная информация, доступ к которой ограничивается в соответствии, с законодательством Российской Федерации. В законе устанавливаются общие правовые требования к организации защиты

такой информации в процессе её обработки, хранения и циркуляции в технических устройствах, информационно-телекоммуникационных системах и комплексах. А также этот закон организовывает контроль за осуществлением мероприятий по защите конфиденциальной информации. При этом следует подчеркнуть, что Закон не разделяет государственную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается.

Защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и так далее.

Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Эффективность защиты информации - степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

Безопасность информации (информационная безопасность) - состояние информации, информационных ресурсов и информационных и телекоммуникационных систем, при котором, с требуемой вероятностью, обеспечивается защита информации.

Требования по безопасности информации - руководящие документы ФАПСИ, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности её защиты.

Криптографическое преобразование - преобразование данных при помощи шифрования и (или) выработки имитовставки.

Криптографическая защита - защита данных при помощи криптографического преобразования данных.

И так, информацию достаточно условно можно разделить на сведения, отнесённые к государственной тайне, конфиденциальную информацию, пер - сональную информацию и остальную информацию. Рассматривать первый тип мы не будем.

Конфиденциальная информация - это информация, требующая защиты (любая, её назначение и содержание не оговариваются). Персональные данные - это сведения о гражданах или предприятиях. В соответствии с Федеральным законом №24 «Об информации, информатизации и защите информации» «защите подлежит любая документированная информация, неправомерное обращение, с которой может нанести ущерб собственнику, владельцу или иному лицу». Следует, что ВЫ обязаны, заботится о сохранности своей информации.

Информация, хранимая в компьютерах, не может использоваться как улики в уголовно-гражданских делах, но вполне возможно её применение для выполнения следственных действий.

Защиту информации следует рассматривать как неотъемлемую часть хранения. Невозможно обеспечить серьёзную защиту, не выполняя резервное копирование информации. Обеспечить сохранность копий гораздо проще, для этого достаточно административных мер (хранение в несгораемых сейфах). Ёмкость стримеров, CD-R, CD-RW, DVD достаточна для составления резервных копий и восстановления из них в кратчайшие сроки. Пренебрежение данными мерами чревато по техническим соображениям - надёжность технических средств хранения далека от 100% (вероятность сбоя Windows в течение рабочего дня достаточно велика) и потерять информацию по причине программного сбоя или поломки накопителя, очень обидно и дорого.

Можно выделить следующие методы защиты информации:

Административные (организационные) меры

Правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации, вводимые в действие административным путём. Сюда же можно отнести нормативно-правовые и морально-этические средства защиты.

Нормативно-правовые - включают в себя законы, правовые акты и механизмы их реализации.

Морально-этические - правила и нормы поведения, направленные на обеспечение безопасности информации, не закреплённые законодательно, но поддержива-

емые в коллективах через традиции и механизм общественного мнения.

Применяют следующие организационные мероприятия:

- принятие правовых обязательств со стороны сотрудников в отношении сохранности доверенных им сведений (информации);
- определение уровней (категорий) конфиденциальности защищаемой информации;
- ограничение доступа в те места и к той технике, где сосредоточена конфиденциальная информация;
- установление порядка обработки защищаемой информации (введение охраняемых зон, ограничение времени обработки и т. п.);
- грамотное ведение резервного копирования информации;
- организация договорных связей с государственными органами регулирования в области защиты информации.

Выполнение этих правил может дать ощутимый эффект и значительно сэкономить средства. Если территория предприятия имеет охрану, персоналу можно доверять, локальная сеть не имеет выходов в глобальные сети, то такую защищённость можно признать очень высокой. Однако такое практически не выполнимо, но пренебрегать этим методом нельзя. Он, как правило, дополняет и контролирует другие методы.

Технические методы зашиты

Технические средства - комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки обрабатываемой или хранящейся информации путём исключения несанкционированного доступа к ней с помощью технических средств съёма.

Применяют следующие технические мероприятия:

определение возможности с помощью технических средств наблюдения отображаемой информации посторонними лицами;

максимальное разнесение информационных кабелей между собой и относительно проводящих конструкций;

анализ расположения предприятия, территории вокруг и подведённые комму-

никации;

проверка используемой техники на соответствие величины побочных излучений допустимым уровням;

экранирование помещения с техникой или техники в помещениях;

использование специальных устройств и средств пассивной и активной защиты. (Пассивные средства основаны на снижении уровня звуковой мощности акустического сигнала. Активные устройства кспользуют дополнительный источник энергии для модуляции акустического сигнала.)

Разработка и реализация мероприятий по защите информации от утечки по техническим каналам осуществляется спецорганизациями, обладающими необходимыми лицензиями компетентных органов.

Технические методы защиты компьютерной информации подразделяемся на:

Аппаратные;

Программные;

Аппаратно-программные

К техническим средствам защиты компьютерной информации также относятся:

Защита средствами операционной системы. Практически все операционные системы имеют встроенные разрешения на доступ, которые позволяют только определённым пользователям осуществлять доступ к компьютеру (его жёсткому диску, памяти, сетевому соединению). Такой доступ реализуется через процедуру входа в систему. Если пользователь не предоставил имя и пароль, ОС не позволит ему использовать компьютер. Но даже после того, как пользователь вошёл в систему, определённые файлы могут остаться недоступными.

Блокировка загрузки оперативной системы

Физическое уничтожение накопителя. (Электромагнит, пробивающий насквозь накопитель или дискету; пиропатрон, установленный под накопителем.) Данному методу трудно что-то противопоставить, но при ложном срабатывании велика стоимость потерь.

Стирание информации. Метод имеет много общего с предыдущим, но при

срабатывании теряется только информация, а не накопитель. Недостаток этого метода заключается в том, программное стирание и комплексы, использующие данную функцию, требуют постоянного нахождения компьютера под напряжением.

Шифрование данных

Направления защиты и соответствующие им средства.

Защита от несанкционированного доступа (НСД) к ресурсам автономно работающих и сетевых персональных компьютеров. Осуществляется с помощью электронных замков, аппаратных шифраторов и т. д.

Защита серверов и отдельных пользователей сети Intenet от злонамеренных хакеров, проникающих извне. Для этого используются межсетевые экраны (брандмауэры).

Защита секретной, конфиденциальной и личной информации от- чтения посторонними лицами и целенаправленного ее искажения. Осуществляется чаще всего с помощью криптографических средств, а также с помощью электронной цифровой подписи.

Защита программного обеспечения от нелегального копирования

Защита от утечки информации по побочным каналам (по цепям питания, каналу электромагнитного излучения от компьютера или монитора). Здесь применяются - экранирование помещения, использование генератора шума, специальных мониторов и комплектующих компьютера, обладающих наименьшей зоной излучения

Защита от шпионских устройств, устанавливаемых непосредственно в комплектующие компьютера, так же как и измерения зоны излучения, выполняется специальными организациями.

Особая роль в защите информации отводиться борьбе с компьютерными вирусами.

Контрольные вопросы:

1. Характеристика методов с применением специализированных аппаратных средств?
2. Характеристика методов основанных на анализе биометрических характеристик пользователя?

3. Разграничение доступа предполагает…?
4. Протоколирование и аудит предполагает…?
5. Цели реализация протоколирования и аудита?
6. Криптографическое преобразование данных предполагает…?
7. Режим секретности это?

Практическое занятие 5

Понятие допуска к государственной тайне

Согласно части третьей статьи 21 Закона РФ «О государственной тайне» данная процедура предусматривает:

принятие гражданином на себя обязательств перед государством по нераспространению доверенных ему сведений, составляющих государственную тайну;

согласие на частные, временные ограничения его прав;

письменное согласие на проведение в его отношении проверочных мероприятий;

определение видов, размеров и порядка предоставления соответствующих социальных гарантий;

ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

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

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке. Принудительно указанная процедура не может быть проведена даже в том случае, если необходимость в подключении работника к работе с государственной тайной возникла в середине трудовой деятельности работника.

Для лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов, установлен особый порядок допуска к государственной тайне и определен он в Положении о порядке до-

пуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне, которое было утверждено постановлением Правительства РФ от 22.08.1998 № 1103.

В соответствии с указанным Положением лица, имеющие двойное гражданство, полученное в соответствии с Законом РСФСР «О гражданстве РСФСР», допускаются к государственной тайне в порядке, определенном для должностных лиц и граждан. Указанные лица допускаются к сведениям, составляющим государственную тайну, с грифом «секретно» только после проведения проверочных мероприятий органами федеральной службы безопасности.

Лица без гражданства могут быть допущены к сведениям, составляющим государственную тайну, на основании решения Правительства РФ. При этом к сведениям особой важности и совершенно секретным сведениям лица без гражданства, как правило, не допускаются. Инициатором принятия такого решения могут выступать только руководители органов государственной власти, наделенные правом по отнесению сведений к государственной тайне, и руководители органов государственной власти субъектов Российской Федерации, если они сами непосредственно заинтересованы в допуске лиц без гражданства к государственной тайне. Для этого они вносят в Правительство РФ проект соответствующего решения, к которому прилагают мотивированное обоснование необходимости допуска, материалы согласования вопроса с Федеральной службой безопасности России и согласованный с Межведомственной комиссией по защите государственной тайны перечень сведений, составляющих государственную тайну, к которым предлагается допустить лицо без гражданства. Мотивированное обоснование должно содержать оценку тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Иностранные граждане допускаются к государственной тайне на основании международного договора, предусматривающего обязательства иностранного государства по защите передаваемых ему сведений, составляющих государственную тайну. При этом иностранные граждане допускаются только к тем сведениям, в отношении которых выполнены процедуры, предусмотренные Положением о подго-

товке к передаче сведений, составляющих государственную тайну, другим государствам, утвержденным постановлением Правительства РФ от 02.08.1997 № 973. Решение о допуске иностранных граждан к государственной тайне принимается руководителями органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, предприятий, учреждений, организаций, уполномоченных Правительством РФ осуществлять передачу сведений, составляющих государственную тайну, другому государству. Это решение должно быть согласовано с Федеральной службой безопасности РФ.

Порядок допуска к государственной тайне лиц из числа эмигрантов и реэмигрантов определяется исходя из гражданства указанных лиц на момент возбуждения ходатайства о допуске их к государственной тайне.

Сведения о гражданстве соискателя вакансии определяются на основании представленных им документов, удостоверяющих личность, а также информации, сообщаемой в специальной анкете. Они, как и другие сведения, предоставленные желающим получить работу, подлежат проверке.

Рассмотрим подробно процедуру решения вопроса о допуске претендующего на работу лица к государственной тайне.

Контрольные вопросы:

1. Допуск к информации, составляющей государственную тайну это…?
2. Допуск должностных лиц и граждан к государственной тайне предусматривает?
3. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне?
4. В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска…?
5. Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются…?
6. Допуск граждан по третьей форме осуществляется…?
7. Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются льготы…?

Практическое занятие 6

Порядок и особенности допуска к государственной тайне отдельных категорий граждан

Для каждой из трех групп сведений — секретных, совершенно секретных и составляющих особую важность — допуск производится по установленной форме.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливают- ся следующие формы допуска:

первая форма — для лиц, допускаемых к сведениям особой важности;

вторая форма — для лиц, допускаемых к совершенно секретным сведениям;

третья форма — для лиц, допускаемых к секретным сведениям.

Наличие у лица допуска к сведениям более высокой степени секретности является основанием для его до- ступа к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности РФ и ее территориальными органами во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.

Допуск граждан по третьей форме по общему правилу осуществляется руководителем организации без про- ведения проверочных мероприятий органами безопасности.

Сами руководители допускаются к секретным сведениям, то есть по третьей форме, только после проведения в отношении их проверочных мероприятий.

Органы безопасности имеют право определять те организации, в которых допуск к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности. В этом случае допуск по третьей форме оформляется после проверочных мероприятий. Проверочные мероприятия органы безопасности могут назначить и в том случае, если у руководителя организации, не включенной в перечень объектов, на которых допуск к секретным сведениям осу-

ществляется только после проведения проверочных мероприятий органами безопасности, имеются обоснованные сомнения в достоверности анкетных данных кандидата на должность, замещение которой предполагает оформление допуска третьей степени.

Граждане, работающие в филиалах организаций (обособленных подразделениях, постоянно действующих экспедициях и т.п.) и постоянно проживающие по месту их нахождения, оформляются на допуск руководителями этих филиалов (подразделений, экспедиций и т.п.). Проверочные мероприятия в этом случае осуществляются органами безопасности по месту расположения (республика, край, область) этих объектов.

Контрольные вопросы:

1. Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях…?
2. В каких правах должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены?
3. Подразделения по защите государственной тайны предназначены для…?
4. Что является основой допуска к государственной тайне?
5. Порядок допуска предприятий, учреждений и организаций к государственной тайне?
6. Органами, уполномоченными на ведение лицензионной деятельности, являются?

Заочная форма обучения

Практическое занятие 1

Законодательство РФ в области информационной безопасности

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;

- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);

- процедурного (меры безопасности, ориентированные на людей);

- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);

- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту

силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 – право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в

процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Контрольные вопросы:

1. Какие общественные отношения являются предметом правового регулирования в информационной сфере?
2. Какова структура информационного законодательства РФ?
3. Какой закон установил принципы правового регулирования отношений, в информационной сфере?
4. Какие документы составляют правовую базу в информационной сфере?
5. На каком законе РФ основывается система защиты государственных секретов?

Практическое занятие 2

Правовые режимы защиты информации конфиденциального характера. Государственное регулирование деятельности в области защиты информации.

Коммерческая тайна - режим, позволяющий избежать неоправданных расходов, увеличить доходы, сохранить положение на рынке товаров, услуг или получить иную коммерческую выгоду.

Наиболее опасными формами проявления уязвимости конфиденциальной документированной информации являются потеря, хищение и разглашение - первые две одновременно могут привести и к утрате, и к утечке информации, вторая (хищение информации при сохранности носителя) и третья могут не обнаружиться, со

всеми вытекающими из этого последствиями. Поэтому необходимо уделять одинаковое внимание предотвращению как утраты защищаемой документированной информации, так и ее утечки, т.к. ущерб собственнику информации наносится в любом случае.

По данным мировой статистики, утрата 20% информации ведет к разорению 65% фирм и компаний. 1

Защита конфиденциальной документированной информации от утраты и утечки осуществляется в определенной мере конфиденциальным делопроизводством. Документирование конфиденциальной информации и организация работы с конфиденциальными документами должны производиться в условиях обеспечения их защиты, и вместе с тем многие вопросы защиты решаются в ходе и путем осуществления систематических операций по учету и обработке документов.

Сегодня, когда предприятия самостоятельно планируют и осуществляют свою деятельность, любые сведения, навыки и приёмы, неизвестные другим, могут дать значительные конкурентные преимущества. А утечка такой информации может привести к серьёзным потерям. В связи с этим особенно важное значение придается понятию - коммерческая тайна.

Коммерческая тайна - совокупность не являющихся государственной тайной сведений, представляющих ценность для субъекта предпринимательства, разглашение которых может нанести ему ущерб и, в отношении которых приняты надлежащие меры по сохранению конфиденциальности.

В соответствии с Законом «О коммерческой тайне» «коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

Информация, составляющая коммерческую тайну: научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в т.ч. составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим

лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны (ст. 3).

Нормы о коммерческой тайне содержатся более чем в 30 законодательных актах, среди которых порядок отнесения информации к конфиденциальной и виды конфиденциальной информации установлены Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» в соответствии с которым к конфиденциальной информации относятся:

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

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

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

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами;

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них и некоторые другие.

Но не вся информация субъекта хозяйствования может составлять коммерческую тайну. Так, в законе «О коммерческой тайне» представлен список сведений, не относящихся к коммерческой тайне. В частности это:

- сведения, содержащиеся в документах, подтверждающие право осуществлять коммерческую деятельность (в уставах, лицензиях и т.п.).

Документ, содержащий коммерческую тайну - это зафиксированная информация, составляющая коммерческую тайну, с реквизитами, позволяющими его идентифицировать;

- сведения о наличии на предприятии опасных факторов, влиянии предприятия на окружающую среду и граждан;

- о составе и численности работников, условиях труда, случаях профзаболеваний и производственного травматизма, о наличии вакансий, задолженности по выплате зарплаты и ряд других сведений.

Таким образом, коммерческая тайна является одним из видов конфиденциальной информации.

За разглашение коммерческой тайны предусматривается административная или уголовная ответственность. Согласно Закону «О коммерческой тайне» привлечь к ответственности в судебном порядке за разглашение коммерческой тайны и (или) использование коммерческой тайны в личных, предпринимательских, иных целях не связанных с выполнением трудовых обязанностей, возможно только в случае установления работодателем режима коммерческой тайны. При этом, если на предприятии или в организации положение о коммерческой тайне не введено, то, согласно закону, нет и информации, составляющей коммерческую тайну.

Первым шагом по реализации мер защиты коммерческой тайны, является принятие на предприятии «Положения (Инструкции) по обеспечению сохранности коммерческой тайны», в которых определяются:

- состав и объем сведений, составляющих коммерческую тайну;

- порядок присвоения грифа «Секрет предприятия» сведениям, работам и изделиям и его снятия;

- процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

- порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

- организация контроля за порядком использования сведений, составляющих коммерческую тайну;

- процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-

либо совместных действий;

- порядок применения предусмотренных законодательством мер дисциплинарного и материального воздействия на работников, разгласивших коммерческую тайну;

- возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

Руководство по введению режима коммерческой тайны.

Для того чтобы ввести в организации режим коммерческой тайны, необходимо разработать определенный пакет документов и провести ряд организационных мероприятий.

Во-первых, сначала следует четко определить в виде перечня совокупность сведений конфиденциального характера, которые будут составлять коммерческую тайну организации.

Во-вторых, определяются способы защиты информации, лица, ответственные за её сохранность, формы ответственности за разглашение.

Необходимо создание «Положения о коммерческой тайне», которое утверждается приказом, в котором отображается каким образом будет осуществляться защита коммерческой тайны, как будут маркироваться ее носители, кто будет иметь право с ними работать, как это будет учитываться, на кого будет возложена функция контроля, какова будет ответственность за разглашение коммерческой тайны и т. д.

В-третьих, осуществить регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров:

- организовать подписание всеми работниками, имеющими доступ к коммерческой тайне, «Обязательства о соблюдении коммерческой тайны», а им, в свою очередь, должны быть обеспечены все необходимые условия для надежного хранения важной информации;

- внести соответствующие пункты в Должностные инструкции, Положения об отделах (структурных подразделениях) и иную организационнораспорядительную

документацию компании.

- в Договоры с контрагентами необходимо внести пункт о том, что все сведения, связанные с договором и его исполнением, являются конфиденциальными и составляют коммерческую тайну организации.

Все сведения, связанные с договором подлежат передаче и разглашению третьим лицам за (исключением государственных (муниципальных) контрольно-надзорных, судебных и других органов) только по обоюдному соглашению сторон.

В-четвертых, необходимо обеспечить ознакомление под роспись всех сотрудников организации (работающих в настоящее время и вновь принимаемых) с разработанными и вводимыми документами и взять у каждого письменное обязательство по сохранению конфиденциальности составляющих коммерческую тайну сведений, которые стали известны в процессе работы в организации.

В этом же документе указать обязанность по неразглашению коммерческой тайны как во время работы в организации, так и в течение определенного времени после увольнения.

В пятых, ограничить доступ к информации, составляющей коммерческую тайну, путём установления порядка обращения с этой информацией и контроля за соблюдением такого порядка:

- утвердить «Приказ о доступе к коммерческой тайне» в отношении всех работников;

- при увольнении работников утверждать «Приказ о прекращении доступа к коммерческой тайне».

В шестых, вести учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена.

Для этого необходимо заполнять «Табель учёта лиц, имеющих допуск к коммерческой тайне» - вносить информацию по приказам о доступе и приказам о прекращении доступа к коммерческой тайне в случае увольнения либо при переводе на должность, не предполагающую доступ к коммерческой тайне, либо при изменении должностных обязанностей, которое не предполагает доступ к коммерческой тайне; либо в случае допуска сотрудников к информации, составляющей коммерческую

тайну.

И наконец, наносить на материальные носители, содержащие информацию, составляющую коммерческую тайну, гриф «Коммерческая тайна».

Включать в состав реквизитов документов, содержащих такую информацию, гриф «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем).

При этом, следует создать работникам все необходимые условия для соблюдения установленного компанией режима коммерческой тайны. Как правило, такими условиями являются создание возможности хранить документы, содержащие конфиденциальные сведения в запираемом месте, обеспечение доступа к персональному компьютеру, локальной сети и сети Интернет по персональному логину и паролю и т. д.

Весьма желательно сразу после введения режима коммерческой тайны, а также в дальнейшем проводить с работниками обучающие мероприятия, в процессе которых рассказывать и объяснять, зачем нужен режим коммерческой тайны, в чем он состоит и т.д.

Практика показывает, что защита конфиденциальных сведений, составляющих коммерческую тайну, равно как и интересов фирмы в целом, наилучшим образом осуществляется, когда каждый работник четко понимает требования, содержащиеся в организационно-распорядительных документах компании, и осознает важность их выполнения. В подобном случае можно говорить о наличии в коллективе высокой деловой и правовой культуры, корпоративного режима конфиденциальности и быть уверенным, что интересы фирмы защищены наилучшим образом.

Одним из основополагающих элементов системы мер по обеспечению безопасности информации, составляющей коммерческую тайну предприятия, является выделение документов, содержащих охраняемые сведения, из общего информационного потока. Выделение таких документов осуществляется присвоением им грифа «Коммерческая тайна».

Проставление грифа «Коммерческая тайна» является меткой, которая включает систему защиты охраняемой информации. Поэтому, если система защиты информации функционирует надежно, своевременность установления грифа «Коммерческая тайна» охраняемой информации имеет принципиально важное значение для ее защиты.

Вместе с тем, в соответствии с общепринятым понятием коммерческой тайны, важным является и то обстоятельство, которое позволяет ограничительный гриф по истечении надобности оперативно снимать.

Предлагаемый порядок установления и снятия грифа «Коммерческая тайна» не окажет должного влияния на защиту охраняемой информации вне связи с другими элементами системы.

Порядок установления и снятия грифа «Коммерческая тайна» для различных предприятий, фирм может различаться. Однако, во всех случаях он должен предусматривать следующие аспекты:

- кто, когда и как устанавливает гриф «Коммерческая тайна» документу и изделие;

- кто, когда и как этот гриф снимает;

- права, обязанности и ответственность должностных лиц, устанавливающих и снимающих ограничительный гриф;

- контроль за этой сферой деятельности.

При необходимости, можно вводить ограничительные пометки психологического характера. Например, на определенные категории документов, содержащих охраняемые сведения, можно прикреплять ярко выполненные таблички: «На столе не оставлять», «Хранить в сейфе».

На документах гриф «Коммерческая тайна» проставляется на первом (титульном) листе и на обложке в правом углу в соответствии с ГОСТ 6.3990.

Если документы с грифом «Коммерческая тайна» направляются с сопроводительным письмом, то на нем этот гриф также проставляется.

Следует помнить, что научно-техническую, проектно-технологическую и другую документацию, содержащую сведения, составляющие коммерческую тайну,

необходимо оформлять таким образом, чтобы сведения, составляющие коммерческую тайну, были максимально локализованы (например, собраны в отдельном томе или разделе документации). Это позволит уменьшить объем документов, что является одним из важных условий обеспечения надлежащей защиты охраняемых сведений.

Снятие грифа «Коммерческая тайна» с документа осуществляет должностное лицо, подписавшее (утвердившее) этот документ или техническую документацию на изделие, или руководитель предприятия. Основанием для снятия являются:

- требования заказчика;

- соответствующая корректировка «Перечня сведений, составляющих коммерческую тайну» предприятия;

- гриф «Коммерческая тайна» был установлен неправильно;

- истечение установленного срока действия грифа.

О снятии грифа «Коммерческая тайна» соответствующее должностное лицо делает отметку на самом документе и в технической (сопроводительной) документации на изделие путем зачеркивания грифа с проставлением своей подписи и даты.

Лица, осуществляющие учет документов с грифом «Коммерческая тайна», делают необходимые отметки в соответствующих учетных документах (формах) с указанием фамилии лица, снявшего гриф, и даты снятия.

О снятии грифа «Коммерческая тайна» предприятие, устанавливавшее гриф, извещает все предприятия, связанные договорными обязательствами с предприятием-разработчиком в части охраны коммерческой тайны.

Извещение является основанием для снятия грифа «Коммерческая тайна» с полученных документов. Выполняют эту операцию лица, осуществляющие учет документов с грифом «Коммерческая тайна».

Одним из инструментов по охране коммерческой тайны является Договор (Соглашение), которым уделяется самое серьезное внимание, поскольку в случае разглашения работником информации, составляющей коммерческую тайну работодателя, такие соглашения составят юридическую основу для привлечения работника к ответственности и взыскания причиненного ущерба. Подобные соглашения могут

заключаться как в виде отдельного документа, так и в виде условия в трудовом договоре.

В трудовом договоре либо в его неотъемлемой части (обязательстве о неразглашении информации, составляющей коммерческую тайну) следует предусмотреть порядок ознакомления работника с действующими в организации положениями и инструкциями по обеспечению сохранности коммерческой тайны. Кроме того, следует определять объем информации, передаваемой каждому конкретному работнику, за которую он должен нести ответственность.

Соглашения о неразглашении заключаются и с контрагентами по различным гражданско-правовым договорам, связанным с раскрытием сторонами по договору различной секретной информации. Для отдельных видов договоров такое условие прямо предусмотрено ГК РФ.

Обязанности по обеспечению сохранности коммерческой тайны возложены на руководителя организации. В связи с этим в контракт, заключаемый с руководителем при его найме, назначении или избрании, целесообразно включить положения, обуславливающие порядок сохранения коммерческой тайны руководителем.

В качестве примера опыт решения проблемы защиты коммерческой тайны, в следующей главе рассмотрим порядок организации работы по обеспечению защиты информации, составляющей коммерческую тайну ОАО «ФСК ЕЭС».

Контрольные вопросы:

1. Какие методы защиты лежат в основе комплексной системы информационной безопасности любого объекта.
2. С принятием каких законов началось формирование законодательства в информационной сфере?
3. Признаки и объекты профессиональной тайны?
4. Какие сведения относятся к служебной тайне?
5. На каких правовых актах основана защита служебной и коммерческой информации на предприятии?

Практическое занятие 3

Основные понятия организации безопасности в области защиты информации

Законодательные и административные меры для регулирования вопросов защиты информации на государственном уровне применяются в большинстве научно-технических развитых странах мира. Компьютерные, преступления приобрели в странах с развитой информационно телекоммуникационной инфраструктурой такое широкое распространение, что для борьбы с ними в уголовное законодательство введены специальные статьи.

Первый закон о защите информации был принят в США в 1906 году. В период с 1967 года по настоящее время здесь принят целый ряд федеральных законов, создавших правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации с учётом интересов национальной безопасности страны. Это законы: «О свободе информации» (1967 год), «О секретности» (1974 год), «О праве на финансовую секретность» (1978 год), «О доступе к информации о деятельности ЦРУ» (1984 год), «О компьютерных злоупотреблениях и мошенничестве» (1986 год), «О безопасности компьютерных систем» (1987 год) и другие. В настоящее время в США имеется около 500 законодательных актов по защите информации, ответственности за её разглашение и компьютерные преступления.

Система защиты информации в нашей стране до начала 90-х годов определялась существовавшей политической обстановкой и действовала в основном в интересах Специальных служб государства, Министерства обороны и Военно-промышленного комплекса. Цели защиты информации достигались главным образом за счёт реализации принципа «максимальной секретности», в соответствии, с которым доступ ко многим видам информации был просто ограничен. Никаких законодательных и иных государственных нормативных актов, определяющих защиту информационных прав негосударственных организаций и отдельных граждан, не

существовало. Происходящие в стране процессы существенно затронули проблему организации системы защиты информации во всех её сферах - разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Прежние традиционные подходы в современных условиях уже не в состоянии обеспечить требуемый уровень безопасности государственно-значимой и частной конфиденциальной информации, циркулирующей в информационно - телекоммуникационных системах страны.

Нормы и требования российского законодательства включают в себя положения ряда нормативных актов Российской Федерации различного уровня. 19 февраля 1993 года Верховным Советом Российской Федерации был принят закон «О федеральных органах правительственной связи и информации» № 4524-1, который является первым собственно российским правовым нормативным актом. Он ввёл сертификацию деятельности в области защиты информации.

Новым шагом в деле правового обеспечения деятельности в области защиты информации явилось принятие Федеральным собранием России федерального закона «Об информации, информатизации и защите информации» от 20. 02. 95 г. №24-ФЗ. Данный закон впервые официально вводит понятие «конфиденциальной информации», которая рассматривается как документированная информация, доступ к которой ограничивается в соответствии, с законодательством Российской Федерации. В законе устанавливаются общие правовые требования к организации защиты такой информации в процессе её обработки, хранения и циркуляции в технических устройствах, информационно-телекоммуникационных системах и комплексах. А также этот закон организовывает контроль за осуществлением мероприятий по защите конфиденциальной информации. При этом следует подчеркнуть, что Закон не разделяет государственную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается.

Защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и так далее.

Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Эффективность защиты информации - степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

Безопасность информации (информационная безопасность) - состояние информации, информационных ресурсов и информационных и телекоммуникационных систем, при котором, с требуемой вероятностью, обеспечивается защита информации.

Требования по безопасности информации - руководящие документы ФАПСИ, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности её защиты.

Криптографическое преобразование - преобразование данных при помощи шифрования и (или) выработки имитовставки.

Криптографическая защита - защита данных при помощи криптографического преобразования данных.

И так, информацию достаточно условно можно разделить на сведения, отнесённые к государственной тайне, конфиденциальную информацию, пер - сональную информацию и остальную информацию. Рассматривать первый тип мы не будем.

Конфиденциальная информация - это информация, требующая защиты (любая, её назначение и содержание не оговариваются). Персональные данные - это сведения о гражданах или предприятиях. В соответствии с Федеральным законом №24 «Об информации, информатизации и защите информации» «защите подлежит любая документированная информация, неправомерное обращение, с которой может нанести ущерб собственнику, владельцу или иному лицу». Следует, что ВЫ обязаны, заботится о сохранности своей информации.

Информация, хранимая в компьютерах, не может использоваться как улики в уголовно-гражданских делах, но вполне возможно её применение для выполнения следственных действий.

Защиту информации следует рассматривать как неотъемлемую часть хранения. Невозможно обеспечить серьёзную защиту, не выполняя резервное копирование информации. Обеспечить сохранность копий гораздо проще, для этого достаточно административных мер (хранение в несгораемых сейфах). Ёмкость стримеров, CD-R, CD-RW, DVD достаточна для составления резервных копий и восстановления из них в кратчайшие сроки. Пренебрежение данными мерами чревато по техническим соображениям - надёжность технических средств хранения далека от 100% (вероятность сбоя Windows в течение рабочего дня достаточно велика) и потерять информацию по причине программного сбоя или поломки накопителя, очень обидно и дорого.

Можно выделить следующие методы защиты информации:

Административные (организационные) меры

Правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации, вводимые в действие административным путём. Сюда же можно отнести нормативно-правовые и морально-этические средства защиты.

Нормативно-правовые - включают в себя законы, правовые акты и механизмы их реализации.

Морально-этические - правила и нормы поведения, направленные на обеспечение безопасности информации, не закреплённые законодательно, но поддерживаемые в коллективах через традиции и механизм общественного мнения.

Применяют следующие организационные мероприятия:

- принятие правовых обязательств со стороны сотрудников в отношении сохранности доверенных им сведений (информации);
- определение уровней (категорий) конфиденциальности защищаемой информации;
- ограничение доступа в те места и к той технике, где сосредоточена конфиденциальная информация;
- установление порядка обработки защищаемой информации (введение охраняемых зон, ограничение времени обработки и т. п.);

- грамотное ведение резервного копирования информации;
- организация договорных связей с государственными органами регулирования в области защиты информации.

Выполнение этих правил может дать ощутимый эффект и значительно сэкономить средства. Если территория предприятия имеет охрану, персоналу можно доверять, локальная сеть не имеет выходов в глобальные сети, то такую защищённость можно признать очень высокой. Однако такое практически не выполнимо, но пренебрегать этим методом нельзя. Он, как правило, дополняет и контролирует другие методы.

Технические методы зашиты

Технические средства - комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки обрабатываемой или хранящейся информации путём исключения несанкционированного доступа к ней с помощью технических средств съёма.

Применяют следующие технические мероприятия:

определение возможности с помощью технических средств наблюдения отображаемой информации посторонними лицами;

максимальное разнесение информационных кабелей между собой и относительно проводящих конструкций;

анализ расположения предприятия, территории вокруг и подведённые коммуникации;

проверка используемой техники на соответствие величины побочных излучений допустимым уровням;

экранирование помещения с техникой или техники в помещениях;

использование специальных устройств и средств пассивной и активной защиты. (Пассивные средства основаны на снижении уровня звуковой мощности акустического сигнала. Активные устройства кспользуют дополнительный источник энергии для модуляции акустического сигнала.)

Разработка и реализация мероприятий по защите информации от утечки по техническим каналам осуществляется спецорганизациями, обладающими необхо-

димыми лицензиями компетентных органов.

Технические методы защиты компьютерной информации подразделяемся на:

Аппаратные;

Программные;

Аппаратно-программные

К техническим средствам защиты компьютерной информации также относятся:

Защита средствами операционной системы. Практически все операционные системы имеют встроенные разрешения на доступ, которые позволяют только определённым пользователям осуществлять доступ к компьютеру (его жёсткому диску, памяти, сетевому соединению). Такой доступ реализуется через процедуру входа в систему. Если пользователь не предоставил имя и пароль, ОС не позволит ему использовать компьютер. Но даже после того, как пользователь вошёл в систему, определённые файлы могут остаться недоступными.

Блокировка загрузки оперативной системы

Физическое уничтожение накопителя. (Электромагнит, пробивающий насквозь накопитель или дискету; пиропатрон, установленный под накопителем.) Данному методу трудно что-то противопоставить, но при ложном срабатывании велика стоимость потерь.

Стирание информации. Метод имеет много общего с предыдущим, но при срабатывании теряется только информация, а не накопитель. Недостаток этого метода заключается в том, программное стирание и комплексы, использующие данную функцию, требуют постоянного нахождения компьютера под напряжением.

Шифрование данных

Направления защиты и соответствующие им средства.

Защита от несанкционированного доступа (НСД) к ресурсам автономно работающих и сетевых персональных компьютеров. Осуществляется с помощью электронных замков, аппаратных шифраторов и т. д.

Защита серверов и отдельных пользователей сети Intenet от злонамеренных хакеров, проникающих извне. Для этого используются межсетевые экраны (бранд-

мауэры).

Защита секретной, конфиденциальной и личной информации от- чтения посторонними лицами и целенаправленного ее искажения. Осуществляется чаще всего с помощью криптографических средств, а также с помощью электронной цифровой подписи.

Защита программного обеспечения от нелегального копирования

Защита от утечки информации по побочным каналам (по цепям питания, каналу электромагнитного излучения от компьютера или монитора). Здесь применяются - экранирование помещения, использование генератора шума, специальных мониторов и комплектующих компьютера, обладающих наименьшей зоной излучения

Защита от шпионских устройств, устанавливаемых непосредственно в комплектующие компьютера, так же как и измерения зоны излучения, выполняется специальными организациями.

Особая роль в защите информации отводиться борьбе с компьютерными вирусами.

Контрольные вопросы:

1. Характеристика методов с применением специализированных аппаратных средств?
2. Характеристика методов основанных на анализе биометрических характеристик пользователя?
3. Разграничение доступа предполагает…?
4. Протоколирование и аудит предполагает…?
5. Цели реализация протоколирования и аудита?
6. Криптографическое преобразование данных предполагает…?
7. Режим секретности это?

Практическое занятие 4

Понятие допуска к государственной тайне

Согласно части третьей статьи 21 Закона РФ «О государственной тайне» данная процедура предусматривает:

принятие гражданином на себя обязательств перед государством по нераспространению доверенных ему сведений, составляющих государственную тайну;

согласие на частные, временные ограничения его прав;

письменное согласие на проведение в его отношении проверочных мероприятий;

определение видов, размеров и порядка предоставления соответствующих социальных гарантий;

ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

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

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке. Принудительно указанная процедура не может быть проведена даже в том случае, если необходимость в подключении работника к работе с государственной тайной возникла в середине трудовой деятельности работника.

Для лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов, установлен особый порядок допуска к государственной тайне и определен он в Положении о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне, которое было утверждено постановлением Правительства РФ от 22.08.1998 № 1103.

В соответствии с указанным Положением лица, имеющие двойное гражданство, полученное в соответствии с Законом РСФСР «О гражданстве РСФСР», допускаются к государственной тайне в порядке, определенном для должностных лиц и граждан. Указанные лица допускаются к сведениям, составляющим государственную тайну, с грифом «секретно» только после проведения проверочных мероприятий органами федеральной службы безопасности.

Лица без гражданства могут быть допущены к сведениям, составляющим гос-

ударственную тайну, на основании решения Правительства РФ. При этом к сведениям особой важности и совершенно секретным сведениям лица без гражданства, как правило, не допускаются. Инициатором принятия такого решения могут выступать только руководители органов государственной власти, наделенные правом по отнесению сведений к государственной тайне, и руководители органов государственной власти субъектов Российской Федерации, если они сами непосредственно заинтересованы в допуске лиц без гражданства к государственной тайне. Для этого они вносят в Правительство РФ проект соответствующего решения, к которому прилагают мотивированное обоснование необходимости допуска, материалы согласования вопроса с Федеральной службой безопасности России и согласованный с Межведомственной комиссией по защите государственной тайны перечень сведений, составляющих государственную тайну, к которым предлагается допустить лицо без гражданства. Мотивированное обоснование должно содержать оценку тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Иностранные граждане допускаются к государственной тайне на основании международного договора, предусматривающего обязательства иностранного государства по защите передаваемых ему сведений, составляющих государственную тайну. При этом иностранные граждане допускаются только к тем сведениям, в отношении которых выполнены процедуры, предусмотренные Положением о подготовке к передаче сведений, составляющих государственную тайну, другим государствам, утвержденным постановлением Правительства РФ от 02.08.1997 № 973. Решение о допуске иностранных граждан к государственной тайне принимается руководителями органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, предприятий, учреждений, организаций, уполномоченных Правительством РФ осуществлять передачу сведений, составляющих государственную тайну, другому государству. Это решение должно быть согласовано с Федеральной службой безопасности РФ.

Порядок допуска к государственной тайне лиц из числа эмигрантов и реэмигрантов определяется исходя из гражданства указанных лиц на момент возбуждения

ходатайства о допуске их к государственной тайне.

Сведения о гражданстве соискателя вакансии определяются на основании представленных им документов, удостоверяющих личность, а также информации, сообщаемой в специальной анкете. Они, как и другие сведения, предоставленные желающим получить работу, подлежат проверке.

Рассмотрим подробно процедуру решения вопроса о допуске претендующего на работу лица к государственной тайне.

Контрольные вопросы:

1. Допуск должностных лиц и граждан к государственной тайне предусматривает?
2. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне?
3. В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска…?
4. Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются…?

Литература

1. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации: Практикум: учеб. Пособие - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.
2. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учеб. Пособие. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.
3. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос АРВ, 2003.
4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ.
5. О связи: Федеральный закон от 07.07.2003 г. № 126-ФЗ.
6. Об электронной цифровой подписи: Федеральный закон от 10.01.2002 г. № 1-ФЗ.
7. О коммерческой тайне: Федеральный закон от 29.07.2004 г. № 98-ФЗ.
8. О персональных данных: Федеральный закон от 27.07.2006 г. № 152.-ФЗ.
9. О лицензировании отдельных видов деятельности: Федеральный закон от 08.08.2001 г. № 128-ФЗ.
10. Об утверждении перечня сведений конфиденциального характера: Указ Президента Российской Федерации от 06.03.1997 г. № 188.