МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«Организация защиты конфиденциальной информации на объектах информатизации»
для студентов
Специальности 10.05.03 Информационная безопасность автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Организация защиты конфиденциальной информации на объектах информатизации» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» системных знаний и практических навыков по обеспечению конфиденциальности информации в информационных системах и на объектах информатизации. В процессе освоения дисциплины студенты научатся выявлять и анализировать угрозы несанкционированного доступа к конфиденциальным данным, разрабатывать и внедрять комплексные меры защиты, включая технические, организационные и правовые средства, а также обеспечивать соблюдение требований законодательства и нормативных актов в области информационной безопасности.

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

ЛАБОРАТОРНЫХ РАБОТ

Раздел 1. Понятие, организация и правовая основа обеспечения информационной безопасности

Тема 1.1. История и современные направления развития информационной безопасности

План.

1. История развития средств и методов защиты информации.
2. Основные этапы решения проблем защиты информации.
3. Защита от информационного воздействия.
4. Информационная война.
5. Понятие информационной безопасности.

Мы живем в мире информации. Владение информацией во все времена давало преимущества той противоборствующей стороне, которая располагала более точными и обширными сведениями о своих соперниках. Государственные и коммерческие секреты появились еще на заре человеческого общества вместе с государствами и торговлей между ними.

Параллельно появилась и развивалась разведывательная деятельность, направленная на добывание этих сведений. Вся история развития государств свидетельствует о широком использовании разведки для добывания информации об их экономике, вооружении, боеготовности армии и др.

В эпоху Возрождения великий итальянский мыслитель XVI века Никколо Макиавелли, считавший допустимым в политической борьбе во имя великих целей пренебрегать законами морали и применять любые средства, оправдывая жестокость и вероломство правителей в их борьбе за власть, указывал: «Чтобы разгадать тайны неприятеля, некоторые полководцы наряжали к нему послов, направляя с ними под видом служителей опытных

воинов, которые высматривали устройство неприятельского войска, узнавали в чем его слабость и сила, и со-
общениями своими облегчали победу»[1].

Впервые же тема разведки на уровне настоящей теории была подробно разработана еще в IV веке до нашей эры китайским стратегом и мыслителем Сунь-Цзы, который говорил: «Негуманно не иметь шпионов,
ибо один шпион сбережет целую армию»[2].

В своей книге «Трактат о военном искусстве» Сунь-Цзы разрабатывает вопросы разведки и контрразведки, ведения психологической войны, использования ложных слухов и фальсификаций, обеспечения безопасности, которые актуальны и в настоящее время. В частности, в ней указывается:

«Великие полководцы достигают успеха, раскрывая тайную игру противника, разрушая его планы, поселяя разлад в его войске... Искусство генерала должно заключаться в том, чтобы держать противника в полном неведении относительно места сражения и чтобы скрыть от него обеспечиваемые пункты, мельчайшие мероприятия... Если ты и можешь что-нибудь, делай вид, что не можешь. Другими словами, сохраняй в тайне все свои военные приготовления, состояние вооружения и т.п.»[3].

Вполне очевидно, что и в настоящее время эти слова не потеряли своей актуальности и их вполне обоснованно можно отнести не только к военному противоборству, но и к разведывательной, экономической, политической деятельности. Они также применимы и к деятельности правоохранительных органов, связанной с проведением боевых операций и осуществлением оперативно-розыскной деятельности.

Наряду с военными секретами противоборствующие стороны всегда охотились и за технологическими секретами, особенно касающимися

---

[1] Лобов В.Н. Военная хитрость в истории войн. - М., 1986. С. 13.

[2] Конрад Н.И. Сунь-Цзы. Трактат о военном искусстве. - М., 1950. С. 55.

[3] Цитируется по: Лобов В.Н. Военная хитрость в истории войн. - М., 1986. С. 7-8.

производства оружия. В частности, в VII веке греки начали применять для поджигания судов и крепостей врага «греческий огонь». Противники Греции, особенно персы, длительное время безуспешно охотились за секретом этого оружия. Затем в XIII веке в Европе появился порох, положивший своеобразное начало научно-технической революции в области вооружения. *История промышленного шпионажа восходит к древнейшим временам. В противовес ему владельцы производственных и коммерческих секретов всегда тщательно охраняли их от конкурентов*. Например, охота европейцев за секретом китайского фарфора, открытого еще в IV веке, продолжалась длительное время и не принесла положительных результатов, пока в начале XVIII века не был изобретен способ производства фарфора в самой Европе. Еще более древним предметом охоты промышленных шпионов был шелк.

В средние века в Европе получил широкое развитие промышленный шпионаж, направленный на добывание секретов цеховых объединений ремесленников, которые монополизировали производство и сбыт определенных видов продукции. Учитывая важность сохранения технологических секретов для обеспечения экономического превосходства над другими странами, многие государства принимали специальные законодательные акты, ограждающие интересы цеховых организаций.

Желание добывать конфиденциальную информацию всегда сопровождалось не меньшим желанием противоположной стороны защитить эту информацию. Поэтому история развития средств и методов разведки – это также история развития средств и методов защиты информации. Причем, появившиеся в древние времена способы защиты информации по сути своей не изменились до настоящего времени, совершенствовалась лишь техника их реализации. Например, такой способ, как маскировка содержания информации, прошел в своем развитии несколько этапов.

Наиболее интенсивное развитие этих методов приходится на период массовой информатизации общества. Поэтому история наиболее интенсивного развития проблемы защиты информации связывается с

внедрением автоматизированных систем обработки информации и измеряется периодом более чем в три десятка лет.

В 60-х годах на Западе стало появляться большое количество открытых публикаций по различным аспектам защиты информации. Такое внимание к этой проблеме вызвано в первую очередь все возрастающими финансовыми потерями фирм и государственных организаций от преступлений в компьютерной сфере. Например, в ежегодном докладе ФБР было сказано, что за 1997 год от противоправной деятельности иностранных спецслужб американские владельцы интеллектуальной собственности понесли ущерб, превышающий 300 миллиардов долларов.

В нашей стране также давно и небезуспешно занимаются проблемами защиты информации – не случайно советская криптографическая школа до сих пор считается лучшей в мире. Однако чрезмерная закрытость всех работ по защите информации, сконцентрированных главным образом в силовых ведомствах, в силу отсутствия регулярной системы подготовки профессионалов в этой области и возможности широкого обмена опытом привела к некоторому отставанию в отдельных направлениях информационной безопасности, особенно в обеспечении компьютерной безопасности.

Тем не менее, к концу 80-х годов бурный рост интереса к проблемам защиты информации не обошел и нашу страну. В настоящее время есть все основания утверждать, что в России сложилась отечественная школа защиты информации. Ее отличительной чертой является то, что в ней наряду с решением сугубо прикладных проблем защиты информации уделяется большое внимание формированию развитого научно-методологического базиса, создающего объективные предпосылки для решения всей совокупности соответствующих задач на регулярной основе.

Естественно, что с течением времени изменялось как представление о сущности проблемы защиты информации, так и методологические подходы к ее решению. Эти изменения происходили постепенно и непрерывно, поэтому

всякие попытки расчленить этот процесс на отдельные периоды и этапы будут носить искусственный характер. Тем не менее, весь период активных работ по рассматриваемой проблеме, в зависимости от методологических подходов к ее решению, довольно четко делится на три этапа.

Начальный этап решения проблем защиты информации (шестидесятые годы и начало семидесятых годов) характеризовался тем, что под этой деятельностью подразумевалось предупреждение несанкционированного получения защищаемой информации. Для этого использовались формальные (т.е. функционирующие без участия человека) средства. Наиболее распространенными в автоматизированных системах обработки данных (АСОД) были проверки по паролю прав на доступ к электронно-вычислительной технике (ЭВТ) и разграничение доступа к массивам данных. Эти механизмы обеспечивали определенный уровень защиты, однако проблему в целом не решали, поскольку для опытных злоумышленников не составляло большого труда найти пути их преодоления. Для объектов обработки конфиденциальной информации задачи ее защиты решались в основном с помощью установления так называемого режима секретности, определяющего строгий пропускной режим и жесткие правила ведения секретного делопроизводства.

Этап развития (семидесятые, начало восьмидесятых годов) выделяется интенсивными поисками, разработкой и реализацией способов
и средств защиты и определяется следующими особенностями:

1. Постепенное осознание необходимости комплексной защиты информации - первым итогом этой работы стало совместное решение задач обеспечения целостности информации и предупреждения несанкционированного доступа к ней.
2. Расширение арсенала используемых средств защиты – повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов, стала широко практиковаться криптографическая защита информации.

3. Целенаправленное объединение всех применяемых средств защиты информации в функциональные самостоятельные системы.

Однако механическое нарастание количества средств защиты и принимаемых мер в конечном итоге привело к проблеме оценки эффективности системы защиты информации, учитывающей соотношение затраченных на создание этой системы средств к вероятным потерям от возможной утечки защищаемой информации. Для проведения такой оценки необходимо применять основные положения теории оценки сложных систем. Другими словами, успешное решение проблемы комплексной защиты информации требует не только научно обоснованных концепций комплексной защиты, но и хорошего инструментария в виде методов и средств решения соответствующих задач. Разработка же такого инструментария, в свою очередь, может осуществляться только на основе достаточно развитых научно-методологических основ защиты информации. Поэтому первой характерной чертой третьего, *современного этапа* комплексной защиты информации (с середины восьмидесятых годов по настоящее время) являются попытки аналитико-синтетической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты, а также формирование на этой основе научно-методологического базиса защиты информации. Основной задачей третьего этапа является перевод процесса защиты информации на строго научную основу.

К настоящему времени уже разработаны основы целостной теории защиты информации. Формирование этих основ может быть принято за начало третьего этапа в развитии защиты информации. Принципиально важным является тот факт, что российские специалисты и ученые, по объективным причинам отстав в разработке некоторых специализированных методов и средств защиты (особенно в области компьютерной безопасности), на

данном этапе внесли существенный вклад в развитие основ теории защиты информации.

Анализ рассмотренных этапов развития проблемы защиты информации показывает, что господствовавшее до недавнего времени представление о защите информации как о предупреждении несанкционированного ее получения является чрезмерно узким. Более того, само понятие «тайна» до недавнего времени ассоциировалось преимущественно с государственными секретами, а то время как в современных условиях повсеместное распространение получают понятия

промышленная, коммерческая, банковская, личная и другие виды тайны.

Таким образом, даже в рамках традиционного представления о защите информации ее содержание должно быть существенно расширено. Исходя из этого, в последнее время проблема защиты информации рассматривается как проблема *информационной безопасности*, заключающейся в комплексном ее решении по двум основным направлениям.

К первому направлению можно отнести традиционно сложившееся в нашем понимании понятие «защита государственной тайны и конфиденциальных сведений», обеспечивающая, главным образом, невозможность несанкционированного доступа к этим сведениям. При этом под конфиденциальными сведениями понимаются конфиденциальные сведения общественного характера (коммерческая, банковская, профессиональная, партийная тайна и т.д.), а также личная конфиденциальная информация (персональные данные, интеллектуальная собственность и т.д.).

Однако в последнее время проблема информационной безопасности рассматривается шире. Оказалось, что современные технические, технологические и организационные системы, а также люди, коллективы людей и общество в целом сильно подвержены внешним информационным воздействиям, причем последствия негативного воздействия могут носить очень тяжелый характер.

Таким образом, информационная безопасность определяется способностью государства, общества, личности:

- обеспечивать с определенной вероятностью защищенность информационных ресурсов и информационных потоков, необходимых для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;
- противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;
- вырабатывать личностные и групповые навыки и умения безопасного поведения;
- поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Исходя из перечисленных задач информационную безопасность можно определить как состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз.

В сложившихся условиях важным является рассмотрение информационной безопасности как неотъемлемой составной части национальной безопасности Российской Федерации. Очевидно, обеспечение информационной безопасности самым теснейшим образом связано не только с решением научно-технических задач, но и с вопросами правового регулирования отношений информатизации, развитием законодательной базы защиты информации.

Тема 1.2. Система организационно-правового обеспечения информационной безопасности

План

1. Система защиты информации.
2. Структура государственной системы защиты информации.
3. Основные субъекты государственной системы защиты информации.
4. Государственная система организационно-правового обеспечения информационной безопасности.

Система защиты информации – это совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных физическими полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и проектов.

Система защиты информации состоит из двух частей - структурной и функциональной. Структурная часть включает в себя совокупность элементов, взаимные связи которых составляют внутреннюю организацию, архитектуру системы защиты информации. Элементы этой системы также имеют и внешние связи, которые целенаправленно воздействуют на внешнюю среду и решают поставленные перед системой задачи. Эти внешние связи и составляют функциональную часть системы. Вполне очевидно, что указанные две части неотделимы друг от друга, они представляют собой внутреннюю (организационную) и внешнюю (исполнительную) стороны системы защиты информации.

Структурная часть системы защиты информации составляет ее внутреннюю организацию, которая позволяет системе эффективно функционировать, создает условия для обеспечения безопасности засекреченной информации, ее обращения только по каналам, образуемым данной системой. Она включает в себя:

1. Систему законов и других государственных правовых актов, устанавливающих:

- порядок и правила защиты информации, а также ответственность за покушение на защищаемую информацию или установленный порядок ее защиты;
- защиту прав граждан, связанных по службе со сведениями, составляющими государственную или иную тайну;
- права и обязанности государственных органов, предприятий и должностных лиц в области защиты информации.

2. Систему засекречивания информации, включающую в себя:
- законодательное или иное определение категорий сведений, которые могут быть отнесены к государственной тайне;
- законодательное определение категорий сведений, которые не могут быть отнесены к государственной тайне;
- наделение полномочиями по отнесению сведений к государственной тайне соответствующих органов государственной власти и их должностных лиц;
- составление перечней сведений, отнесенных к государственной тайне.

3. Систему режимных служб, обеспечивающих функционирование всей системы защиты информации.

Функциональная часть системы защиты информации более адаптивна, подвижна и пластична. Она стремится максимально учесть потребности внешней среды при обращении защищаемой информации, обеспечении ею потребителей, а также направлена на перекрытие каналов утечки информации, исключение ее разглашения или раскрытия.

Основными элементами функциональной части системы защиты информации являются:
- порядок и правила определения степени секретности сведений, указания грифа секретности на носителях информации, а также рассекречивания информации или снижения степени ее секретности;

- поддерживаемые на объекте режим секретности, внутриобъектовый режим и режим охраны, соответствующие степени секретности накапливаемой и используемой на объекте информации;
- система обработки, хранения, учета, выдачи, отправления и получения носителей защищаемой информации, правила секретного делопроизводства;
- разрешительная система, регламентирующая порядок доступа потребителей к носителям защищаемой информации, на режимные объекты и в их отдельные помещения;
- система выявления возможных каналов утечки защищаемой информации и меры по их перекрытию;
- система контроля наличия на объекте носителей защищаемой информации и выявления попыток их выноса за пределы объекта.

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс становится сегодня одной из главных основ экономической и военной мощи любого государства. Информация, проникая во все сферы деятельности государства, приобретает конкретные политическое, материальное и стоимостное выражения, определяемые рядом факторов, в том числе и размерами наносимого ущерба, вызванного снижением ее качества.

Одним из показателей качества информации является ее безопасность. Проблема безопасности информации с точки зрения государственных интересов в последние годы приобрела остроактуальный характер и рассматривается как одна из приоритетных государственных задач, как важный элемент национальной безопасности.

Обозначенная проблема настолько сложна, многоаспектна и специфична, что решать ее можно только в динамическом развитии – от традиционной защиты информации в системах ее обработки, передачи и хранения до обеспечения комплексной безопасности объектов защиты. Такими объектами

могут быть не только специальные военные и оборонные объекты, подразделения правоохранительных органов, предприятия и организации, но и целые отрасли экономики, регионы и другие государственные образования. Как неотъемлемый элемент государственности защита информации существует в любом государстве и в своем развитии проходит множество этапов, определяющих ее качественный рост в зависимости от потребностей государства в защите информации, возможностей, методов и средств ее добывания, правового режима государства и реальных его усилий по обеспечению защиты информации. При этом под государственной системой защиты информации понимается система правовых, организационных, технических и иных мер, федеральных органов власти, местного самоуправления, предприятий, организаций и учреждений, направленных на обеспечение безопасности Российской Федерации, сохранения ее государственной, служебной, коммерческой, других видов тайн и сведений ограниченного доступа, информационных ресурсов, систем, технологий и средств их обеспечения.

Защита информации рассматривается как деятельность, направленная на предотвращение утечки информации с ограниченным доступом, а также по предотвращению различного рода несанкционированных и нежелательных непреднамеренных воздействий на информацию и ее носители. Острая актуальность проблемы обеспечения защиты информации обусловлена рядом объективных факторов, играющих существенную роль в жизни современного общества. Среди этих факторов следует особо выделить:

- неуклонное повышение роли информации в обеспечении жизнедеятельности общества и государства;
- все усиливающаяся интенсификация процессов информатизации различных сфер деятельности;
- устойчивая
- тенденция органического слияния традиционных (бумажных) и автоматизированных (безбумажных) технологий обработки информации;

- резкая децентрализация использования современных средств электронно-вычислительной техники и др.

При общем положительном влиянии, объективной целесообразности и неизбежности перечисленных обстоятельств, они порождают и ряд негативных явлений, одно из которых заключается в резком повышении уязвимости накапливаемой, хранимой и обрабатываемой информации. При этом указанные явления могут носить как случайный, так и преднамеренный характер.

Всем сказанным определяется настоятельная необходимость развития государственной системы защиты информации, совершенствования ее нормативной базы и создания эффективных методик обеспечения информационной безопасности. Рассмотрим структуру существующей государственной системы защиты информации и основные функции составляющих ее органов.

Основным органом, координирующим действия государственных структур по вопросам защиты информации, является *Межведомственная комиссия по защите государственной тайны*, созданная Указом Президента РФ № 71 от 20 января 1996 года. Межведомственная комиссия

– коллегиальный орган, основной функцией которого является координация деятельности федеральных органов государственной власти субъектов Российской Федерации по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне.

Она действует в рамках Государственной системы защиты информации от утечки по техническим каналам, положение о которой введено в действие постановлением Правительства РФ от 15 сентября 1993 года № 912-51. В этом постановлении определены структура, задачи и функции, а также организация работ по защите информации применительно к сведениям,

составляющим государственную тайну. Основной задачей Государственной системы защиты информации от утечки по техническим каналам является проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности страны.

Межведомственная комиссия при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту и в Правительство РФ предложения:

- по организации разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне;
- по правовому регулированию вопросов защиты государственной тайны, совершенствованию системы защиты государственной тайны,
- по порядку определения размеров ущерба, который может быть нанесен безопасности России вследствие несанкционированного распространения секретных сведений или засекречивания информации, находящейся в собственности предприятий;
- по правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности.

Государственная система защиты информации в нашей стране на официальном уровне была оформлена в декабре 1973 г. Возглавила эту систему Государственная комиссия СССР по противодействию иностранным техническим разведкам, в состав которой входили руководители всех оборонных отраслей промышленности. Создание в стране такого органа и возглавляемой им государственной системы защиты информации было вынужденной ответной мерой на действия США и их союзников по созданию глобальной системы разведки, бурное развитие и широкое использование ими технических разведывательных средств. Объектами защиты являлись вооружение и военная техника, военные и военно-

промышленные объекты, системы боевого управления войсками и оружием, оборонные работы.

В восьмидесятых годах во внешней и внутренней политике России произошли кардинальные изменения, следствием которых явились радикальные экономические преобразования, конверсия оборонной промышленности, введение режимов «открытости», развертывание совместных с инофирмами предприятий и производств, развитие информационных процессов. Эти изменения создали дополнительные условия и предпосылки для ведения разведки иностранными государствами, к действиям по широкому сбору различной «чувствительной» информации во всех областях деятельности государства

– оборонной, экономической, научно-технической, политической, правоохранительной и т.д. Особую тревогу вызывала утечка сведений, составляющих государственную и служебную тайну. Стало очевидным, что система защиты информации, сложившаяся в СССР в рамках только оборонной тематики, перестала соответствовать потребностям и задачам нашего государства в новых правовых условиях.

Указом Президента Российской Федерации от 5 января 1992 года в целях общей координации работ по защите информации, обрабатываемой техническими средствами, на базе Гостехкомиссии СССР была образована Государственная техническая комиссия при Президенте Российской Федерации – *Гостехкомиссия России* (в настоящее время преобразована в Федеральную службу по техническому и экспортному контролю - ФСТЭК), а государственная система защиты информации получила свое второе рождение, сферы ее интересов существенно расширились. Следует отметить, что проверенные многими годами практической работы основные принципы и формы организации защиты информации были сохранены – сохранилась коллегиальность в принятии решений по важнейшим направлениями защиты информации, при утверждении нормативных и методических документов, с одной стороны, и полная самостоятельность и персональная ответственность

руководителей всех уровней за исполнение принятых решений и эффективность информации –

с другой.

В состав ФСТЭК входят руководители федеральных органов государственного управления, определяющих научно-техническую и финансовую политику по защите информации в политической, экономической, военной областях, или первые их заместители. ФСТЭК в пределах своей компетенции осуществляет следующие функции:

- формирует общую стратегию и определяет приоритетные направления защиты информации в жизненно важных сферах деятельности государства с целью предотвращения ущерба интересам страны;
- определяет основные направления исследований, рассматривает и утверждает концепции, требования, нормы и другие нормативно-технические и методические документы;
- рассматривает и представляет на утверждение правительству проекты государственных программ по защите информации;
- заслушивает руководителей министерств и ведомств, государственных предприятий и объединений, главных конструкторов по вопросам, связанным с защитой информации.

Федеральная служба безопасности России осуществляет контроль за обеспечением в органах государственного управления и на предприятиях, ведущих работы по оборонной и другой секретной тематике, организационно-режимных мероприятий.

Росстандарт выступает в качестве национального органа по стандартизации и сертификации продукции.

Другие органы государственного управления (министерства,

ведомства) в пределах своей компетенции:

- определяют перечень охраняемых сведений;

- обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;
- организуют и координируют проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в области защиты информации в соответствии с государственными (отраслевыми) программами;
- разрабатывают по согласованию с ФСТЭК отраслевые документы по защите информации;
- контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;
- создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;
- организуют подготовку и повышение квалификации специалистов по защите информации.

Для осуществления указанных функций в составе органов государственного управления функционируют научно-технические подразделения (центры) защиты информации и контроля.

На предприятиях, выполняющих оборонные и иные секретные работы, функционируют научно-технические подразделения защиты информации и контроля, координирующие деятельность в этом направлении научных и производственных структурных подразделений предприятия, участвующие в разработке и реализации мер по защите информации, осуществляющие контроль эффективности этих мер.

Кроме того, в отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за деятельностью в области оказания услуг по защите информации, органы сертификации СВТ и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы аттестации объектов информатики.

Государственная система защиты информации подразумевает необходимость разделения прав и обязанностей между субъектами обеспечения защищенности информации: государством, предприятиями, их объединениями, учреждениями и организациями, а также отдельными должностными лицами.

Государство, как основной субъект обеспечения защиты информации, через свои органы законодательной, исполнительной и судебной властей с целью создания условий для осуществления защиты и координации действий по защите информации организует:

- создание системы правовых норм, регулирующих отношения в области защиты информации;
- проведение единой технической политики в этой области, разработку государственных программ по защите информации, требований, норм и рекомендаций;
- создание технических систем и средств защиты и контроля;
- согласование проводимых работ по защите информации, общее и методическое руководство ими;
- общий контроль за состоянием защиты информации в стране, отдельных регионах и на важнейших объектах защиты.

Предприятия и их объединения, учреждения и организации, независимо от их организационно-правовой формы и формы собственности, а также отдельные должностные лица, выполняющие работы, связанные с использованием сведений, отнесенных к государственной и служебной тайнам, должны обеспечить их защиту.

В соответствии с изложенными задачами государственной системы защиты информации в ее организационной структуре можно выделить пять основных категорий органов защиты информации, реализующих следующие функции:

1. *Административные* – формируют общую стратегию информационной безопасности, осуществляют общую организацию и

координацию работ, решают вопросы финансирования работ, организуют промышленное производство средств защиты. В общегосударственном масштабе рассмотренные функции реализуют такие органы, как Совет безопасности РФ, Межведомственная комиссия по вопросам защиты государственной тайны, ФСТЭК РФ. На региональном уровне могут создаваться аналогичные органы при руководящих органах управления субъектов РФ. Практически во всех ведомствах, особенно в силовых (ФСБ, МВД, ФСО РФ и др.) существуют постоянно действующие комиссии по вопросам информационной безопасности.

2. *Научно-исследовательские* – организуют осуществление научно-исследовательских и опытно-конструкторских работ, координируют проведение исследований и разработок в области защиты информации. К таким органам на государственном уровне относятся всероссийские научно-исследовательские институты и центры, работающие под непосредственным руководством ФСТЭК России. Многие силовые ведомства имеют свои научно-исследовательские органы, например, в МВД – Научно-исследовательский институт специальной техники.

3. *Учебно-методические* – осуществляют подготовку и повышение квалификации специалистов в области обеспечения информационной безопасности, проводят исследования в этой области, разрабатывают учебную и учебно-методическую базу преподавания дисциплин по защите информации. На государственном уровне эти функции выполняют учебно-методические объединения, разрабатывающие единую политику в области подготовки специалистов, руководящие нормативные документы (образовательные стандарты, программы и т.д.), координирующие данную деятельность в России. Кроме того, существует множество вузов общероссийского масштаба, а также ведомственных и региональных учебных заведений, готовящих специалистов по информационной безопасности.

4. *Специализированные центры защиты информации* – проводят научно-исследовательские и опытно-конструкторские работы в области информационной безопасности, оказывают широкий спектр услуг предприятиям, учреждениям и фирмам в этой области. Такие центры, как на государственном, так и на региональном уровне могут проводить аттестацию объектов, обрабатывающих сведения, содержащие государственную тайну, или персональные данных; производить специальные проверки помещений, специальное исследование технических средств; разрабатывать и устанавливать на объектах системы защиты информации и другие работы. Причем, центры могут создаваться как на государственной, так и на коммерческой основе. Например, наиболее крупными негосударственными центрами защиты информации в России являются фирмы «NOVO», «Нелк», «Конфидент» и др.

5. *Службы защиты информации* – осуществляют решение всего комплекса вопросов, связанных с непосредственной защитой информации. Такие службы в обязательном порядке создаются на объектах, обрабатывающих сведения, составляющие государственную тайну, на предприятиях оборонной промышленности. Свои службы защиты информации могут создавать и банки, крупные государственные предприятия и коммерческие фирмы.

Существующий состав органов защиты информации охватывает все уровни государственного управления и все сферы деятельности государства, связанные с использованием секретной и служебной информации, и обеспечивает проведение мероприятий по защите информации постоянно на всей территории страны. Основными формами организации работ по защите информации являются:

- осуществление государственного заказа на проведение соответствующих работ;

- лицензирование деятельности предприятий и организаций по вопросам защиты информации и допуска предприятий к работе со сведениями, составляющими государственную тайну;
- сертификация систем и средств получения, обработки, хранения и передачи информации в части защищенности информации от утечки по техническим каналам, а также средств защиты и контроля;
- аттестация объектов по выполнению требований безопасности информации;
- проведение контрольных мероприятий по оценке эффективности защиты информации.

Органы государственной системы защиты информации в своей деятельности руководствуются решениями высших органов федеральной власти по вопросам:

- назначения особого режима закрытия административно-территориальных образований;
- регламентируемого посещения иностранными представителями отдельных объектов и территорий;
- выбора приоритетных направлений защиты информации в жизненно-важных сферах деятельности государства;
- осуществления единой технической политики, правового регулирования защиты информации и экспертизы наиболее важных сведений.

Основными государственными органами, осуществляющими организацию защиты информации в различных сферах деятельности, являются ФСБ, ФСО, МВД, Минобороны, Минатом России и входящие в них структурные подразделения защиты информации. Эти органы в пределах своей компетенции имеют определенные цели и объекты защиты и располагают специфическими способами защиты. Их права и функции в области защиты информации определяются соответствующими законами и положениями об этих органах.

Подразделения по защите информации являются самостоятельными структурными подразделениями или входят в состав одного из основных научно-технических или специальных управлений органа государственной власти. Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия и организации, имеющие лицензии на проведение работ в области защиты информации.

Значительная роль в государственной системе защиты информации отводится научно-исследовательским, научно-техническим, проектным и конструкторским организациям, которые призваны внести свой вклад не только в разработку всей совокупности нормативных и методических документов по защите информации, но и реально на практике реализовать разработку и внедрение методов, способов и средств защиты информации.

С принятием в последнее время Правительством Российской Федерации ряда нормативных документов по проблеме защиты государственной тайны более активно стали развиваться региональные структуры по защите информации в субъектах РФ.

Важное место в государственной системе защиты информации принадлежит высшим учебным заведениям и институтам повышения квалификации по подготовке и переподготовке кадров в области защиты информации, которые осуществляют:

- первичную подготовку специалистов по комплексной защите информации;
- переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;
- усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

Таким образом, в настоящее время в основном завершен организационный период создания государственной системы защиты информации. За время становления накоплен обширный опыт ее функционирования в переходный

период, характеризовавшийся формированием новой законодательно-правовой базы в области защиты информации, уточнением полномочий и функций элементов этой системы.

Следующий этап развития государственной системы защиты информации заключается в разработке и практическом освоении специалистами методического обеспечения, адекватного целям и задачам этой системы. Необходимо проведение научных исследований по вопросам комплексной оценки потенциальных угроз безопасности информации и эффективности системы ее защиты, а также лицензирования деятельности в области защиты, сертификации средств защиты, определения ущерба от несанкционированного распространения информации, регламентации правовой и материальной ответственности должностных лиц и специалистов за утечку информации по техническим каналам связи, ее разрушение, искажение и утрату.

Организационно-правовое обеспечение информационной безопасности представляет собою совокупность решений, законов, нормативных актов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и функционирование систем защиты информации на конкретных объектах. Поэтому организационно-правовая база защиты информации должна обеспечивать выполнение следующих основных функций:

1) разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;

2) определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области;

3) создание полного комплекса нормативно-правовых руководящих и методических документов, регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте;

4) определение мер ответственности за нарушения правил защиты;

5) определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Разработка законодательной базы информационной безопасности является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений развития государства. Особое внимание к формированию такой базы вызвано неуклонным ростом затрат на борьбу с «информационными» преступлениями.

Основой для создания государственной системы организационно-правового обеспечения информационной безопасности является рассмотренная выше государственная система защиты информации, под которой понимается совокупность федеральных и иных органов управления и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и направленных на обеспечение безопасности информационных ресурсов.

Государственная система организационно-правового обеспечения информационной безопасности создается для решения следующих проблем, требующих законодательной поддержки:

- защита государственных секретов;
- защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;
- создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;
- борьба с компьютерной преступностью, в первую очередь в финансовой сфере;
- защита персональных данных;
- страхование информации и информационных систем;
- сертификация и лицензирование в области защиты информации,

контроль безопасности информационных систем;

- организация взаимодействия в сфере защиты информации со странами СНГ и другими государствами.

Анализ современного состояния информационной безопасности в России показывает, что уровень ее в настоящее время не соответствует жизненно важным потребностям личности, общества и государства. К негативным факторам, осложняющим обеспечение информационной безопасности, относятся:

- обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение;
- несовершенство нормативно-правовой базы, отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве;
- слабое обеспечение органов государственной власти и управления полной и достоверной информацией, неразвитость информационных отношений в сфере предпринимательства;
- недостаточная защищенность государственного информационного ресурса и слабость мер по обеспечению сохранности государственных секретов в органах государственной власти и управления;
- необеспеченность прав граждан на информацию, манипулирование информацией, вызывающее неадекватную реакцию населения и ведущее к политической нестабильности в обществе.

Такое положение в области обеспечения информационной безопасности требует безотлагательного решения ряда ключевых организационно-правовых проблем:

1. Развитие концепции информационной безопасности, являющейся основой государственной политики в этой области.
2. Формирование законодательной и нормативно-правовой базы обеспечения информационной безопасности.

3. Разработка механизмов реализации прав граждан на информацию.

4. Формирование системы информационной безопасности, обеспечивающей реализацию государственной политики в этой области.

5. Совершенствование методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработка критериев и методов оценки эффективности систем и средств информационной безопасности.

7. Исследование форм и способов цивилизованного воздействия государства на формирование общественного сознания.

8. Комплексное исследование деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Лабораторная работа: Система организационно-правового обеспечения информационной безопасности

При поведении занятия необходимо рассмотреть следующие вопросы:

Система защиты информации. Структура государственной системы защиты информации. Основные субъекты государственной системы защиты информации. Государственная система организационно-правового обеспечения информационной безопасности.

Рекомендуемая литература:

1. Гончаренко, Л. П. Управление безопасностью: учеб. пособие / Л.П. Гончаренко, Е.С. Куценко. - М.: КноРус, 2005 - 272 с.

2. Старостенко, К.В. Национальная безопасность: учебно-метод. пособие / К.В. Старостин - Орел: ОРАГС, 2003 - 124 с.

3. Малюк А.А. Информационная безопасность: концептуальные и метологические основы защиты информации: учеб. пособие для вузов / А.А. Малюк - М.:Горячая линия-Телеком, 2004 - 280 с.

4. Гринберг, А.С. Защита информационных ресурсов государственного управления: учеб. пособие / А.С. гринберг, Н.Н. Горбачев, А.А. Тепляков - М.:ЮНИТИ. 2003. - 327 с.

Тема 1.3 Правовая основа информационной безопасности

План

1. Требования к законодательству в области информационной безопасности
2. Правовая основа обеспечения информационной безопасности в России.
3. Конституция и законодательные акты РФ о защите информации.
4. Регламентирование вопросов защиты информации в ведомственных нормативных актах.
5. Ответственность за нарушение требований защиты информации.

Анализ зарубежного опыта формирования законодательной базы в области информационной безопасности показывает, что разработка проблемы правового обеспечения защиты информации идет по трем направлениям:

1. Защита прав личности на частную жизнь.

Этот аспект не является новым для мирового сообщества. Основные принципы установления пределов вмешательства в частную жизнь со стороны государства и других субъектов определены основополагающими нормами: Декларацией прав человека, Конвенцией ООН и Конвенцией Совета Европы по правам человека.

Развитие информатики в странах Запада и связанный с этим рост угрозы нарушения прав личности (бесконтрольное распространение и доступ к

персональной информации) потребовали разработки специальных актов, учитывающих фактор информационной безопасности.

К концу 70-х годов были сформулированы три основных принципа обеспечения информационной безопасности, нашедшие впоследствии отражение в национальном законодательстве по информатике:

- установление пределов вмешательства в частную жизнь с использованием компьютерных систем;
- введение административных механизмов защиты граждан от такого вмешательства;
- защита интеллектуальной собственности личности.

К этому направлению можно отнести резолюцию Европарламента «О защите прав личности в связи с прогрессом информатики» (1979 г.) и конвенцию ЕС «О защите лиц при автоматизированной обработке данных персонального характера» (1980 г.).

2. Защита государственных интересов.

Проблема решается с помощью достаточно разработанных национальных законодательств, определяющих национальные приоритеты в этой области. Интеграция стран - членов ЕС потребовала координации усилий в данной области, в результате чего общие принципы засекречивания информации были отражены в Конвенции ЕС «По защите секретности». Механизм защиты предусматривает следующие аспекты:

- установление приоритетов защиты;
- определение исполнительских механизмов и нормативное обеспечение механизмов защиты.

3. Защита предпринимательской и финансовой деятельности.

Это направление деятельности осуществляется путем создания законодательного механизма, обеспечивающего защиту коммерческой тайны и создающего условия для осуществления «добросовестной» конкуренции.

При создании в нашей стране правовой основы информационной безопасности необходимо учитывать:

- состояние и состав международных норм в области информатизации;
- состояние отечественного законодательства в этой и смежных областях;
- формирование системы законодательства с охватом всех ее уровней, обеспечением преемственности и совместимости норм в законах разного уровня – конституционных, общих, специальных;
- последовательный выход на развитие ведомственных и местных нормативных актов с опорой на законодательную основу;
- создание механизмов, обеспечивающих организацию, применение, действенность законодательной базы информатизации.

Направления создания правовой базы в области информационной безопасности должны затрагивать все уровни законодательства России:

- конституционное законодательство;
- основные общие законы;
- законы по организации государственной системы управления;
- специальные законы.

Например, конституционно должны быть закреплены и оформлены права граждан, организаций, государства на информацию и последовательно обеспечены во всех основных законах – о собственности, правах граждан, гражданстве, предпринимательстве и т.д.

Вопросы информационного обеспечения обязательно должны присутствовать в законах о разделении компетенции и правовом статусе различных государственных систем, органов и организаций государственного устройства по вертикали и горизонтали.

Специальные законы в области информатизации должны быть ориентированы на создание условий в организации и упорядочении самой информации, управление государственными информационными ресурсами, обеспечение процесса включения современных технологий во все

направления информатизации, создание системы защиты информации, установление гарантий и т.д.

Кроме федерального законодательства вопросы информационной безопасности должны быть учтены в законодательстве республик в составе Российской Федерации.

Важное место в правовом обеспечении информатизации должны занимать подзаконные нормативные акты, отражающие процессы защиты информации.

Завершить эту иерархическую структуру системы законодательства должно правоохранительное законодательство, включающее нормы об ответственности за правонарушения при работе с информацией.

На уровне административного государственного регулирования в порядке исполнения указанных законов соответствующими органами государственного управления должны быть разработаны государственные стандарты, устанавливающие нормы защищенности информации, а также требования и правила организационного и технического характера. В них должны учитываться характеристики уязвимости информации, определена совокупность комплексных мер защиты, необходимых для безопасной обработки информации в зависимости от уровня ее ценности или общественной опасности нарушений в работе информационных систем.

Анализ рассмотренной структуры законодательной базы информационной безопасности позволяет сделать вывод о том, что в настоящее время осуществляется переход от принципа «интегральной защиты» информации к принципу «дифференциальной защиты», обеспечивающему равносильную защиту различных видов защищаемых сведений. При этом следует отметить, что задача создания стройной законодательной системы, одновременно удовлетворяющей всем изложенным требованиям комплексной защиты информации, оказывается весьма сложной и на сегодняшний день не имеет адекватных решений.

Базовым актом информационного законодательства Российской Федерации является принятый в 2006 г. Федеральный закон *«Об информации, информационных технологиях и защите информации»*. В нем впервые законодательно закрепляются права и обязанности граждан, организаций и государства в информационной области, устанавливается правовой режим обработки и использования информации, порядок защиты прав субъектов информационных отношений. В этом Законе указаны следующие основные направления государственной политики, связанные с обеспечением национальной безопасности в сфере информатизации:

- обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
- формирование и защита государственных информационных ресурсов;
- обеспечение национальной безопасности в сфере информатизации
- обеспечение реализации прав граждан и организаций в условиях информатизации;
- развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

В указанном законе формулируются следующие цели защиты информации и обеспечения прав субъектов в области информационных процессов и информатизации:

- предотвращение утечки, хищения, утраты, искажения и подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

– обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны и конфиденциальности документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Закон«Об информации, информационных технологиях и защите информации» впервые в законодательной практике России нормативно урегулировал следующие вопросы:

– закрепил права граждан, организаций и государства на информацию;

– установил правовой режим информации на основе применения в этой области института собственности, правил документирования, деления информации на открытую и закрытую (с ограниченным доступом), методов формирования информационных ресурсов и пользования ими;

– установил основные права и обязанности граждан, организаций и государства в процессе создания информационных систем, развития научно-технической базы информатизации, формирования рынка информационной продукции и информационных услуг;

– установил гарантии безопасности субъектов в процессе реализации их права на информацию;

– определил порядок включения страны в международные информационные системы.

В указанном Законе информация признается объектом права собственности граждан, организаций, общественных объединений и государства. В нем подчеркивается, что информационные ресурсы могут быть товаром и в

качестве материальных ценностей включаться в состав имущества организаций. При этом собственник информации имеет право устанавливать режим доступа к информации и правила ее защиты. Режим доступа к информационным ресурсам определяется тем, что информация подразделяется на категории открытого и ограниченного доступа, при этом информация ограниченного доступа в соответствии с условиями ее правового режима может быть секретной или конфиденциальной.

Принятый Государственной Думой 5 июня 1996 года *Федеральный закон «Об участии в международном информационном обмене»* устанавливает порядок обмена между государствами конфиденциальной и массовой информацией. В соответствии с этим Законом органы государственной власти обязаны:

- создавать условия для обеспечения, своевременного и достаточного пополнения государственных информационных ресурсов Российской Федерации иностранными информационными продуктами и услугами;
- содействовать внедрению современных информационных технологий для участия в международном информационном обмене;
- обеспечивать защиту государственных информационных ресурсов и соблюдение правового режима информации;
- стимулировать расширение взаимовыгодного международного информационного обмена документированной информацией;
- создавать условия для защиты от некачественной и недостоверной иностранной информации, недобросовестной конкуренции со стороны физических и юридических лиц иностранных государств в информационной сфере;
- способствовать развитию товарных отношений при международном информационном обмене.

В соответствии со статьей 8 указанного закона введены ограничения на перемещение из Российской Федерации документальной информации,

отнесенной к государственной тайне или иной конфиденциальной информации, общероссийскому национальному достоянию, архивному фонду и иным категориям документированной информации, вывоз которой может быть ограничен российским законодательством.

Защита государственных секретов регламентируется и международными нормативными актами. Например, в январе 1993 года в Минске было подписано Соглашение между странами СНГ о взаимном обеспечении сохранности межгосударственных секретов, где зафиксированы общие принципы обеспечения режима секретности при осуществлении политического, экономического, научно-технического и военного сотрудничества между государствами-участниками соглашения. Правовая основа защиты информации включает в себя и ряд других законов, указов, постановлений и подзаконных актов, которые косвенно регламентируют правовые отношения в сфере обеспечения информационной безопасности. Перечислим и кратко охарактеризуем наиболее важные из них.

Принятый 27 декабря 1991 года *Закон Российской Федерации «О средствах массовой информации»* устанавливает право на свободу информации: в статье 1 указывается, что поиск, получение, производство и распространение массовой информации не подлежат ограничениям за исключением случаев, оговоренных законодательством. В частности, в соответствии со статьей 40 указанного Закона средствам массовой информации может быть отказано в получении запрашиваемой информации в случае, если она содержит сведения, составляющие государственную, коммерческую или иную специально охраняемую тайну.

Статья 41 Закона ограничивает права средств массовой информации на распространение конфиденциальной информации: редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Редакция обязана сохранять в тайне источник информации и не в праве называть лицо, предоставившее сведения с условием неразглашения его имени, за

исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом.

В статье 4 Закона говорится о недопустимости использования средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны. В связи с опасностью использования методик нейролингвистической психологии (НЛП), таких как «эффект 25 кадра», Закон запрещает использование в теле-, видео-, а также кинохроникальных программах скрытых вставок, воздействующих исключительно на подсознание людей.

Федеральные законы *«Об органах федеральной службы безопасности Российской Федерации»* от 10 апреля 1995 г. и «*О внешней разведке»* от 10 января 1996 г. имеют много общего в части, касающейся добывания, обработки и использования разведывательной информации, а также в вопросах защиты государственной тайны.

В статье 20 Закона «Об органах федеральной службы безопасности Российской Федерации» указано, что хранение в информационных системах сведений о физических и юридических лицах не является основанием для принятия мер, ограничивающих права этих лиц. В соответствии со статьей 6 указанного Закона полученные в процессе деятельности органов Федеральной службы безопасности (ФСБ) Российской Федерации сведения о частной жизни, затрагивающие честь и достоинство гражданина или способные повредить его законным интересам, не могут сообщаться органами ФСБ кому бы то ни было без добровольного согласия этого гражданина, за исключением случаев, предусмотренных федеральными законами.

Закон «О внешней разведке» запрещает применение органами внешней разведки методов и средств разведывательной деятельности в отношении граждан России на территории Российской Федерации. Наряду с деятельностью Службы внешней разведки (СВР), этот закон также регламентирует деятельность подразделений и частей радиоразведки ФАПСИ, которые ведут разведывательную деятельность в сфере шифрованной, засекреченной и иных видов специальной связи.

Принятый 27 мая 1996 г. *Федеральный Закон «О государственной охране»* обязывает органы Федеральной службы охраны (ФСО) Российской Федерации осуществлять следующие виды деятельности:

- организовывать и проводить в пределах своих полномочий мероприятия по развитию и совершенствованию системы президентской связи, обеспечению ее надежности, информационной безопасности и оперативности при предоставлении объектам государственной охраны
- производить шифровальные работы;
- организовывать и проводить на охраняемых объектах, а также в местах постоянного и временного пребывания объектов государственной охраны оперативно-технический контроль;
- осуществлять во взаимодействии с федеральными органами правительственной связи и информации меры по противодействию утечке информации по техническим каналам.

Органы внутренних дел в соответствии с *Законом РСФСР «О милиции»*, принятым 18 апреля 1991 г., имеют широкие полномочия по проведению работ в информационной сфере. В частности, милиция обязана «принимать и регистрировать заявления, сообщения и иную поступающую информацию о преступлениях, административных правонарушениях и событиях, угрожающих личной или общественной безопасности» (п.3, ст.10).

В соответствии со ст. 11 милиции предоставлено право «получать от граждан и должностных лиц необходимые объяснения, сведения, справки, документы и копии к ним» (п.4). Кроме того, разрешается «проводить регистрацию,

фотографирование, звукозапись, кино- и видеосъемку, дактилоскопирование лиц, заключенных под стражу, задержанных по подозрению в совершении преступлений или занятии бродяжничеством, обвиняемых в совершении умышленных преступлений, подвергнутых административному аресту, а также лиц, подозреваемых в совершении административного правонарушения при невозможности установления их личности...» (п.15). Информационные центры и экспертно-криминалистические подразделения во взаимодействии с другими подразделениями органов внутренних дел и службами иных правоохранительных органов (в том числе и зарубежных) выполняют функции формирования и ведения общегосударственных справочно-информационных фондов (п.15).

Положение о Министерстве внутренних дел Российской Федерации, утвержденное Указом Президента Российской Федерации от 18 июля 1996 г. № 1039, устанавливает право МВД на формирование, ведение и использование федеральных учетов, банков оперативно-справочной, розыскной, криминалистической, статистической и иной информации, осуществление справочно-информационного обслуживания органов внутренних дел, внутренних войск и иных заинтересованных государственных органов, организацию государственной статистики и статистики в системе Министерства.

Гражданский кодекс Российской Федерации рассматривает информацию в качестве объекта гражданского права наряду с интеллектуальной собственностью и имуществом (ст.128). В нем также дается определение информации, составляющей служебную и коммерческую тайну. В ст. 139 ГК изложена суть особых формальностей, которые позволяют применять какие-либо санкции к нарушителям конфиденциальности информации:

- во-первых, эта конфиденциальная информация должна иметь действительную или потенциальную коммерческую ценность и она не может быть известна третьим лицам;

- во-вторых, учреждение, владеющее конфиденциальной информацией, на законных основаниях принимало определенные меры для исключения свободного доступа к этой информации и охране ее конфиденциальности;
- в-третьих, все сотрудники, знакомые с этими сведениями, были официально предупреждены об их конфиденциальности.

Принятый 24 мая 1996 г. Уголовный кодекс Российской Федерации закрепляет принципиально новые для отечественного законодательства подходы к некоторым проблемам уголовного права. В частности, глава 28 «Преступления в сфере компьютерной информации» определяет, какие общественно-опасные деяния в сфере использования компьютерной информации являются преступными. Так, в соответствии со статьей 272 УК РФ устанавливается уголовная ответственность за «неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), в системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». Статья 273 УК РФ впервые в отечественном законодательстве устанавливает уголовную ответственность за создание, использование и распространение вредоносных программ для ЭВМ или «внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». В соответствии со статьей 274 УК РФ к числу уголовных преступлений теперь относится и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим к ним доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации.

К разряду преступлений против конституционных прав и свобод человека и гражданина, носящих информационный характер, в Уголовном кодексе отнесены следующие деяния:

– нарушение неприкосновенности частной жизни, то есть «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстных или иной личной заинтересованности и причинили вред правам и законным интересам граждан» (статья 137 УК);

– нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 138 УК), отказ в предоставлении гражданину информации, то есть «неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан» (статья 140 УК);

– воспрепятствование законной профессиональной деятельности журналистов путем принуждения их к распространению либо к отказу от распространения информации (статья 144 УК);

– нарушение авторских и смежных прав (статья 146 УК);

– нарушение изобретательских и патентных прав (статья 147 УК).

Среди преступлений против основ конституционного строя и безопасности государства следует выделить такие «информационные» противоправные деяния, как государственная измена (статья 275), шпионаж (статья 276 УК), разглашение государственной тайны (статья 283 УК) и утрата документов, содержащих государственную тайну (статья 284 УК).

Лабораторная работа: Правовая основа информационной безопасности

При поведении занятия необходимо рассмотреть следующие

вопросы:

Требования к законодательству в области информационной безопасности. Правовая основа обеспечения информационной безопасности в России. Конституция и законодательные акты Российской Федерации о защите информации. Регламентирование вопросов защиты информации в ведомственных нормативных актах. Ответственность за нарушение требований защиты информации.

Рекомендуемая литература:

1. Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации: учеб. пособие для вузов / А.А. Фатьянов. М.: Юристъ, 2001. - 412 с.
2. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для вузов / В.П. Мельников, С.А. Клейменова, А.М. Петраков. - М.: Академия, 2007. - 336 с.
3. Снытников, А.А. Обеспечение и защита права на информацию / А.А. Снытников. - М.: Городец-издат, 2001. - 344 с.
4. Партыка, Т.Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум-Инфра- М, 2004 - 368 с.
5. Ярочкин, В.И. Информационная безопасность: учеб. для вузов / В.И. Ярочкин. -М.: Трикса: Акад.проект, 2005.-544 с.
6. Расторгуев С.П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. - М.: Академия, 2007. - 192 с.

Раздел 2. Принципы, методы и средства защиты информации Тема 2.1. Источники угроз защищаемой информации.

План

1. Классификация и содержание возможных угроз информации.
2. Причины и условия утечки защищаемой информации.
3. Способы незаконного получения защищаемой информации.

Вернемся к рассмотренному выше понятию «информационной безопасности», которое определялось как «состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних угроз». Исходя из содержания этого понятия, можно определить, что **угроза защищаемой информации – это возможное воздействие дестабилизирующих факторов на состояние информированности, подвергающее опасности жизненно важные интересы личности, общества и государства**. Под угрозой информации в системах ее обработки понимается возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

В настоящее время известно множество различных *видов угроз* информации, основными из которых являются угрозы, которые могут повлечь нарушения:

- физической целостности (уничтожение, разрушение элементов);
- логической целостности (разрушение логических связей);
- содержания (изменение блоков информации, внешнее навязывание ложной информации);
- конфиденциальности (разрушение защиты, уменьшение степени защищенности информации);
- прав собственности на информацию (несанкционированное копирование, использование).

Для систем обработки информации наиболее опасными являются следующие угрозы:

- подверженность физическому искажению или уничтожению;
- возможность несанкционированной модификации данных;
- опасность несанкционированного получения информации лицами, не имеющими официального допуска к ней.

По характеру происхождения угрозы безопасности информации в современных системах ее обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы) разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными (преднамеренными) угрозами понимаются такие угрозы, которые обусловливаются злоумышленными действиями людей. Случайными (естественными) являются угрозы, не зависящие от людей.

Источниками угроз защищаемой информации являются:

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда.

Существуют следующие основные *причины возникновения угроз информации*:

- количественная недостаточность – физическая нехватка средств обработки информации, вызывающая нарушения технологического процесса обработки;
- качественная недостаточность – несовершенство конструкции (организации) элементов информационной системы, в силу чего может возникнуть возможность случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;
- деятельность разведывательных органов иностранных государств – специально организуемая деятельность государственных органов разведки,

профессионально ориентированных на добывание необходимой информации всеми доступными средствами и методами;

- промышленный шпионаж – негласная деятельность отечественных и зарубежных предприятий (фирм), направленная на получение незаконным путем конфиденциальной информации, используемой для достижения промышленных, коммерческих, политических или подрывных целей;
- злоумышленные действия уголовных элементов – хищение информации, средств ее обработки или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;
- плохое психофизиологическое состояние – постоянное или временное дискомфортное психофизиологическое состояние сотрудников, приводящее при определенных нестандартных внешних воздействиях к увеличению ошибок и сбоев в обслуживании систем обработки информации или непосредственно к разглашению конфиденциальной информации;
- недостаточная качественная подготовка сотрудников – уровень теоретической и практической подготовки персонала к выполнению задач по защите информации, недостаточная степень которого может привести к нарушению процесса функционирования системы защиты информации.

В процессе деятельности предприятия или организации защищаемая информация может по различным причинам выйти из владения субъектов, которые являются ее собственниками, или которым она была доверена или стала известной по службе или работе. При этом защищаемая информация выходит за пределы установленной сферы обращения, охраняемой специальными режимными мерами, и утрачивается контроль за ее распространением – происходит утечка информации.

Утечка защищаемой информации – это несанкционированное разглашение, выход ее за пределы круга лиц, которым эта информация была доверена. Иными словами, утечка защищаемой информации – это неправомерное

завладение соперником этой информацией и получение тем самым возможности ее использования в своих интересах.

Утечку информации в общем плане можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена. Утечка информации по своей сущности предполагает противоправное (тайное или явное, осознанное или случайное) овладение конфиденциальной информацией, независимо от того, каким путем оно достигается.

Наряду с утечкой информации следует выделить и такие близкие к ней понятия, как разглашение, раскрытие и распространение защищаемой информации, несанкционированный доступ к ней.

Разглашение защищаемой информации - это несанкционированное ознакомление с такой информацией лиц, не имеющих законного доступа к ней, осуществленное лицом, которому эти сведения были доверены или стали известны по службе. Разглашение может быть совершено среди своих коллег, не имеющих доступа к данной информации, среди родственников, знакомых и иных лиц.

Раскрытие защищаемой информации - это опубликование ее в средствах массовой информации, использование в выступлениях на публичных конференциях или симпозиумах лицами, которым эти сведения стали известны по службе. Вследствие таких действий защищаемая информация становится достоянием неопределенно широкого круга лиц и утрачивает свою секретность.

Распространение защищаемой информации - это открытое использование сведений ограниченного распространения.

Несанкционированный доступ – получение в обход системы защиты с помощью программных, технических и других средств, а также в силу сложившихся случайных обстоятельств доступа к защищаемой информации.

Одной из наиболее важных проблем защиты информации является защита самих носителей информации, так как защищаемые сведения не могут существовать отдельно от них. Однако не все носители можно спрятать в сейф или за прочные стены, ведь информацией могут располагать люди, она содержится в различного рода излучениях, каналах связи и т.п. Обычно к ним и стремится получить доступ соперник, прокладывая пути к интересующей его информации.

Таким образом, источник утечки защищаемой информации - это любой носитель секретной информации, к которому сумел получить несанкционированный доступ соперник, располагающий необходимыми знаниями и техническими средствами для «снятия», извлечения информации с носителя, ее расшифровки и использования в своих целях в ущерб интересам собственника информации.

Наиболее распространенными причинами утечки информации являются:

- несовершенство нормативных актов, регламентирующих защиту информации;
- недостаточность наличных сил и средств для перекрытия каналов утечки информации;
- нарушение лицами, допущенными к работе с защищаемой информацией, установленных правил ее защиты.

Указанные причины приводят к утечке информации в том случае, если этому способствуют соответствующие субъективные или объективные условия. К субъективным условиям утечки информации относятся:

- незнание исполнителями нормативных актов по вопросам защиты информации;
- слабая воспитательно-профилактическая работа в коллективе;
- недостаточное внимание со стороны руководителей к вопросам обеспечения режима секретности;
- слабый контроль за состоянием системы сохранения секретов;

- принятие руководителями решений без учета требований режима секретности.

К объективным условиям утечки информации относятся:

- несовершенство или отсутствие нормативных актов, регламентирующих правила защиты информации по отдельным вопросам;
- несовершенство перечня сведений, подлежащих засекречиванию;
- текучесть кадров из режимных подразделений;
- несоответствие помещений требованиям, необходимым для осуществления работ с секретными документами и изделиями.

Указанные причины и условия создают предпосылки и возможности для образования канала утечки защищаемой информации. Не следует отождествлять это понятие с каналом связи, который представляет собой канал (физическую среду) передачи информации от одной системы (передатчика) к другой (приемнику).

Канал утечки защищаемой информации - это социальное явление, отражающее противостояние защитника (собственника) информации и его соперников. В зависимости от используемых соперником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают агентурные, технические, легальные и иные каналы утечки информации.

Агентурные каналы утечки информации - это использование противником тайных агентов для получения несанкционированного доступа к защищаемой информации.

Технические каналы утечки информации - это совокупность технических средств разведки, демаскирующих признаков объекта защиты и сигналов, несущих информацию об этих признаках.

Легальные каналы утечки информации - это использование соперником открытых источников информации, выведывание под благо-видным предлогом сведений у лиц, которым они доверены по службе.

Иными каналами утечки информации являются добровольная (инициативная) выдача сопернику защищаемой информации, экспортные поставки секретной продукции за рубеж и т.п.

Методы и средства добывания защищаемой информации могут быть гласными и негласными. Для добывания защищаемой информации, свободного доступа к которой нет, чаще применяются негласные силы, средства и методы. При этом источники добываемой информации могут быть открытыми и закрытыми. Проникновение к источникам защищаемой информации может сопровождаться преодолением режимных мер защиты информации. Обычно такая деятельность является противоправной и уголовно наказуемой.

В настоящее время достаточно условно разведку можно разделить на агентурную и техническую. Условность состоит в том, что добывание информации агентурными методами осуществляется с использованием технических средств, а техническую разведку ведут люди. Поэтому отличия заключаются только в преобладании человеческого или технического факторов.

Наиболее эффективным способом добывания защищаемой информации, является ***агентурная разведка***, которая базируется на использовании завербованных или внедренных тайных агентов. Одним из видов агентурной разведки является шпионаж - целенаправленное собирание, похищение, хранение и передача иностранному государству сведений, составляющих государственную тайну. Опасность шпионажа заключается в том, что эти действия подготавливают почву для других преступлений направленных на причинение вреда государственной безопасности, создающих угрозу территориальной неприкосновенности, военной мощи, экономическим интересам государства.

Методы агентурной разведки известны с древнейших времен. Например, еще в IV веке до нашей эры известный китайский полководец Сунь-Цзы в главе «Использование секретных агентов» своей книги «Трактат о военном

искусстве» раскрыл методы ведения шпионажа, многие из которых используются и в наши дни. Автор говорит о пяти видах агентуры: лица, имеющие доступ к секретным сведениям («внутренние шпионы»), местные жители («местные шпионы»), двойники («обратные шпионы»), перебежчики («шпионы смерти») и активно действующие агенты («шпионы жизни»).

Агентура из местных жителей и лиц, имеющих доступ к секретам – это негласные сотрудники, которых мы сейчас назвали бы агентами, внедренными в разрабатываемый объект.

Двойник – это агент, проникший в лагерь противника, разоблаченный его контрразведкой, перевербованный и используемый в «обратном» направлении.

Агенты-перебежчики – своеобразная китайская хитрость, используемая для дезинформации противника. Эти агенты, перебежав на другую сторону, становятся добровольными заложниками: их могут казнить, если узнают, что сообщенная ими информация ложна. Но готовность пожертвовать собой способствует тому, что противник без колебаний принимает дезинформацию за правдивые сведения. Как видно из истории, роль таких агентов исполняли послы или влиятельные люди государства, которые стремились своими действиями или переданной информацией ввести противника в заблуждение, склонить к действиям, которые принесут ему вред. Когда противник ослаблял бдительность и терял осторожность, противная сторона развязывала боевые действия.

Агенты, которых китайский военачальник назвал «активно действующими», позже стали называться агентами внедрения. Они проникают в расположение противника, собирают информацию и ухитряются возвратиться назад живыми.

Опасность агентурной разведки заключается в том, что агент имеет непосредственный доступ к секретной информации. Он находится среди тех, кто работает с секретными сведениями и осуществляет их защиту. Поэтому

разведки всех стран не скупятся, стремясь завербовать именно таких секретоносителей.

Для добывания защищаемой информации через агентуру используются следующие методы: доступ к секретам по службе, выведывание, наблюдение. Используя доступ по службе к секретным работам и документам агент спецслужбы в целях сбора интересующей его информации может ее запомнить, делать выписки из документов, копировать документы от руки или на ксероксе, сфотографировать и т.д. При выведывании информации расчет делается на людскую болтливость, жажду известности, утрату бдительности и просто внутреннюю расхлябанность. Наблюдение может быть физическим, электронным или комплексным, т.е. сочетающим в себе элементы того и другого. Физическое наблюдение осуществляется непосредственно агентом или иным лицом, заинтересованным в получении защищаемой информации. Электронное наблюдение основано на применении специальных технических средств, оно может сопровождаться фиксацией полученной аудио-и видеоинформации.

Техническая разведка - это вид разведывательной деятельности, которая направлена на выявление и фиксирование данных об интересующих объектах с помощью технических средств. Многообразие видов носителей информации породило множество видов технической разведки. При классификации по физической природе носителя информации техническая разведка подразделяется на следующие виды:

- оптическая (носитель - световое излучение в видимой и инфракрасной части спектра);
- радиоэлектронная (носитель - радиоволны и электрический ток);
- акустическая (носитель - звуковые колебания);
- химическая (носитель - частицы вещества);
- радиационная (носитель - радиоактивное излучение);
- магнитометрическая (носитель - магнитное поле).

Представленные виды технической разведки обеспечивают добывание, съем, перехват, копирование информации с любых известных носителей.

Говоря об опасности того или иного вида разведки, следует отметить, что, несмотря на достижения научно-технической революции, обусловившие широкое использование в разведывательных целях технических средств для добывания, обработки и хранения защищаемой информации, агентурная разведка все же остается наиболее опасной. Она может решать любые задачи, в том числе и те, которые решаются технической и иными разведками. Агентурная разведка может действовать избирательно, добывая наиболее важную информацию: документы, образцы изделий, сами сведения и т.п. Поэтому мероприятия по защите информации должны быть направлены прежде всего на перекрытие именно этого канала утечки информации.

Тема 2.2. Криминалистическая характеристика способов незаконного получения защищаемой информации

План.

1. Похищение документов, содержащих защищаемые сведения.
2. Незаконное получение конфиденциальной информации

Криминалистика различает два основных способа незаконного получения защищаемых сведений:

1) получение сведений путем завладения документом (или иным носителем информации, техническими средствами), в котором они содержатся;

2) получение сведений без завладения документом.

Первый способ включает в себя:

а) похищение документов, находящихся во владении ответственного за них лица (в том числе «заказные похищения» с участием специально внедренных агентов, либо представителей криминальных структур);

б) завладение документами, вышедшими из законного владения в результате его утраты и находящимися без охраны.

Второй способ охватывает:

а) получение сведений в устной форме от осведомленных о них лиц; б) получение неучтенных копий документов, изготовленных путем ксерокопирования, сканирования, копирования магнитных носителей; в) получение сведений в результате перехвата информации, циркулирующей в технических средствах, помещениях, средствах транспорта.

Как правило, для незаконного получения информации применяются:

1) похищение документов и других носителей информации;

2) выведывание защищаемой информации у осведомленных о ней лиц из числа сотрудников организации (в том числе и бывших) путем подкупа, угроз, уговоров, замаскированного выпытывания информации;

3) внедрение агентуры на должности, позволяющие получить непосредственный доступ к защищаемым сведениям и документам, либо скрытно собирать конфиденциальную информацию в процессе служебной (производственной) деятельности;

4) перехват информации, циркулирующей в технических средствах и помещениях (служебных, жилых и иных);

5) несанкционированный доступ к сведениям, содержащимся в средствах вычислительной техники и электронных банках данных. Поведение преступника в ходе реализации противоправных намерений складывается из активных и разнообразных действий, в ходе которых могут использоваться различные психологические приемы, технические и иные средства. Предпринимаются действия по маскировке

преступления, как правило, логически согласованные с предыдущим поведением преступника в процессе подготовки и совершения преступления. Все это оставляет характерные следы, позволяющие получить сведения о сути совершенного правонарушения (преступления), его обстоятельствах и виновном лице. Рассмотрим криминалистические особенности каждого из перечисленных выше способов получения защищаемой информации.

1) Похищение документов, содержащих защищаемые сведения.

Выбор способа похищения документа нередко определяется наличием тех или иных отступлений от правил конфиденциального делопроизводства, снижающих степень защищенности объекта посягательства.

В подавляющем большинстве случаев документы похищаются тайно. Тайное похищение состоит из следующих элементов:

1. Подготовка к совершению преступления.
2. Завладение документом.
3. Маскировочные действия.

Добывание защищаемых сведений, нередко связано с проведением масштабных, многоходовых подготовительных операций. Наиболее объемной по затратам усилий и времени, как правило, является подготовка к похищению документов, связанная с внедрением в организацию, владеющую сведениями, специальных агентов. Иногда такие «кроты» внедряются поэтапно, через промежуточные фирмы или государственные структуры.

В подобных случаях подготовительные действия агентов направлены на получение официального доступа к конфиденциальному делопроизводству, либо назначения на должность, позволяющую поддерживать деловые контакты с лицами, работающими с закрытыми материалами. Агенты устанавливают неслужебные связи с лицами, допущенными к конфиденциальному делопроизводству. Они выявляют устойчивые нарушения правил обращения с конфиденциальными документами с целью выбора ситуации, удобной для тайного завладения ими. Ищут возможность бесконтрольного пребывания в помещении, где хранится или обрабатывается конфиденциальная информация, пытаются получить в свое пользование штатный ключ от указанного помещения или сейфа. Заранее готовят тайники для краткосрочного или долговременного хранения похищенных конфиденциальных материалов.

Указанные действия могут дополняться: подысканием соучастников преступления; изготовлением, приисканием орудия совершения

преступления; устранением обстоятельств, препятствующих похищению. Часть указанных элементов подготовки к похищению документов характерна и для противоправных действий подкупленного сотрудника организации, а также лица, похищающего документы по собственной инициативе с целью их продажи.

В отдельных случаях подготовительный этап и маскировочные действия могут отсутствовать вовсе, либо присутствовать в предельно сжатой форме. Такие случаи, как правило, связаны с ситуативным формированием преступного умысла, в частности у лиц, имеющих санкционированный доступ к документам.

К числу подготовительных действий при похищении документов следует отнести различные виды слежки, которая проводится с целью выявления обстоятельств, способствующих совершению преступления. По словам одного из бывших руководителей DGSE каждый ее представитель за рубежом должен знать, какие крупные контракты заключаются в текущий период, внимательно следить за маршрутами поездок представителей фирм-конкурентов, чтобы прогнозировать возможные темы торговых переговоров и заблаговременно планировать операции по добыванию необходимой документации.

В ряде зарубежных коммерческих фирм существуют подразделения, которые занимаются вскрытием сейфов, тайным проникновением в гостиничные номера и установкой подслушивающих устройств в жилых помещениях конкурентов и возможных будущих партнеров с целью экономического шпионажа. С их деятельностью уже столкнулись представители российского бизнеса. Подразделения с негласными функциями слежки, подслушивания, снятия информации с технических каналов связи и т.п. в настоящее время имеются также в составе некоторых российских коммерческих структур.

По способу завладения документом похищение делится на два основных вида:

1. Завладение документом, находящимся в ведении ответственного лица без достаточной охраны

2. Завладение документом, вышедшим из ведения ответственного лица в результате утери.

Практика свидетельствует о том, что наиболее распространенным является первый вид похищений. Действия, совершенные указанным способом, несут более обширную криминалистическую информацию, а обобщенные данные о них отражают устойчивые характеристики
преступных посягательств на завладение документами[4].

Установлено, в частности, что более половины похищений документов совершено из запертых хранилищ, находившихся в служебных
кабинетах охраняемых помещений, с использованием штатного ключа. Похитители использовали основной или запасной ключи, хранившиеся в ненадлежащем месте, похищали их у ответственного лица, присваивали при передаче хранилища в пользование других сотрудников. Случаи использования при похищении нештатного ключа (путем подбора или подгонки) носили эпизодический характер.

Следующее место по распространенности занимает способ завладения документами, оставленными на время вне сейфа в служебном кабинете (иногда на квартире, в номере гостиницы), путем проникновения через незапертую дверь; через запертую дверь с использованием ключа либо отмычки и других приспособлений; иногда через незакрытое окно. Относительно менее распространены случаи, когда для противоправного завладения документом преступник использует факт его без учетной выдачи (выдачи, без надлежащего оформления) либо скрывает полученный
в установленном порядке документ после внесения незаконных изменений

[4] См.: Ткачук И.Б. Коммерческая тайна: организация защиты, расследование посягательств. – М.: «Щит-М», 1999. – С. 40.

в учеты ответственного лица (подложная запись, похищение расписки, реестра, карточки).

Последнее место по распространенности занимают случаи завладения документом, оставленным без надлежащей охраны в процессе санкционированного уничтожения. Тем не менее, именно этот способ представляется наиболее опасным, поскольку факт похищения и незаконного использования документов маскируется наиболее убедительно.

Специфическую разновидность похищений представляют собой случаи противоправного завладения документами, не обеспеченными должной охраной, в процессе их несанкционированного перемещения в транспортных средствах (самолетах и поездах), хранения в номерах и сейфах гостиниц и других мест проживания. Как правило, указанные хищения являются «заказными», и выполняются специально подготовленными сотрудниками государственных спецслужб, частных организаций либо криминальными элементами. Маршруты перемещения документов заранее отслеживаются, действия похитителей тщательно планируются и маскируются под обычную кражу.

При этом не исключается, что в отдельных случаях умысел похитителя действительно был направлен на похищение имущества (ПЭВМ, чемодан, портфель), а находившиеся в них документы в расчет не принимались. По имеющимся данным, конфиденциальные документы часто похищались при посягательствах на имущество ответственных лиц путем кражи, грабежа, разбойного нападения. Показательно, что во многих изученных случаях ответственные лица находились в нетрезвом состоянии.

Следует учитывать, что ошибочное завладение документом вовсе не исключает возможности причинения ущерба интересам обладателя защищаемой информации. При этом угроза перехода похищенного в распоряжение противника потенциально возрастает вследствие ненадлежащего обращения. Не исключается возможность возникновения у

похитителя новой цели, предусматривающей использование документа в ущерб интересам собственника.

Завладение документом, вышедшим из ведения ответственно лица в результате утери, является менее распространенным. Практика показывает, что в большинстве случаев утерянные документы обнаруживаются правопослушными гражданами, которые возвращают их по принадлежности либо передают правоохранительным органам. В то же время отдельные лица, обнаружив утерянный документ, завладевают им с противоправной целью, в том числе для разглашения либо незаконного использования содержащихся в нем сведений.

Отсутствие у таких лиц заранее сформировавшихся мотива и цели деяния, а также их устойчивых типологических черт личности, затрудняют выбор направления поисковых мероприятий. Следует учесть, однако, что отсутствие стойких побудительных мотивов в данном случае повышает возможности склонения злоумышленника к возврату похищенного документа. Положительные результаты в этом случае могут дать обращение через средства массовой информации, объявления об утрате иным способом.

Побудительным мотивом к возвращению документа могут стать желание лица получить официальное одобрение его поступка от имени организации, ведомства, сочувствие к ответственному лицу, жалость, надежда получить материальное вознаграждение.

В то же время не следует упускать из виду, что случайная утеря может быть использована злоумышленником, который в течение более или менее продолжительного времени вынашивал намерение завладеть документами, содержащими конфиденциальную информацию, и собирался осуществить его одним из способов при благоприятном стечении обстоятельств.

Основные направления маскировочных действий, которые применяют лица, похищающие документы, можно свести к следующим действиям:

1. *Сокрытие факта похищения.* Как правило, такие действия связаны с использованием специфического способа изъятия конфиденциальных

материалов, который не позволяет обнаружить их недостачи на основе документальных учетов. Чаще всего - это похищение документа во время санкционированного уничтожения. Известны факты похищения предметов и изделий, которые числятся израсходованными или использованными по назначению. В связи с тем, что названный способ позволяет скрыть не только участие в совершении преступления, но и сам факт преступления, он нередко используется лицами, посягающими на завладение документом с целью передачи организациям-конкурентам.

2. *Сокрытие участия в похищении документа.* Этот способ является наиболее распространенным направлением маскировочных действий похитителя. Правонарушители предпринимают активные действия по сокрытию и уничтожению следов проникновения в хранилище (сейф) и пребывания на месте происшествия, фальсифицируют материальные и идеальные следы, дающие основание подозревать в совершении преступления других конкретных лиц, либо порождающие видимость имевшей место утери документа, его ошибочного уничтожения, передачи другим лицам и т.п.

Просчеты лиц, проводящих разбирательство, дознание или предварительное следствие, в оценке сфальсифицированных следов могут значительно расширить число проверяемых версий, повлечь необоснованные подозрения в отношении непричастных лиц, ввести к необоснованному прекращению розыска. С другой стороны, выявление следов маскировочных действий нередко имеет существенное значение для распознания способа совершения преступления, получения других сведений, позволяющих определить верное направление розыска похитителя.

Изучение практики свидетельствует, что разбирательство (расследование) по событию утраты в отдельных случаях целесообразно начинать с поиска следов маскировки. Их обнаружение в значительном числе случаев способствовало получению данных, необходимых для раскрытия сути происшедшего, и предопределило успех поисков.

3. *Сокрытие подлинных мотивов завладения конфиденциальными материалами* встречается в случаях обнаружения их у похитителя либо поимки его с поличным. Некоторые из них разрабатывают ложные объяснения причин случившегося. Как правило, эти объяснения направлены на маскировку преступного характера событий. Завладение документом, в зависимости от обстоятельств, объясняется служебной необходимостью, ошибкой, небрежностью, желанием пошутить, «преподать урок бдительности», привлечь внимание к фактам нарушения правил конфиденциального делопроизводства.

Признаки умышленных действий, направленных на похищение документов, характеризуются следующими показателями. Похищение документов, произошедшее в условиях неочевидности, на первоначальном этапе разбирательства предстает в качестве события утраты. Выяснить существо этого события доподлинно без проверки версии возможного посягательства на завладение документов злоумышленника, а в случае ее подтверждения – без установления степени интенсивности действий похитителя, невозможно. В связи с этим особый интерес для лиц, изучающих факт исчезновения документа при невыясненных обстоятельствах, представляют признаки умышленных действий, направленных на похищение конфиденциальных материалов. Такими признаками являются:

1. Отсутствие документа в месте хранения, когда выход его из владения другим способом исключается.
2. Одновременное либо последовательное исчезновение нескольких документов, хранившихся в одном или разных местах (сейфах), либо использовавшихся в работе.
3. Исчезновение, наряду с утраченным документом, денег, ценных предметов, личных вещей, хранившихся в сейфе или в служебном кабинете, где находился сейф.
4. Вывод из строя либо отключение защитной сигнализации помещения, в котором хранился документ.

5. Наличие обстоятельств, свидетельствующих о намерении дезорганизовать работу учреждения либо отдельного лица с целью сокрытия следов другого преступления. Исчезновение документа накануне проверки сигнала о злоупотреблениях отдельных лиц и т.п.

6. Наличие обстоятельств, могущих вызвать озлобление, зависть и другие низменные чувства у похитителя: объявление взыскания, нежелательное перемещение по работе и пр.

7. Высказывание угроз похищения документа либо попытки противоправно завладеть им в период, предшествовавший событию.

8. Необычная осведомленность отдельных лиц об отсутствии документа наряду с проявлением замаскированного интереса во вскрытии факта утраты: анонимное сообщение об утрате, обращение с просьбой предоставить документ для выполнения работы, не вызывающейся необходимостью и т.п.

9. Поступление документа или его части в вышестоящие организации или в адрес лиц, наделенных функциями контроля, нетрадиционным способом.

Разумеется, названные признаки, взятые в отдельности, не всегда свидетельствуют о похищении документа. Они могут быть объяснены другими причинами. Чтобы избежать ошибки в их оценке следует опираться на комплекс взаимосвязанных обстоятельств, среди которых наиболее важное значение имеют следы похищения документов.

Умышленные посягательства на похищение документов с криминалистической точки зрения характеризуются наличием специфических материальных следов в месте хранения документа. Ими являются:

- следы несанкционированного отпирания сейфа - трассы нештатного ключа или отмычки, металлические опилки на деталях и коробе замка;
- нарушение целостности печати, либо следы ее временного удаления (с последующим восстановлением) путем срезания, отделения от корпуса

хранилища после замораживания, выворачивания проушин, крепящих приспособление для опечатывания;

- следы использования запасного ключа, хранящегося в уставленном месте (вскрытие пакета или пенала одним из способов);
- следы повреждения корпуса сейфа - взлом, отжим, разрезание;
- следы рук и одежды на корпусе сейфа, а также на документах и предметах, оставшихся после похищения в хранилище, в том числе частицы кожи и следы крови на острых кромках
- следы извлечения документа через проем поврежденного хранилища;
- следы проникновения постороннего на охраняемый объект и пребывания в помещении, где обнаружено отсутствие конфиденциальных материалов;
- вывод из строя или отключение защитной сигнализации
- признаки отпирания двери помещения нештатным ключом или отмычкой, отжима двери или ригеля замка, запирание двери необычным способом;
- признаки проникновения в помещение через окно либо каким-нибудь другим способом:
- следы рук, ног постороннего в помещении, выброшенные или оброненные им предметы.

Характерные материальные следы в ходе преодоления защитных средств, вскрытия сейфа и контакта с похищенными конфиденциальными материалами остаются на самом похитителе и его одежде. К ним относятся ссадины, царапины, микрочастицы документа или предмета.

Кроме того, противоправное завладение конфиденциальными материалами предполагает их использование (а в отдельных случаях - уничтожение) злоумышленниками. Это, в свою очередь, создает предпосылки обнаружения следов похищения и разоблачение виновных. К *следам использования* похищенных конфиденциальных материалов относятся:

- материальные следы на похищенном документе - отпечатки пальцев, наслоение микрообъектов и т.п. следы уничтожения похищенного документа
- клочки документа, обуглившиеся его части, несгоревшие фрагменты, скрепки, детали изделия, остатки вещества изделия либо продуктов его горения.

В широком смысле слова следами использования похищенных конфиденциальных материалов могут служить факты использования документа предприятиями-конкурентами, частными лицами с целью разглашения либо незаконного использования из корыстных побуждений, для учебных и научных целей, а также факты, свидетельствующие о получении лицом, подозреваемым в похищении конфиденциальных материалов, значительных денежных сумм или ценностей.

Международная и российская практика знает разнообразное множество других способов, которые используются для незаконного получения конфиденциальной информации.

Незаконное получение конфиденциальной информации путем похищения малогабаритных персональных компьютеров и магнитных носителей в целом не имеет существенных отличий от описанных выше примеров похищения документов. К числу особенностей в данном случае необходимо отнести следующие обстоятельства:

- технические средства, в которых содержится информация, в отличие от документов, чаще всего похищаются за пределами охраняемых служебных помещений (в авиационном или железнодорожном транспорте, гостиницах, временных служебных помещениях выставочных комплексов, в квартирах по месту постоянного проживания владельцев);
- к совершению указанного преступления нередко привлекаются лица из криминальной среды, специализирующиеся на незаконном проникновении в помещения и вскрытии сейфов и иных хранилищ

(французская DGSE использует в этих целях сотрудников так называемой службы «водопроводчиков»);

- нередко в совершение преступления вовлекается обслуживающий персонал гостиниц, авиа- и железнодорожных компаний;
- оказывающий похитителям помощь в проникновении в помещения и вскрытии сейфов;
- совершение преступления с целью незаконного получения конфиденциальной информации обычно маскируется под обычною кражу имущества.

Незаконное получение конфиденциальной информации путем выведывания. Типичные способы выведывания защищаемых сведений, (далее - выведывание сведений, выведывание), характеризуются следующими признаками.

Открытый опрос. Лицо подстрекается к разглашению доверенных ему сведений путем подкупа, угроз, уговоров. При этом могут быть использованы также обстоятельства, связанные с родственной, этнической или расовой близостью, желанием выместить обиду за несправедливость руководителей или увольнение. Сведения могут быть разглашены путем устного пересказа, предоставления возможности ознакомиться с текстом документа либо с текстом, выведенным на экран монитора ПЭВМ, а также путем передачи информации, скопированной на неучтенный твердый носитель (бумагу, дискету).

Замаскированное получение информации (разведопрос). В этом случае речь идет о применении специальных приемов получения информации от осведомленных лиц, которые разглашают защищаемую информацию, не осознавая этого. Например, сведения собираются из разрозненных высказываний и обмолвок осведомленных лиц, инициированных правонарушителем.

Этот прием, как правило, дополняется накоплением соответствующей информации из случайно услышанных или преднамеренно подслушанных (без использования технических средств) служебных разговоров, выступлений на совещаниях, просмотра текста на экране монитора. При этом лицо, собирающее информацию, может использовать для подслушивания недостаточную звукоизоляцию стен и перегородок, особенности конструкций вентиляционных воздуховодов и кондиционеров, отсутствие визуальной защиты экранов от неохраняемой зоны. Названные способы незаконного получения информации применяются в ходе совместной работы или неслужебного общения, в процессе торгово-промышленных выставок, презентаций, семинаров экспертов и бизнесменов.

Большое распространение приобрели случаи замаскированного сбора информации с использованием специальных анкет и вопросников, рассылаемых организациям по почте, телефаксу и другими способами. Как правило, подобные операции проводятся под прикрытием известных консультативных и иных фирм и мотивируются желанием наладить сотрудничество. Вопросы «разведывательного» характера дробятся, тщательно маскируются среди остальных. Безопасность этого способа и сравнительно небольшие расходы на его применение позволяют проводить подобные акции в широких масштабах.

Специально для выведывания конфиденциальных сведений организуются различные симпозиумы, конференции. В отдельных случаях учреждаются фирмы-однодневки, которые заключают ложные контракты и мнимые коммерческие сделки. Известны факты создания специально для завладения сведениями, составляющими коммерческую тайну, совместных предприятий. Как правило, исполнение контрактов и совместная деятельность сначала затягиваются, а затем и вовсе отменяются под надуманными предлогами.

Вследствие трудностей, возникающих при доказывании противоправности подобных деяний, лица собирающие информацию, как правило, остаются безнаказанными.

Незаконное получение конфиденциальной информации путем внедрения агентов. Особенности этого способа заключаются в получении защищаемых сведений путем внедрения специальных сотрудников – «кротов» на должности, позволяющие получить непосредственный доступ к информации и документам, либо скрытно собирать конфиденциальную информацию в процессе служебной (производственной) деятельности. Действия таких лиц, направленные на собирание сведений, могут заключаться:

- в похищении документов, бракованных или неучтенных копий, копировании документов с использованием фототехники, ксерокса, сканера, телефакса;
- в изготовлении дополнительных экземпляров документов при их тиражировании; в копировании магнитных носителей;
- в записи информации на диктофон либо на бумажный носитель, запоминании информации.

Для передачи (разглашения) собранных сведений могут использоваться личные встречи с «заказчиком» добытой информации (или другим лицом по его поручению), а также почтовые либо технические и другие каналы связи. Подготовка к внедрению «крота» включает в себя действия по добыванию сведений о владельце и видах охраняемой информации, местах ее хранения, процедуре получения, обработки, накопления, правилах ознакомления, возможности выноса документов и иных носителей за пределы территории. Выясняется установленный в организации порядок ознакомления с конфиденциальной информацией структура и эффективность деятельности службы безопасности, технические средства охраны. Тщательно изучаются требования к лицам, поступающим на работу, источники пополнения кадров. Разрабатывается легенда, убедительно аргументирующая факт поступления лица в организацию, положительно характеризующая его с деловой и личностной сторон. Предпринимаются действия, маскирующие его связи с конкурентами и криминальными элементами, отдельные биографические

данные, факты неблаговидного поведения или конфликтов с законом, кредиторами, налоговыми и иными правоохранительными органами.

Признаки, свидетельствующие о возможной причастности лица к категории «кротов», могут быть выявлены в процессе проверки, связанной с решением вопроса о допуске к работе с защищаемыми сведениями.

Наиболее эффективным направлением повышения защищенности информации торговых и промышленных секретов хозяйственных российских субъектов от проникновения лиц, внедренных специальными службами и организациями иностранных государств, преступными отечественными организациями, является организация делового сотрудничества с отечественными спецслужбами и правоохранительными органами. Удачным примером такого взаимодействия является совместная деятельность подразделений МВД РФ и служб безопасности Ассоциации российских банков в рамках соглашений о взаимодействии в области обеспечения банковской безопасности.

Незаконное получение конфиденциальной информации путем перехвата информации, циркулирующей в технических средствах и помещениях.

Действия, направленные на незаконное получение сведений, циркулирующих в технических средствах и помещениях, существенно различаются в зависимости от того, с каких объектов и каким способом снимается информация, использовал ли правонарушитель технические средства и устройства перехвата информации (какие именно) или получал сведения путем непосредственного восприятия без использования технических средств

Объекты, с которых снимается информация, разделяются на основные технические средства и системы (и их коммуникации), используемые для обработки, хранения и передачи конфиденциальной информации, и вспомогательные технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами или в

защищаемых помещениях. К ним относятся различного рода телефонные средства, средства радиосвязи, охранной и пожарной сигнализации, системы кондиционирования, системы проводной радиотрансляционной сети, средства электронной оргтехники.

Особенности перехвата информации с помощью технических средств различаются в зависимости от того, сигнал какого объекта информатизации они снимают, каким способом снимается и передается информация, является ли устройство стационарным или переносным, располагается ли оно в пределах защищаемой зоны либо за ее пределами

В число обычно применяемых устройств перехвата информации входят автономные автоматические средства и электронные устройства («закладки»); устройства перехвата информации, подключенные к каналам связи; портативные устройства для перехвата электронных сигналов и накопления информации, перемещаемые субъектом под одеждой (скрытоносимые), либо замаскированные в находящихся при нем вещах или «нейтральных» приборах при посещении служебных жилых и иных помещений.

Электронные устройства перехвата информации различаются на следующие виды:

- встроенные в основные технические средства обработки и передачи информации (как правило, до их приобретения организацией - собственником защищаемых сведений);
- снимающие информацию за счет побочных электромагнитных излучений;
- снимающие информацию в виде акустического (речевого) сигнала.

Внедрение устройств перехвата информации второго и третьего типа в ограждающие конструкции помещения, системы отопления и вентиляции, мебель и другие предметы интерьера, а также линии и арматуру систем связи, электропитания, освещения и сигнализации, как правило, требует проникновения в защищаемое помещение (на охраняемую территорию).

Аппаратура виброакустического перехвата устанавливается с использованием механического или оптического контакта с ограждающими конструкциями помещения.

Перечисленные выше различия технических средств непосредственно связаны со способом их установки и использования и определяют особенности личности правонарушителя. Так, лицо внедряющее «закладку» в защищаемом помещении должно располагать определенными техническими навыками, иметь возможность временного либо бесконтрольного постоянного пребывания в помещении. Указанные лица, как правило, являются сотрудниками организации либо представителями технических и иных служб организаций, участвующих в наладке и ремонте оборудования.

Средства перехвата информации, скрытно устанавливаемые за пределами защищаемого помещения (территории), могут представлять собой устройства, не требующие механического контакта с контролируемым объектом, либо подключаться к линиям и коммуникациям, выходящим за пределы защищаемой территории. Установку указанных средств может осуществить лицо, не связанное с работой в конкретной организации.

Перехват информации, циркулирующей в защищаемом помещении или средствах информатизации без использования специальных технических средств, как правило, осуществляется путем прослушивания (подслушивания) разговоров.

К разряду указанных способов перехвата информации относится прослушивание телефонных переговоров с помощью контрольной аппаратуры под видом проведения профилактических работ на АТС, кроссах, кабельных коммуникациях, просмотра информации с экранов дисплеев и других средств ее отображения через двери и окна.

Получение информации без использования технических средств, как правило, связано с пребыванием собирающего ее лица непосредственно в

защищаемом помещении. Таким лицом обычно является сотрудник организации.

Следами совершения правонарушения могут служить:

- наличие радиоизлучений, свидетельствующих о функционировании электронных «закладок» и аппаратуры виброакустического перехвата, находящихся в технических средствах, конструкциях помещений, мебели и других предметах интерьера, в механическом либо оптическом контакте с оконными рамами, стеклами и другими конструкциями помещения, либо подключенных к каналам связи;
- механические изменения в конструкциях помещения, системах отопления и вентиляции, мебели и других предметах интерьера, а также на линиях и арматуре систем связи, электропитания, освещения и сигнализации, произошедшие в результате установки указанных закладок и аппаратуры;
- наличие повреждений на двери защищаемого помещения отсутствие штампа на печати, которой она опечатана;
- признаки отпирания замка нештатным ключом;
- признаки несанкционированного проникновения лица в защищаемое помещение;
- повреждение изоляции кабеля и проводов связи;
- появление несанкционированного разрыва линии (и восстановления) связи;
- нарушение целостности печати или пломбы кабельных колодцев и распределительных шкафов (коробок);
- повреждение изоляции шнуров в пультах коммутаторов.

Незаконное завладение конфиденциальной информацией содержащейся в средствах вычислительной техники и автоматизированных системах. Действия лиц, незаконно завладевающих конфиденциальной информацией, содержащейся в средствах

вычислительной техники и автоматизированных системах, обусловлены видом и особенностями носителя информации.

В одних случаях посягательство может быть совершено на технические или программные средства вычислительной техники, средства и линии связи, предназначенные для перемещения и копирования
информации.

В других - злоумышленник посягает на накопители памяти ЭВМ, в которых может находиться информация, на магнитные или бумажные носители информации.

Типичным способом реализации умысла является внедрение в объект информатизации программных или технических средств, позволяющих обойти средства защиты и получить несанкционированный доступ к информации. Не менее распространенным является перехват информации, содержащейся в средствах вычислительной техники с использованием радиоэлектронных средств.

Кроме того, для противоправного завладения защищаемой информацией может использоваться хищение машинных или других оригиналов носителей информации, программных или аппаратных ключей и средств криптографической защиты информации.

Не следует упускать из виду, что действия злоумышленников могут быть направлены не только на преодоление технических и программных средств защиты. В качестве способа незаконного получения информации может быть использовано воздействие на сотрудников организации, имеющих официальный доступ к сведениям, в виде подкупа, угроз, шантажа. Последствием несанкционированного доступа к защищаемой информации могут быть ознакомление со сведениями путем прочтения, копирование информации, завладение оригиналами носителей информации, внесение изменений в содержание информации или ее уничтожение.

Следами незаконного завладения информацией, содержащейся в средствах вычислительной техники и автоматизированных системах, служат

зарегистрированные ЭВМ сведения о попытках несанкционированного доступа (дата, время, использование конкретных технических и программных средств). О совершенных противоправных действиях может свидетельствовать обнаружение в объекте информатизации нештатных программных или технических средств.

Признаками незаконного завладения информацией могут служить следы хищения машинных или других оригиналов носителей информации, программных или аппаратных ключей и средств криптографической защиты информации. Способы их обнаружения и фиксации не имеют принципиальных отличий от следов похищения конфиденциальных документов, описанных выше.

Для получения наиболее полной информации о событии противоправного завладения защищаемыми сведениями имеет криминологическая характеристика личности правонарушителя, то есть субъекта посягательства.

В первую очередь это касается ее отношения к

организации - обладателю сведений. Так, штатные сотрудники организации, обслуживающие средства вычислительной техники, связи, оперативную полиграфию, как правило, допущены к конфиденциальному делопроизводству и имеют возможность входить в помещение, где производится обработка информации. Они, в первую очередь, должны быть проверены на причастность к утечке конфиденциальной информации.

Другими субъектами утраты сведений могут стать приватные специалисты, сотрудники смежных и обслуживающих организаций, программисты и математики-криптографы, разработчики технологических систем обработки информации и наладчики оборудования. Не имея официального доступа в защищаемое помещение либо на охраняемую территорию, они могут получить информацию используя произвольные каналы связи с банками данных или специально разработанные программы. Следует иметь в виду и возможность причастности к противоправному завладению информацией

криминальных элементов. Последние могут являться сотрудниками организации либо не быть ими.

Лабораторная работа: Криминалистическая характеристика способов незаконного получения защищаемой информации

При поведении занятия необходимо рассмотреть следующие ***вопросы:***

Методы расследования фактов утраты конфиденциальных документов. Похищение документов, содержащих защищаемые сведения. Типичные свойства личности субъектов, совершающих похищение документов. Основные направления маскировочных действий, которые применяют лица, похищающие документы. признаки умышленных действий, направленных на похищение конфиденциальных материалов. Незаконное получение конфиденциальной информации путем выведывания. Незаконное получение конфиденциальной информации путем внедрения агентов. Незаконное получение конфиденциальной информации путем перехвата информации, циркулирующей в технических средствах и помещениях. Незаконное завладение конфиденциальной информацией содержащейся в средствах вычислительной техники и автоматизированных системах.

Рекомендуемая литература:

1. Конев, И. Информационная безопасность предприятия / И. Конеев, А. Беляев. - СПб.: БХВ-Петербург, 2003. - 752 с.
2. Информатизация бизнеса: концепции, технологии, система / А.М. Карминский, С.А. Карминский, В.П. Нестеов, Б.В. Черников. - М.: Финансы и статистика. 2004. - 624 с.

Тема 2.3. Принципы защиты информации.

План.

1. Правовые принципы защиты информации.
2. Организационные принципы защиты информации.
3. Специфические принципы защиты информации.

Под принципами защиты секретной или конфиденциальной информации понимаются основополагающие теоретические идеи и важнейшие практические рекомендации по организации и осуществлению этой деятельности. Они учитываются при создании нормативной базы защиты информации, вводятся в качестве правовых норм в законодательные и подзаконные нормативные акты, и, таким образом, становятся нормативными требованиями, обязательными для исполнения субъектами защиты информации. Эти принципы выработаны длительной практикой деятельности режимных организаций и подразделений в нашей стране, в них также учитывается зарубежный опыт защиты государственных и иных секретов. Большинство действующих нормативных документов, в которых заложены эти принципы, регламентируют вопросы защиты государственных секретов, однако в силу универсальности таких принципов, они могут и должны использоваться при организации защиты коммерческой, профессиональной, личной и иных видов тайны. Принципы защиты информации можно разделить на правовые и организационные.

Правовые принципы защиты информации гарантируют соблюдение законности при засекречивании информации и обеспечении ее защиты от неправомерного получения и использования.

Принцип законности защиты информации заключается в необходимости нормативно-правового регулирования этой важной области общественных отношений в государстве. В законодательных и подзаконных нормативных актах должны быть четко и однозначно определены права и обязанности субъектов защиты информации, детально изложены критерии отнесения сведений к государственной, коммерческой и иным видам охраняемой законом тайны, подробно регламентирован порядок засекречивания информации и правил ее защиты, а также установлена уголовная, административная, материальная и иная ответственность за незаконное покушение на защищаемую информацию.

Должностные лица и другие работники учреждений и предприятий, которым по службе или работе доверяются секреты, в соответствии с законами и подзаконными актами должны наделяться правами, необходимыми для обеспечения надежной защиты доверенной им секретной или конфиденциальной информации. При этом на них возлагаются обязанности по соблюдению требований соответствующего режима, выполнение которых обеспечивает сохранность информации.

Принцип приоритета международного права над внутригосударственным предусматривает, что объектом засекречивания не могут быть сведения, которые подлежат открытому использованию в соответствии с международными соглашениями. Наша страна приняла на себя обязательство привести свое внутреннее законодательство в соответствие с положениями конвенций и соглашений Европейского союза, Международного валютного фонда и других международных экономических организаций, участником которых она является. Одним из условий членства в этих организациях является предоставление информации о реальном положении дел в национальной экономике.

Принцип равноправия на засекречивание информации означает право суверенного государства наравне с другими странами защищать и засекречивать сведения из тех областей, которые обеспечивают его национальную безопасность. Каждое государство имеет право само решать, что оно будет засекречивать, а что открывать. При этом взаимность и равноправие между государствами или их коалициями на защиту национальных секретов будет способствовать развитию доверия в международных отношениях, помогать устранению асимметрии режимных ограничений, сложившихся в разных странах. Излишняя закрытость государства всегда вызывает настороженность других стран, так как такие действия обычно связывают с недобрыми намерениями.

Принцип собственности на информацию определяет право собственников (владельцев) информации принимать меры к ее защите. Для этого могут использоваться нормы авторского и патентного права, механизмы защиты интеллектуальной собственности, коммерческой или банковской тайны и др. Только собственник информации имеет право определять, какие сведения следует засекретить, какой гриф (степень) секретности им присвоить, кого к ним допускать, какие материальные средства расходовать на их защиту, какие методы и средства использовать для обеспечения защиты принадлежащей ему информации. В связи с этим в российском законодательстве приняты правовые акты, регламентирующие имущественные отношения в области интеллектуальной собственности, информационных ресурсов, коммерческой тайны, а также регулирующие права собственников на владение, распоряжение и защиту информации.

Принцип экономической целесообразности защиты информации заключается в том, что затраты на защиту сведений должны быть экономически оправданы. Секретность должна оцениваться как потребительское свойство и ее стоимость должна включаться в цену производимого продукта. Прибыль от использования секретной информации должна окупать затраты на осуществление режимных мероприятий по ее защите. Секретность является также и экономической категорией, поэтому ее соблюдение в условиях рыночной экономики является делом владельцев секретов, которые должны сами устанавливать степень время действия секретности сведений с учетом потенциальной выгоды при ее использовании или возможных убытков при ее утечке. В области защиты государственной тайны действуют и другие (политические, военные и т.д.) факторы при решении проблем защиты информации.

Организационные принципы защиты информации отражают общие правила и подходы к защите секретов, поэтому они за последние годы претерпели значительно меньше изменений по сравнению с правовыми принципами. Они используются при любой общественно-политической и экономической

системе, являясь одинаково эффективными при защите государственной, коммерческой, банковской, профессиональной или иной тайны.

Принцип системного подхода к организации защиты информации предполагает, с одной стороны, выявление возможных каналов утечки защищаемой информации, а с другой - изучение возможностей противника (конкурента) по добыванию защищаемой информации. Такой анализ осуществляется с учетом условий деятельности определенного предприятия, учреждения, отрасли или в отношении конкретной проблемы. Системный подход позволяет создать органически взаимосвязанную совокупность сил, средств и специальных методов для оптимального ограничения сферы обращения защищаемой информации и предотвращения несанкционированного доступа к ней. При создании системы защиты информации осуществляется комплекс защитных мер, направленных на предупреждение утраты и утечки информации.

Принцип максимального ограничения числа лиц, допускаемых к защищаемой информации, широко применяется во всех сферах деятельности государственных и коммерческих структур при осуществлении защиты информации. Основной смысл этой меры сводится к тому, что сохранность засекреченной информации находится в прямой зависимости от количества лиц, допущенных к обращению с нею. Чем уже этот круг, тем выше вероятность сохранения в тайне данной информации. Оганизационно эта защитная мера реализуется следующим образом: к секретными работам и документам допускаются только те лица, которые имеют разрешение (допуск) на ознакомление со сведениями с соответствующей степенью секретности и право доступа к конкретной информации, с которой они непосредственно связаны по работе.

Принцип персональной ответственности за сохранность доверенных секретов эффективен в том случае, когда каждый сотрудник, допущенный к защищаемой информации, осознает личную заинтересованность в сохранении в тайне доверенной ему информации. Если же работник видит,

что сохранение какой-то информации в тайне нужно лишь предприятию или государству, а ему лично ничего не дает, то он будет относиться к защите информации формально, выполняя соответствующие требования только лишь из боязни ответственности. При этом эффективным способом повышения ответственности сотрудников за сохранение доверенных им секретов является обучение их правилам защиты информации и обращения с конфиденциальными документами.

Принцип непрерывности защиты информации означает, что защитные мероприятия должны осуществляться непрерывно с момента появления этой информации, на всех этапах ее обработки, передачи, использования и хранения, вплоть до этапа ее уничтожения или рассекречивания. При этом должностные лица, имеющие отношение к работам с защищаемой информацией, при решении производственных, финансовых, маркетинговых и иных задач не должны упускать из виду и связанные с ними режимные вопросы.

Рассмотренные выше организационные и правовые принципы защиты информации имеют достаточно общий и универсальный характер, поэтому они в равной степени используются в различных областях деятельности. Однако при осуществлении защиты различных видов информации и информационных процессов используются и специфические принципы, обусловленные особенностями предмета защиты, а также применяемых в защитных целях сил, средств и методов.

Тема 2.4. Мероприятия, методы и средства защиты информации.

План.

1. Понятие защиты информации.
2. Мероприятия по защите информации.
3. Методы защиты информации.
4. Способы защиты информации.

5. Средства защиты информации

Защищаемая информация может составлять государственную, служебную, коммерческую и иные виды охраняемой законом тайны, каждый из которых имеет свои особенности в области регламентации, организации и осуществления этой защиты. Наиболее общими признаками защиты любого вида охраняемой информации являются следующие:

- защиту информации осуществляет ее собственник или уполномоченные на то лица;
- защита информации направлена на сохранение прав собственника владеть и распоряжаться информацией;
- защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющих несанкционированный доступ к засекреченной информации.

Защищаемая информация обычно не просто хранится в сейфах - она постоянно используется, обращается, устаревает и обновляется. Чтобы эта информация не стала достоянием посторонних лиц, ее собственник устанавливает определенный режим, ограничивающий сферу обращения этой информации. Выход засекреченной информации за пределы режимной сферы будет создавать угрозу ознакомления с ней лиц, от которых она защищается.

В настоящее время защита информации не ограничивается только решением задач сохранения секретных сведений от возможной утечки или утраты. Широкое использование компьютерной техники при обработке, накоплении и хранении информации требует обеспечения защиты информационных массивов от разрушения, искажения, подделки, блокирования и иных вмешательств в информацию и информационные системы. Таким образом, защита информации - это деятельность собственника информации или уполномоченных им лиц по обеспечению своих прав на владение,

распоряжение и управление защищаемой ин-формацией, предотвращению утечки и утраты информации, сохранению ее полноты, достоверности и целостности, обеспечению секретности защищаемой информации в соответствии с законодательными и иными нормативными актами.

Защита информации тесно связана с обеспечением режима секретности, который представляет собой комплекс мер по защите ин-формации на конкретном объекте (в министерстве, ведомстве, организации) или при выполнении определенной работы (например, при разработке нового вида изделия). Основная задача режима секретности заключается в установлении на режимном объекте уровня защиты информации, соответствующего степени секретности имеющихся там защищаемых сведений. Таким образом, режим секретности - это реализация на конкретном объекте действующих норм и правил защиты сведений, составляющих государственную, коммерческую или иную охраняемую законом тайну.

Режим секретности предусматривает осуществление различных защитных мер:

- внедрение разрешительной системы, определяющей порядок доступа сотрудников к защищаемой информации или в определенные помещения, где ведутся секретные работы;
- соблюдение правил секретного делопроизводства по размножению, обращению, пересылке секретных документов;
- установление пропускного и внутриобъектового режима, соответствующего степени секретности сведений, имеющихся на объекте;
- проведение воспитательно-профилактической работы с сотрудниками, работающими с защищаемой информацией.

Следует отметить, что обеспечение режима секретности на объекте создает определенные трудности для работающих с защищаемой информацией. Во-первых, режимные требования приводят к некоторому замедлению решения управленческих, служебных, научных и производственных задач. Это вызвано необходимостью совершения различных формальностей, связанных

с получением, регистрацией и своевременной сдачей секретных документов. Во-вторых, разрешительная система ограничивает возможности работников использовать в своей деятельности информацию, не относящуюся к области их непосредственной деятельности. Система допуска к защищаемой информации создается таким образом, что каждый специалист может знакомиться только с теми сведениями, которые нужны ему по службе.

Направления защиты информации определяются используемыми мероприятиями по обеспечению защиты секретных и конфиденциальных сведений.

Правовые меры, регламентирующие вопросы защиты информации, можно разделить на две основные группы:

- законы и подзаконные акты, указы Президента и постановления Правительства России, ведомственные нормативные акты, регламентирующие правила защиты информации;
- уголовный, гражданский и административный кодексы России, другие правовые акты, устанавливающие ответственность за покушение на сведения, составляющие государственную или иную тайну, за преступления против установленного порядка сохранения засекреченной информации.

Уголовно-правовые нормы, с одной стороны, запрещают гражданам под страхом уголовного наказания совершать преступления против защищаемой информации, а с другой - обязывают органы внутренних дел, федеральной службы безопасности, суда и прокуратуры привлекать лиц, виновных в таких преступлениях, к уголовной ответственности. Кроме этого, нарушения режима секретности, правил сохранения государственной и иной тайны могут повлечь ответственность материального, дисциплинарного или административного характера, например увольнение со службы, отстранение от секретных работ, понижение в должности или звании, лишение допуска к секретным работам и документам.

Организационные мероприятия по защите информации направлены на организацию выполнения правил, процедур и требований защиты государственной или иной тайны на основе правил, установленных законами и подзаконными актами. Эти мероприятия предусматривают тщательный подбор и расстановку кадров, обучение сотрудников правилам защиты информации, контроль за соблюдением режима секретности.

Организационные мероприятия направлены на предотвращение утечки защищаемой информации в печати, при контактах сотрудников с иностранцами и возникновении других условий, создающих объективные предпосылки появления каналов утечки информации. Основное их назначение - предотвратить несанкционированный доступ к защищаемой информации, ее разглашение или раскрытие.

Инженерно-технические мероприятия по защите информации - это комплекс организационных и технических мероприятий, направленных на то, чтобы исключить или существенно затруднить добывание с помощью технических средств разведки (ТСР) защищаемой информации. Всю совокупность инженерно-технических мероприятий можно разделить на три группы: общепредупредительные, организационно-технические и технические меры.

Общепредупредительные меры включают в себя правовое регулирование вопросов использования технических средств в процессе выполнения секретных работ, установление и поддержание соответствующего режима секретности для предотвращения утечки защищаемой информации.

Организационно-технические меры включают в себя анализ и обобщение информации о новых разработках ТСР, определение их возможностей и составление прогнозов их развития, выработка способов защиты информации от ТСР.

Технические меры включают комплекс инженерно-технических средств и мероприятий, используемых для скрытия от ТСР защищаемых сведений и технической дезинформации соперника. Они реализуются путем использования специальных транспортных средств, аппаратуры

засекречивания. Для маскировки различных излучений, снижения их интенсивности и изменения спектра используют средства электронного зашумления, естественные и индустриальные помехи, эквивалентные и направленные антенны, а также введение режима радиомолчания и соблю дение установленных правил использования средств связи и вычислительной техники.

Программно-математические мероприятия предусматривают проведение комплекса следующих мер по защите информации в средствах вычислительной техники (СВТ):

- *меры организационно-режимного характера*: обеспечение установленного режима для помещений, где производится компьютерная обработка и накопление защищаемой информации, соблюдение правил секретного делопроизводства при компьютерном наборе документов;
- *меры инженерно-технического характера*: экранирование помещений, электронное зашумление, использование сертифицированных компьютеров и др.;
- *программно-технические меры*, разграничивающие доступ пользователей информационных сетей к соответствующим категориям защищаемой информации, антивирусные программы и др.;
- *криптографические меры* по кодированию и шифрованию информации в СВТ.

Для защиты информации используют следующие основные методы: скрытие, ранжирование, дезинформация, дробление, морально-нравственные меры, учет, кодирование и шифрование.

Скрытие защищаемой информации является одним из наиболее широко применяемых методов. Его сущность заключается в проведении следующих мероприятий:

- засекречивание информации, установление на носителях соответствующего ей грифа секретности и разграничение в связи с этим доступа к ней пользователей в соответствии с имеющимся у них допуском;

- устранение или ослабление технических демаскирующих признаков объектов защиты и технических каналов утечки информации.

Ранжирование защищаемой информации осуществляется путем деления ее по степени секретности, разграничения доступа к ней в соответствии с имеющимся у пользователя допуском, предоставления отдельным пользователям индивидуальных прав на пользование секретными документами и выполнение секретных работ. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации. Этот метод является частным случаем метода скрытия, так как информация скрывается от тех пользователей, которые не имеют к ней допуска.

Дезинформация заключается в распространении заведомо ложных сведений относительно истинного назначения каких-либо объектов или содержания защищаемых сведений. Она обычно проводится путем распространения ложной информации по различным каналам, имитацией
или искажением признаков и свойств отдельных элементов объектов защиты, осуществлением ложных действий, по своим признакам похожих на интересующие соперника действия и др.

Частным случаем дезинформации является легендирование – снабжение противника искаженными сведениями о характере и предназначении защищаемой информации или объекта, когда их наличие полностью не скрывается, а маскируются действительное предназначение и характер действий.

На практике, учитывая очень высокую степень развития современных средств ведения разведки, является чрезвычайно сложным полное скрытие информации об объектах. Так, современные средства фоторазведки позволяют делать из космоса снимков с разрешающей способностью в несколько десятков сантиметров.

Дробление (расчленение) информации на части осуществляется для того, чтобы знание какой-то одной ее части не позволило восстановить всю

картину. Этот метод широко применяется при производстве средств вооружения, но может использоваться и для защиты технологических секретов, составляющих коммерческую тайну.

Морально-нравственные методы защиты информации предполагают воспитательную работу с сотрудником, допущенным к секретным работам и документам, направленную на формирование у него определенных моральных принципов, взглядов и убеждений, таких как патриотизм, понимание важности защиты информации для него лично, его работы, организации, ведомства и государства в целом. При этом воспитательная работа может дополняться методами профилактики и контроля, иными способами привития положительных качеств у сотрудников.

Учет - один из важнейших методов защиты информации, позволяющий контролировать наличие и местонахождение носителей защищаемой информации, а также данные о лицах, которые ими пользовались. Основными принципами учета являются:

- обязательность регистрации всех носителей защищаемой информации;
- однократность регистрации конкретного носителя такой информации;
- указание в учетах адреса, куда отправлен или где находится в настоящее время данный носитель засекреченной информации;
- единоличная ответственность за сохранность каждого носителя защищаемой информации.

Кодирование заключается в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, а также при обработке и хранении информации в СВТ. Для кодирования используются обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при помощи которых информация может быть закодирована таким образом, что прочесть ее можно будет, только располагая соответствующим ключом (кодом) для ее

раскодирования. Кодирование информации может производиться с использованием технических средств или вручную.

Шифрование информации обычно используется при передаче сообщений по техническим каналам связи (радио, проводным, компьютерным сетям). Шифрование заключается в преобразовании информации в вид, исключающий понимание ее содержания, если перехвативший не имеет соответствующего ключа для расшифровки. Шифрование может быть предварительным, когда текст документа шифруется заблаговременно перед его передачей по телетайпу, электронной почте и иным средствам связи, или линейным, когда шифрование информации (разговора, текста, графического изображения, компьютерного файла) производится непосредственно в процессе передачи. Для шифрования обычно используется специальная засекречивающая аппаратура (шифрмашины), аналоговые и цифровые скремблеры.

О важности и эффективности такой меры защиты информации свидетельствует то, что государственным шифрам, кодам и соответствующей засекречивающей аппаратуре обычно присваивается наиболее высокий гриф секретности, так как они дают ключ к рассекречиванию перехваченных радиограмм.

В настоящее время разработано множество методов и средств защиты информации. Их многообразие определяется множеством известных способов воздействия на дестабилизирующие факторы, создающих угрозы защищаемой информации. Рассмотрим содержание этих способов.

Препятствие заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры. Типичными примерами препятствий являются блокировки, не позволяющие техническому устройству или программе осуществить несанкционированные действия; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств и т.п.

Управление заключается в определении на каждом этапе функционирования системы обработки информации таких управляющих воздействий на элементы системы, следствием которых будет решение задач защиты информации. Например, управление доступом на объект включает следующие функции защиты:

- идентификацию лиц, претендующих на доступ, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка предполагает такие преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется. К маскировке относятся криптографические методы преобразования информации, скрытие, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы.

Регламентация заключается в разработке и использовании таких правил обращения с конфиденциальной информацией и средствами ее обработки, которые позволят максимально затруднить получение этой информации злоумышленником.

Принуждение – создание таких условий, в которых сотрудники вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение есть способ защиты информации, заключающийся в стимулировании персонала материальными, моральными, этическими психологическими и другими мотивами к соблюдению установленных правил защиты информации.

Как отдельный способ, применяемый при ведении активных действий противоборствующими сторонами, можно выделить такой способ, как *нападение*. При этом подразумевается как применение информационного оружия при ведении информационной войны, так и непосредственное физическое устранение противника (при ведении боевых действий) или его средств разведки.

Рассмотренные выше способы обеспечения защиты информации реализуется посредством применения различных средств. **Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, компьютерных**

программ, используемых для решения различных задач по защите информации.

Средства защиты информации делятся на физические, аппаратные и программные.

Физические средства – механические, электрические, электронно-механические и другие устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

Аппаратные средства – различные электронные и электронно-механические устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Например, для защиты от утечки по техническим каналам используются генераторы шума.

Программные средства – специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения

автоматизированных систем с целью решения задач защиты информации. Это могут быть различные программы по криптографическому преобразованию данных, контролю доступа, защиты от вирусов и др.

Физические и аппаратные средства объединяются в класс *технических средств защиты информации*. К ним предъявляются следующие требования:

- состояние постоянной готовности к применению;
- высокая степень вероятности обнаружения попыток несанкционированного проникновения на режимный объект, к носителям защищаемой информации;
- высокая аппаратная надежность;
- малое энергопотребление и возможность автономного электроснабжения аппаратуры;
- малые габаритные размеры, обеспечивающие малозаметность технических средств защиты информации;
- минимальные затраты на техническое обслуживание.

С помощью технических средств защиты информации решаются следующие задачи:

1. Создание физических (механических) препятствий на пути проникновения к носителям информации (решетки, сейфы, бронированные двери и стекла, замки и др.).
2. Выявление попыток проникновения на объект охраны, к местам сосредоточения носителей защищаемой информации (средства охранной сигнализации).
3. Предупреждение о возникновении чрезвычайных ситуаций (пожар, наводнение и т.п.) и их ликвидация (пожарная сигнализация, средства пожаротушения, средства оповещения и т.п.).
4. Поддержание связи с различными организациями, подразделениями, помещениями и другими объектами охраны (радио- и проводные средства связи, сигнальные устройства и т.п.).

5. Нейтрализация, поглощение или отражение излучения используемых радиотехнических устройств (экраны, защитные фильтры, разделительные устройства в сетях электроснабжения, средства электромагнитного зашумления и т.п.).

6. Введение технических разведок в заблуждение (дезинформация) относительно истинного содержания защищаемой информации.

7. Комплексная проверка режимных помещений, использующихся каналов связи и средств обработки информации на соответствие требованиям безопасности информации, профилактические мероприятия по защите использующейся там информации (средства акустического зашумления помещений, «прожигатели» телефонных подслушивающих устройств, индикаторы электромагнитных излучений, программно-аппа-ратные средства контроля радиоэфира и т.п.).

8. Комплексная защита информации в автоматизированных системах обработки данных с помощью фильтров, электронных замков и ключей, систем разграничения доступа к защищаемой информации в целях предотвращения ее несанкционированного копирования, искажения или изменения.

К несомненным достоинствам технических средств относятся:

- широкий круг решаемых задач;
- достаточно высокая надежность;
- возможность создания развитых комплексных систем защиты;
- гибкое реагирование на попытки несанкционированных действий;
- традиционность используемых методов осуществления защитных функций.

Основные недостатки технических средств заключаются в следующем:

- высокая стоимость многих средств;
- необходимость регулярного проведения регламентных работ и контроля;
- возможность подачи ложных тревог.

Лабораторная работа: Мероприятия, методы и средства защиты информации

Вопросы для обсуждения:

Понятие защиты информации. Мероприятия по защите информации. Методы защиты информации. Способы защиты информации. Средства защиты информации.

Рекомендуемая литература:

1. Шлыков, В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. - СПб: Алетейя,1999. - 138 с.
2. Куприянов, А.И. Основы защиты информации: учеб. пособие для вузов / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. - М.: Академия, 2007. - 256 с.

Тема 2.5. Понятие защищаемой информации.

План.

1. Особенности защищаемой информации
2. Носители защищаемой информации
3. Классификация защищаемой информации

Основу любой деятельности людей составляет ее информационное обеспечение. Информация становится одним из основных средств решения задач государственной, производственной, научной, коммерческой или иной деятельности. Однако в некоторых случаях эта информация чего-то стоит только тогда, когда она известна ограниченному кругу лиц.

Информация как категория, имеющая действительную или потенциальную стоимость, как и любой другой вид ценности, охраняется и защищается ее собственником или владельцем. Собственник защищаемой информации - это юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией. Владелец защищаемой информации - это физическое или юридическое лицо, которое имеет полномочия владеть, пользоваться и распоряжаться данной

информацией по договору с собственником, в силу закона или решения административных органов.

Каждое государство защищает свои информационные ресурсы. Информационные ресурсы государства в целом можно разделить на три большие группы:

- открытая информация, на распространение и использование которой не имеется никаких ограничений;
- запатентованная информация, которая охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;
- закрытая информация, которая охраняется с помощью механизмов защиты государственной, коммерческой или другой защищаемой информации.

Понятие защищаемой информации включает в себя две категории информации - секретную и конфиденциальную. К секретной информации в настоящее время принято относить сведения, содержащие государственную тайну. К конфиденциальной информации обычно относят сведения, содержащие коммерческую, профессиональную, производственную тайну, а также тайну, касающуюся личной (неслужебной) жизни и деятельности граждан.

Применительно к органам государственной власти и управления под тайной понимается то, что скрывается от других и что известно строго определенному кругу людей. Основное направление использования этого понятия - засекречивание государством определенных сведений, сокрытие которых от соперников или потенциальных противников дает ему возможность успешно решать жизненно важные вопросы в области обороны, а также политические, экономические, научно-технические и иные проблемы с меньшими затратами сил и средств и без ущерба для государственной безопасности страны.

Защищаемая информация имеет следующие отличительные признаки:

- засекречивать информацию, то есть ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;
- чем важнее для собственника информация, тем тщательнее он ее защищает в соответствии с присвоенной ей степенью секретности;
- защищаемая информация должна иметь определенную ценность и приносить пользу ее собственнику, оправдывая затрачиваемые на ее защиту силы и средства.

Появление новой защищаемой информации есть результат деятельности субъекта - собственника информации или уполномоченных им лиц, засекретивших информацию. После создания она как бы отчуждается от субъекта-автора, самостоятельно диктуя всем, кто с нею сталкивается, правила ее использования. Уровень защиты информации определяется установленным ее автором или собственником грифом секретности или конфиденциальности.

Созданная один раз защищаемая информация (как и несекретная) может быть использована многократно в течение неограниченного времени сколь угодно большим количеством потребителей. Она обладает способностью не уничтожаться, не убывать со временем и даже возрастать по мере использования, то есть порождать новую информацию. Свойство возрастания информации создает объективные предпосылки для ее уязвимости: если кто-то позаимствовал секретные сведения без нарушения физической целостности носителя (произошла, как говорят, утечка информации), то ее собственник может об этом не узнать вообще или узнать уже из других источников информации. Секретная информация также обладает определенным генетическим свойством: созданные на ее основе сведения, документы и изделия также являются, как правило, секретными.

Существует и такая особенность, как распространение информации. Для открытой информации оно имеет случайный характер, тогда как

распространение защищаемой информации происходит детерминировано: заранее определяется возможное количество потребителей засекреченной информации, в соответствии с которым размножается определенное количество экземпляров соответствующего документа, которые и рассылаются заранее определенным адресатам.

Информация может отображаться на каких-то или в каких-то материальных объектах, которые длительное время могут сохранять ее в относительно неизменном виде или переносить ее из одного места в другое. Материальные объекты, используемые для получения, фиксации, накопления, хранения, передачи и последующего применения сведений, называются носителями информации.

Как правило, носители защищаемой информации охраняются ее собственником. Это объясняется тем, что если к ним получит доступ лицо, от которого они охраняются, то носитель может стать источником информации, из которого это лицо получит возможность незаконно добыть интересующие его сведения. В ст. 2 Закона РФ «О государственной тайне» дается определение понятия «носители сведений, составляющих государственную тайну», в соответствии с которым к этой категории относятся «материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов». Носителями защищаемой информации могут быть документы, изделия, вещества и материалы, электромагнитные, тепловые, радиационные и другие излучения, гидроакустические, сейсмические и другие поля, геометрические формы и размеры объектов и т.п.

Документ - это зафиксированная на материальном носителе ин-формация с реквизитами, позволяющими ее идентифицировать. По форме документы могут быть самыми разнообразными: бумага, кино- и фотопленка, магнитные ленты и диски, топографические карты и т.п.

Документы являются наиболее информативными носителями, так как они содержат, как правило, достоверную информацию в отработанном и сжатом виде. Особенно ценными для противника являются подписанные и утвержденные документы, что подтверждает их достоверность.

На документе, который является носителем защищаемой информации, указывается гриф секретности, по которому потребитель может определить, кому и как с этой информацией обращаться. Слабыми свойствами документа является то, что получивший доступ к нему недобросовестный потребитель может воспользоваться имеющейся там информацией в своих целях, а также скопировать, похитить, испортить или уничтожить этот документ.

Секретный документ может быть и в электронном виде, что ни в коем случае не снижает его важность как источника секретной информации.

Изделия (предметы), такие, как военная и другая техника, в том числе технические средства, материалы и вещества, негласно используемые при осуществлении оперативно-розыскной деятельности, также могут являться носителями защищаемой информации. Отходы режимных предприятий, образцы воды, воздуха, осадков, грунта и растений, взятые в непосредственной близости от них, позволяют иностранным разведкам получать информацию о характере деятельности этих предприятий. Даже при печатании на пишущей машинке остаются следы текста на копировальной бумаге, которую после использования неопытный или небдительный сотрудник бросает в корзину для бумаг, что может привести к утечке секретной информации. Для такой возможности существуют и психологические предпосылки, так как сотрудники часто не воспринимают отходы как источник секретной информации.

Электромагнитные излучения различной частоты переносят информацию от источника (радиопередатчика, излучателя) к приемнику информации. Их распространение, как правило, неконтролируемо, вследствие чего они могут быть перехвачены соответствующими устройствами. Для ознакомления с

содержанием передаваемой информации перехваченные сигналы должны быть декодированы.

В качестве носителя информации иногда рассматривают и человека, мозг которого представляет исключительно сложную систему, хранящую и перерабатывающую информацию, поступающую из внешнего мира. Свойство мозга отражать и познавать внешний мир, накапливать в своей памяти колоссальные объемы информации, в том числе и секретной, естественно, ставит человека на первое место как носителя (а точнее – источника) конфиденциальной информации. Человек обладает возможностью не только получения и хранения информации, он также способен анализировать и перерабатывать ее с целью создания новой информации.

У человека как носителя защищаемой информации могут присутствовать позитивные и негативные качества. Положительно то, что без согласия человека-секретоносителя из его памяти, как правило, никакая информация не может быть извлечена. Он может оценивать степень секретности сведений и соответственным образом обращаться с ними, знать, кому и какую информацию можно доверить.

В то же время секретоноситель может заблуждаться в отношении истинности потребителя защищаемой информации, по халатности или иным причинам утратить секретные документы, потеряв бдительность разболтать секреты своим знакомым и родственникам, из низменных побуждений совершить государственную измену (собирание, похищение, хранение в целях передачи иностранному государству сведений, составляющих государственную тайну, выдача секретных сведений врагу и т.п.).

Обычно сотрудники, допущенные к сведениям, составляющим государственную тайну, располагают объемом секретной информации, превышающим необходимый для выполнения ими служебных обязанностей. Следует иметь в виду, что в результате неформальных межличностных отношений секретная информация может поступать к посторонним лицам,

которые к сохранению «чужих» тайн относятся менее ответственно, чем к своим. Тщеславные люди часто непреднамеренно разглашают конфиденциальные сведения в публичных выступлениях и беседах, стремясь продемонстрировать свою осведомленность и заинтересовать собеседника.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания к лабораторным работам

Защита конфиденциальных данных в информационных системах

Ставрополь, 2017

Лабораторная работа №1

Тема: Программирование арифметических алгоритмов

Введение

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

1. Цель работы

Исследование и разработка основных методов симметричных криптосистем.

2. Краткие сведения из теории

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптосистемы разделяются на ***симметричные*** и *с* ***открытым ключом***.
В ***симметричных криптосистемах*** и для шифрования, и для дешифрования используется ***один и тот же ключ***.
В ***системах с открытым ключом*** используются два ключа - ***открытый*** и ***закрытый***, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений. Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования - расшифрования. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

– алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;

– алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;

– гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;

– аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа, как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Симметричные криптосистемы.

Шифры перестановки. В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Сегодня новый день” записывается в таблицу из 4 строк и 4 столбцов по столбцам.

С	Д	О	Д
Е	Н	В	Е
Г	Я	Ы	Н

О	Н	Й	Ь

Для получения шифрованного сообщения текст считывается по строкам и группируется по 4 букв: СДОД_ЕНВЕ _ГЯЫН_ОНЙЬ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово Ваза, получим следующую таблицу

В	А	З	А					А	А	В	З
3	1	4	2					1	2	3	4
С	Д	О	Д					Д	Д	С	О
Е	Н	В	Е					Н	Е	Е	В
Г	Я	Ы	Н					Я	Н	Г	Ы
О	Н	Й	Ь					Н	Ь	О	Й

До перестановки. После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: ДДСО_НЕЕВ_ЯНГЫ_НЬОЙ.

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от

длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок будет обратный. Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

Пример данного метода шифрования показан в следующих таблицах. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы:

	2	4	1	3			1	2	3	4			1	2	3	4
4	С	Е	Г	О		4	Г	С	О	Е		1	Я	Д		Н
1	Д	Н	Я	Н		1	Я	Д	Н	Н		2	Ы	О		В
2	О	В	Ы	Й		2	Ы	О	Й	В		3	Н	Д		Е
3	Д	Е	Н	Ь		3	Н	Д	Ь	Е		4	Г	С		Е

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка: ЯДННЫОЙВНДЬЕГСОЕ. В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой

диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

3. Порядок выполнения работы

На языке DELPHI, VBA C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

4. Вопросы для самопроверки

1. Цель и задачи криптографии.
2. Шифры одиночной перестановки и перестановки по ключевому слову.
3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

Дополнительно

8. ftp://ftp.kiae.su/msdos/crypto/pgp
9. http://drago.centerline.com:8080/franl/pgp/…
10. Yahoo - Computers, Security-and-Encryption

Лабораторная работа №2

Тема: Программирование алгебраических алгоритмов

Введение

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

1. Цель работы

Исследование и разработка классических методов симметричных криптосистем

2. Краткие сведения из теории

Шифры простой замены. Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены. Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i=Г(ш)_i+Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i=Г(ш)_i+Т(ш)_i$.

3. Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.
2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
8. Если не достигли конца входной строки, то перейти к шагу 4.
9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

Алгоритм дешифрации аналогичен алгоритму шифрации за исключением того, что из ASCII –кода вычитаем 256 и проверяем больше ноля или нет.

Open Filename For Input As # FileNumber –открытие файла для чтения.

Out Put –для вывода.

В ASCII –коде символы 10 и 13 (возврат каретки).

Надо открывать файлы как двоичные, ключевое слово Binary.

Line Input # FileNumber, A$ -переменная строковая.

Print –для записи.

Для чтения и записи двоичного файла объявляем переменную типа Variant.

Put # NF,, VA

Get # NF,, VA

Close –закрытие файла.

На языке VBA, C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

4. Вопросы для самопроверки

1. Шифр Гронсфельда.
2. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
3. Шифр многоалфавитной замены и алгоритм его реализации.

Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.

4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

Лабораторная работа №3

Тема: Защита от закладок при разработке программ

1. Цель работы

Исследование и анализ служебных программ Windows XP для повышения эффективности работы компьютера.

2. Краткие сведения из теории

Брандмауэр - это система безопасности, действующая как защитный барьер между сетью и внешним миром. Брандмауэр подключения к Интернету (Internet Connection Firewall, ICF) - это программное средство, используемое для настройки ограничений, регулирующих обмен данными между Интернетом и домашней или небольшой офисной сетью. Для настройки параметров сетевого подключения можно использовать мастер настройки сети. Открывая общий доступ к ресурсам компьютера, никогда не открывайте для доступа весь диск «C:» так как в каталоге Windows хранятся ваши пароли.

3. Порядок выполнения работы

Задание 1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети. Запретите доступ к ресурсам вашего компьютера из Интернета.

1. Для проверки подлинности доступа к ресурсам компьютера из локальной сети выполните следующие действия.

Откройте Панель управления, выбрав в Главном меню Windows команду **Пуск-Настройка-Панель управления.** Откройте двойным щелчком значок **Сетевые подключения** и в окне *Свойства сетевых подключений* выберите закладку **Проверка подлинности.** Включите флажки **Управлять сетевым доступом с помощью IEEE 802.1X, Проверять подлинность как у компьютера при доступности сведений о компьютере и Проверять подлинность как у гостя при отсутствии сведений о компьютере или пользователе.**

2. Чтобы включить брандмауэр подключения к Интернету, установите флажок, откройте закладку **Дополнительно** и включите флажок **«Защитить мое подключение к Интернету».** Щелкнув на кнопке «ОК», завершите настройку свойств сетевых подключений.

Задание 2. Разрешить удаленный доступ к ресурсам вашего компьютера.

1. Щелкнув правой кнопкой мыши на значке Мой компьютер, откройте окно *Свойства системы* па вкладке Удаленное использование. Включите флажок Разрешить удаленный доступ к этому компьютеру и щелкните на кнопке «ОК», чтобы закрыть окно *Свойства системы.*

2. Для разрешения общего доступа к принтеру, установленному на данном компьютере из сети, выбрав в главном меню Windows команду **Настройка - Принтеры и факсы**, откройте окно *Принтеры и факсы.* Выберите в окне нужный принтер и откройте окно свойств принтера. На вкладке Доступ щелкните ссылку «Если риск безопасности известен, но требуется разрешить общий доступ к принтеру без запуска мастера, щелкните здесь». В окне *Разрешение общего доступа к принтеру* включите вариант «Разрешить

общий доступ» и щелкните на кнопке «ОК». После этого в окне свойств принтера на вкладке Доступ включите флажок Общий доступ к данному принтеру, в поле *Сетевое имя* задайте имя принтера. Щелкнув на кнопке «Применить», примените внесенные в свойства принтера изменения, и закройте окно свойств принтера, щелкнув на кнопке «ОК». В окне *Принтеры и факсы* под значком принтера появится изображение ладони, указывающее на общий доступ к данному принтеру. Закройте окно *Принтеры и факсы.*

3. Для просмотра параметров доступа и безопасности диска или определенной папки укажите объект (диск или отдельную папку) и в контекстном меню выберите команду Общий доступ и безопасность. В окне *Свойства* откройте вкладку Доступ и включите флажок Открыть общий доступ к этой папке. Задайте имя, под которым данный ресурс будет виден пользователям сети. Если вы разрешаете пользователям сети изменять файлы в данной папке, включите флажок. Разрешить изменение файлов по сети. Щелкнув на кнопке «Применить», примените внесенные в свойства папки изменения, и закройте окно свойств, щелкнув на кнопке «ОК».

Задание 3. Использование удаленного доступа к сетевым ресурсам.

1. Для подключения к сетевому диску или папке откройте окно проводника Windows и выберите в меню Сервис команду **Подключить сетевой диск.** В окне *Подключение сетевого диска* укажите букву диска и сетевую папку, к которой необходимо подключиться. Если вам не известно точное имя папки, щелкнув на кнопке «Обзор», выберите ее в окне *Обзор папок* и щелкните на кнопке «ОК». Если подключение к данной сетевой папке нужно всякий раз восстанавливать при входе в систему, включите флажок **«Восстанавливать при входе в систему».** Щелкнув на кнопке «Готово», завершите подключение к сетевому ресурсу.

2. Для подключения к сетевому принтеру выберите в Главном меню Windows команду **Настройка - Принтеры и факсы.** В окне *Принтеры и факсы* выберите в меню **Файл** команду **Установить принтер.** В окне *Мастер*

установки принтеров выберите тип устанавливаемого принтера, включив флажок на варианте Сетевой принтер, подключенный к другому компьютеру. Щелкнув на кнопке «Далее», выберите вариант «Подключиться к принтеру», в поле *Имя* задайте имя принтера.

Щелкнув на кнопке «Готово», завершите подключение к сетевому принтеру.

Закройте окно *«Принтеры и факсы».*

Задание 4. Защита и восстановление данных на компьютере

1. Используя служебную программу **Архивация данных,** архивируйте данные из папки C:\Program Files\Microsoft Office\ Templates в архив с именем Templates на диске D:.

Для запуска приложения Архивация данных выберите в меню **Пуск** команды **Программы-Стандартные-Служебные-Архивация данных.** Если программа архивации запускается в режиме мастера, то для переключения в расширенный режим нажмите кнопку «Расширенный» в окне мастера архивации.

Для архивации выбранных файлов и папок на жестком диске перейдите на вкладку **Архивация** и установите флажок в списке Установите флажки для папки C:\Program Files\Microsoft Office\ Templates, данные из которой вы хотите заархивировать.

Задайте в качестве носителя диск D: и имя файла для архива Templates, нажмите на кнопку «Архивировать», а затем в окне *Сведения о задании архивации* выберите вариант **Затереть данные носителя этим архивом.**

Щелчком на кнопке «Архивировать» запустите процедуру архивации. После этого в окне *Ход архивации* пронаблюдайте за процессом архивации, по окончании которого будет выведено окно сообщения о завершении архивации с краткими сведениями. Для просмотра подробного текста отчета щелкните на кнопке «Отчет».

2. Используя служебную программу **Архивация данных,** создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа. Приготовьте чистую дискету емкостью 1,44 Мбайта для сохранения параметров системы, затем запустите приложение Архивация в режиме **Расширенный. В** меню **Сервис** выберите команду **Мастер** аварийного восстановления системы. Следуйте инструкциям, появляющимся на экране. Для перехода к следующему шагу мастера щелкайте на кнопке «Далее». Выбрав тип носителя для системного архива и имя носителя для хранения архивных данных, например, D:\Arxiv\Backup.bkf, щелкните на кнопке «Далее» для создания архива. После этого будет выполнена архивация системных файлов, необходимых для загрузки системы, и создание дискеты аварийного восстановления.

По окончании процесса архивации в ответ на предложение вставить дискету вставьте чистую дискету, после этого будет создана дискета аварийного восстановления. Для просмотра подробного отчета щелкните на кнопке «Отчет». Закройте окно программы **Архивация данных.**

4. Задание к работе

1. Используя программу Сведения о системе, определите следующие параметры компьютерной системы: сведения об имеющихся на компьютере портах, звуковом устройстве, о системных драйверах и автоматически загружаемых программах.

2. Используя стандартную программу Windows **Проверка диска,** проверьте диск А: на наличие поврежденных секторов и ошибок файловой системы. При этом если будут обнаружены ошибки, то задайте режим восстановления поврежденных секторов диска автоматического исправления системных ошибок.

3. Используя стандартную программу **Очистка диска, выполните очистку диск D:**

4. Используя стандартную программу **Дефрагментация диска,** выполните

оценку фрагментированности файлов на диске D: и, если требуется, то выполните дефрагментацию этого диска.

5. Используя служебную программу **Архивация данных,** архивируйте данные из папки C:\Program Files\Microsoft OfficeVTemplates в архив с именем Templates на диске D:.

6. Используя служебную программу **Архивация данных,** создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа.

5. Вопросы для самопроверки

1. Почему при эксплуатации компьютерной системы важно знать ее параметры?
2. Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы?
3. Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер обеспечения информационной безопасности?
4. Опишите причины нарушений в работе магнитных дисков.
5. Почему необходима процедура очистки диска?
6. Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска?
7. В каких случаях рекомендуется выполнить дефрагментацию диска?
8. С какой целью выполняется архивация данных компьютера?
9. Что такое дискета аварийного восстановления? Какой программой она создается?
10. Какие вы знаете программы восстановления информации на магнитных дисках?

Рекомендуемая литература

1. Гук М. Аппаратные средства IBM PC. Энциклопедия. - СПб.: Питер, 2002, - 928 с.

На страницах этой книги приведено систематизированное описание «железной» части семейства самых распространенных персональных компьютеров. Книга дает глубокие знания как по отдельным электронным подсистемам (память, процессоры, диски и т.п.), так и по их соединению в единое целое. Аппаратные средства рассматриваются во взаимодействии с программным обеспечением, что дает целостную картину функционирования компьютера.

2. Мииаси М. Модернизация и обслуживание персонального компьютера. Базовый курс. - М.; Век, 2000. - 592 с.

Лабораторная работа №4

Тема: Программирование алгоритмов криптосистем с открытом ключом

Введение

Как бы ни были сложны и надежны криптографические системы - их слабое мест при практической реализации - проблема *распределения ключей*. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены *системы с открытым ключом.*

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется *открытым*, а другой *закрытым*. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату.

1. Цель работы

Исследование и анализ основных методов ассимметричных криптосистем

2. Краткие сведения из теории

В самом определении необратимости присутствует неопределенность. Под *необратимостью* понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Схема шифрования Эль Гамаля. Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y = G^x \bmod P$.
4. Получатель выбирает целое число K, $1 < K < P-1$.
5. Шифрование сообщения (M): $a = G^K \bmod P$, $b = Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA. Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В настоящее время алгоритм RSA используется во многих стандартах, среди которых SSL, S-HHT*P*, S-MIME, S/WAN, STT и *P*CT.

Последовательность действий пользователя:

6. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $N=pq$; $M=(p-1)(q-1)$.
7. Получатель выбирает целое случайное число d, которое является взаимопростым со значением M, и вычисляет значение e из условия $ed=1 \pmod M$.
8. d и N публикуются как открытый ключ, e и M являются закрытым ключом.
9. Если S –сообщение и его длина: $1<\text{Len}(S)<N$, то зашифровать этот текст можно как $S'=S^d \pmod N$, то есть шифруется открытым ключом.
10. Получатель расшифровывает с помощью закрытого ключа: $S=S'^e \pmod N$.

Пример Зашифруем сообщение "CAB". Для простоты будем использовать маленькие числа (на практике применяются гораздо большие).

1. Выберем $p=3$ и $q=11$.

2. Определим n=3*11=33.

3. Найдем (p-1)(q-1)=20. Следовательно, в качестве d, взаимно простое с 20, например, d=3.

4. Выберем число e. В качестве такого числа может быть взято любое число, для которого удовлетворяется соотношение (e*3) (mod 20) = 1, например 7.

5. Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: A1, B2, C3. Тогда сообщение принимает вид (3,1,2). Зашифруем сообщение с помощью ключа {7,33}.

ШТ1 = (3^7) (mod 33) = 2187 (mod 33) = 9,

ШТ2 = (1^7) (mod 33) = 1 (mod 33) = 1,

ШТ3 = (2^7) (mod 33) = 128 (mod 33) = 29.

6. расшифруем полученное зашифрованное сообщение (9,1,29) на основе закрытого ключа {3,33}:

ИТ1 = (9^3) (mod 33) = 729 (mod 33) = 3,

ИТ2= (1^3) (mod 33) = 1 (mod 33) = 1,

ИТ3 = (29^3) (mod 33) = 24389 (mod 33) = 2.

Итак, в реальных системах алгоритм RSA реализуется следующим образом: каждый пользователь выбирает два больших простых числа, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d. Как результат умножения первых двух чисел (p и q) устанавливается n.

{e,n} образует открытый ключ, а *{d,n}* - закрытый (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно раскрыть с помощью открытого ключа. Владелец же закрытого ключа без труда может расшифровать принятое сообщение.

3. Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.
2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
8. Если не достигли конца входной строки, то перейти к шагу 4.
9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

4. Задание к работе

На языке VBA, C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

5. Вопросы для самопроверки

1. Алгоритм шифрации двойным квадратом. Шифр Enigma.
2. Алгоритм шифрования DES.
3. Алгоритм шифрования ГОСТ 28147-89.
4. Алгоритм шифрования RSA.
5. Алгоритм шифрования Эль Гамаля.
6. Задачи и алгоритмы электронной подписи.
7. Задачи распределения ключей.

Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

Дополнительно

8. ftp://ftp.kiae.su/msdos/crypto/pgp
9. http://drago.centerline.com:8080/franl/pgp/…

10. Yahoo - Computers, Security-and-Encryption

Лабораторная работа №5

Тема: Профилактика заражения вирусами компьютерных систем

1. Цель работы

Анализ и исследование антивирусных программ.

2. Краткие сведения из теории

Антивирус Касперского 7.0 это принципиальный новый подход к защите информации. Антивирус Касперского 7.0- это новое поколение решений по защите информации.

Основное отличие Антивируса Касперского 7.0 от существующих продуктов, в том числе и от продуктов компании ЗАО «Лаборатория Касперского», - это комплексный подход к защите информации на компьютере пользователя.

Антивирус Касперского 7.0 - это принципиально новый подход к защите информации. Главное в приложении - это объединение и заметное улучшение текущих функциональных возможностей всех продуктов компании в одно комплексное решение защиты. Приложение обеспечивает не только антивирусную защиту, но и защиту от неизвестных угроз.

Больше не нужно устанавливать несколько продуктов на компьютер, чтобы обеспечить себе полноценную защиту. Достаточно просто установить Антивирус Касперского 7.0.

Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента приложения позволяет максимально гибко адаптировать Антивирус Касперского под нужды конкретного пользователя. Предусмотрена также единая настройка всех компонентов защиты.

Вы можете работать с Антивирусом Касперского посредством командной строки. При этом предусмотрена возможность выполнения следующих операций:

- запуск, остановка, приостановка и возобновление работы компонентов приложения;
- запуск, остановка, приостановка и возобновления выполнения задач проверки на вирусы;
- получение информации о текущем статусе компонентов и задач и их статистики;
- проверка выбранных объектов;
- обновление баз и модулей приложения;
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

avp.com <команда> [параметры]

В качестве <команд> используются:

ACTIVATE	активация приложения через интернет с помощью кода активации
ADDKEY	активация приложения с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
START	запуск компонента или задачи
PAUSE	приостановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
RESUME	возобновление работы компонента или задачи
STOP	остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
STATUS	вывод на экран текущего статуса компонента или задачи
STATISTICS	вывод на экран статистики по работе компонента или задачи
HELP	помощь по синтаксису команды, вывод списка команд

SCAN	проверка объектов на присутствие вирусов
UPDATE	запуск обновления приложения
ROLLBACK	откат последнего произведенного обновления приложения (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXIT	завершение работы с приложением (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
IMPORT	импорт параметров защиты Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXPORT	экспорт параметров защиты Антивируса Касперского

Защита Антивируса Касперского строится исходя из источников угроз, то есть на каждый источник предусмотрен отдельный компонент программы, обеспечивающий его контроль и необходимые мероприятия по предотвращению вредоносного воздействия этого источника на данные пользователя. Такое построение системы защиты позволяет гибко настраивать приложение под нужны конкретного пользователя или предприятия в целом.

Антивирус Касперского включает:

- Компоненты постоянной защиты, обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации.
- Задачи поиска вирусов, посредством которых выполняется поиск вирусов в отдельных файлах, каталогах, дисках или областях, либо полная проверка компьютера.
- Обновление, обеспечивающее актуальность внутренних модулей приложения, а также баз, использующихся для поиска вредоносных программ.

- Сервисные функции, обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить его функциональность.

В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту файловой системы вашего компьютера от заражения, - Файловый Антивирус. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

Индикатором работы компонента является значок Антивируса Касперского в области уведомлений панели задач Microsoft Windows, который принимает вид каждый раз при проверке файла.

По умолчанию Файловый Антивирус проверяет только новые или измененные файлы, то есть файлы, которые добавились или изменились со времени последнего обращения к ним. Процесс проверки файла выполняется по следующему алгоритму:

1. Обращение пользователя или некоторой программы к каждому файлу перехватывается компонентом.
2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базе iChecker™ и iSwift™. На основании полученной информации принимается решение о необходимости проверки файла.

Процесс проверки включает следующие этапы:

1. Файл анализируется на присутствие вирусов. Распознавание вредоносных объектов происходит на основании баз приложения. Базы содержат описание всех известных на настоящий момент вредоносных программ, угроз, сетевых атак и способов их обезвреживания.
2. В результате анализа возможны следующие варианты поведения приложения:

a. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл и пытается его лечить. В результате успешного лечения файл становится доступным для работы, если же лечение произвести не удалось,

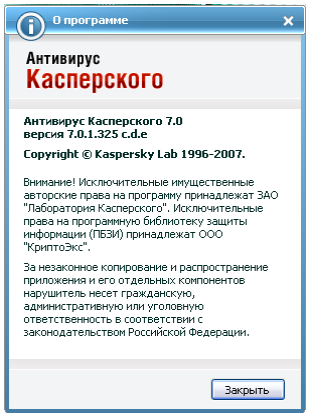
файл удаляется. При выполнении лечения файла или его удалении копия файла помещается в резервное хранилище.

b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл помещается в специальное хранилище- карантин. Позже можно попытаться вылечить его с обновленными базами.

c. Если в файле не обнаружено вредоносного кода, он сразу же становится доступным для работы.

3. Порядок выполнения работы

Задание 1.1. Ознакомьтесь с энциклопедией компьютерных вирусов на сайте лаборатории Касперского в Интернете по адресу **http:// www.viruslist.com/viruslist.asp,** для чего, загрузив web-обозреватель и указав адрес энциклопедии, изучите разделы; Что такое компьютерный вирус, классификация компьютерных вирусов. Просмотрите описание одного из самых популярных вирусов недели на сайте лаборатории Касперского. В разделе «Методы обнаружения и удаления компьютерных вирусов» изучите тему Методика использования антивирусных программ.



2. Запустите Антивирус Касперского 7.0 изучите главное окно программы.

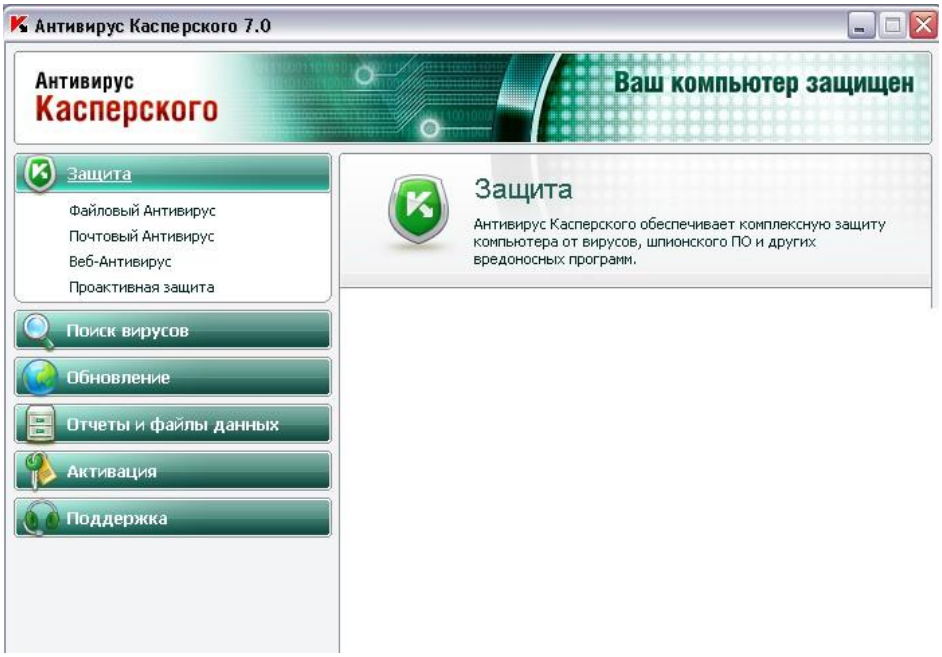


Рис. 5.1. Главное окно Антивирус Касперского 7.0

3. Одной из важных составляющих обеспечения антивирусной защиты компьютера является поиск вирусов в указанных пользователем областях. Антивирус Касперского 7.0 позволяет проверять на присутствие вирусов как отдельные объекты (файлы, папки, диски, сменные устройства), так и весь компьютер в целом. Проверка на вирусы позволяет исключить возможность распространения вредоносного кода, не обнаруженного компонентами постоянной защиты по тем или иным причинам.

В состав Антивируса Касперского 7.0 по умолчанию включены следующие задачи поиска вирусов:

Критические области

Проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные сектора дисков, системные каталоги Windows и system32. Цель задачи - быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.

Мой Компьютер

Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.

Объекты автозапуска

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

Поиск руткитов (rootkit)

Поиск на компьютере руткитов, обеспечивающих сокрытие вредоносных программ в операционной системе. Данные утилиты внедряются в систему, маскируя свое присутствие, а также наличие в системе процессов, каталогов, ключей реестра любых вредоносных программ, описанных в конфигурации руткита.

По умолчанию данные задачи выполняются с рекомендуемыми параметрами. Вы можете изменять эти параметры, а также устанавливать расписание запуска задач.

Также предусмотрена возможность создавать собственные задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых ящиков раз в неделю или задачу поиска вирусов в каталоге Мои документы.

Кроме того, вы можете проверить на вирусы любой объект (например, один из жестких дисков, на котором находятся программы и игры, почтовые базы, принесенные с работы, пришедший по почте архив и т.п.), не создавая для этого специальной задачи проверки. Выбрать объект для проверки можно из интерфейса Антивируса Касперского 7.0 или стандартными средствами операционной системы Microsoft Windows (например, в окне программы Проводник или на Рабочем столе и т.д.).

Полный список задач поиска вирусов, сформированных для вашего компьютера, можно просмотреть в разделе Поиск вирусов в левой части главного окна приложения.

Вы можете создать диск аварийного восстановления, который предназначен для восстановления системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка. Для этого воспользуйтесь ссылкой Создать диск аварийного восстановления.

4. Для проверки работоспособности Файлового Антивируса;

1. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя. Для этого установите флажок «Записывать» некритические события в разделе «Отчеты» и файлы данных окна настройки приложения.

2. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации, а также созданные вами модификации тестового «вируса».

Файловый Антивирус перехватит обращение к файлу, проверит его и уведомит вас об обнаружении опасного объекта:

Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить реакцию Файлового Антивируса при обнаружении объектов различных типов.

Полный результат работы Файлового Антивируса можно посмотреть в отчете по работе компонента.

5. Для проверки задачи Поиска вирусов;

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации, а также созданные вами модификации тестового «вируса».

2. Создайте новую задачу поиска вирусов и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов».

3. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя. Для этого установите флажок «Записывать» некритические события в разделе «Отчеты» и файлы данных окна настройки приложения.

4. Запустите задачу поиска вирусов на выполнение.

При проверке, по мере обнаружения подозрительных или зараженных объектов, на экран будут выведены уведомления с информацией об объекте и запросом дальнейшего действия у пользователя:

Таким образом, выбирая различные варианты действий, вы сможете проверить реакцию Антивируса Касперского при обнаружении объектов различных типов.

Полный результат выполнения задачи поиска вирусов можно посмотреть в отчете по работе компонента.

7. Для ознакомления с возможностями программы и управлением ею выберите в меню **Справка** команду **Содержание.** В окне *Справочная система: Kaspersky Anti-Virus Scanner* изучите раздел **Работа с антивирусным сканером,** темы **Интерфейс программы, Настройка параметров сканирования, Поиск и удаление вирусов, Запуск программы обновления антивирусных баз.** После изучения справочной информации закройте окно справки.

8. Для просмотра сведений о вирусах в Интерактивной вирусной энциклопедии щелкните на задаче View Online Virus Encyclopedia. После этого откроется web-страница онлайн-энциклопедии вирусов на сайте компания Symantec (http://securityresponse.Symantec.com/avcenter/virfodb.html?prodid = nav2007). На этой странице можно просмотреть, чем заражен тот или иной файл и как удалить этот вирус.

9. Для просмотра протокола работы программы щелкните на задаче View Activity log. После этого откроется протокол работы программы по трем параметрам - обнаруженные вирусные угрозы, сканирование и ошибки.

Задание 2. Изучить дополнительные возможности программы Norton AntiVirus по защите данных (восстановление ошибочно удаленных файлов и гарантированного удаления файлов и папок).

Для защиты данных Norton AntiVirus имеет UnEraze Wizard (мастер восстановления ошибочно уничтоженных файлов) и Wipe Info (инструмент

для гарантированного удаления файлов). Вызвав мастера UnEraze Wizard, достаточно указать имя (или часть) файла, его расширение и место расположения на дисках компьютера. После поиска UnEraze Wizard покажет все найденные по предложенным критериям файлы и предложит выбрать, какой из них подлежит восстановлению.

Если вам часто приходится удалять файлы, и хочется иметь гарантию невозможности их восстановления, то поможет инструмент Wipe Info. Но рекомендуется в настройках Wipe Info установить защиту от удаления системных файлов, чтобы после необдуманного действия не столкнуться с отказом операционной системы от загрузки.

1. Для восстановления ошибочно уничтоженных файлов щелкните в главном окне на «кнопке Advanced Tools». Затем в окне *Advanced Tools* выберите вариант UnErase Wizard и щелкните на кнопке «Start Tool». На следующем шаге мастера восстановления выберите вариант поиска удаленных файлов, включите флаг **Find Norton Protected Users files** (Поиск всех защищенных файлов) и щелкните на кнопке «Далее». После этого будет выполнен поиск выбранной вами категории файлов. На следующем шаге мастера восстановления, указав восстанавливаемые файлы, щелкните на кнопке «Recover» (Восстановить). Щелчком на кнопке «Далее» перейти к сообщению о результатах восстановления. Просмотрев сообщение и щелкнув на кнопке «Готово», завершите работу мастера восстановления.

2. Для гарантированного удаления файлов выберите в окне *Advanced Tools* вариант Wipe Info и щелкните на кнопке «Start Tool». На следующем шаге мастера удаления перетащите в окно *Wipe Info* файлы и папки, которые требуется гарантированно удалить. После этого щелкните на кнопке «Wipe All» (Удалить все).

4. Задание к работе

1. Используя пакет программ, демонстрирующих действие вирусов, изучите действие вирусов различного типа. Поочередно запуская программы из пакета демонстрационных программ, изучите проявление вирусного

заражения. По окончании наблюдения перезагрузить компьютер.

2. Запустите программу DrWeb и выполните проверку оперативной памяти компьютера на наличие вирусов. Выполните тестирование дисков A; и C: на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.

3. Загрузите из Интернета и установите на компьютере ознакомительную версию ADinf32. Задайте расписание работы ADinf, чтобы ее активизация осуществлялась еженедельно по субботам с 18.00.

4. Загрузите из Интернета и установите на компьютере ознакомительную версию антивируса Kaspersky Anti-Virus. Создайте новую задачу сканирования дисков компьютера на вирусы.

5. Загрузите из Интернета и установите на компьютере ознакомительную версию антивируса Norton AntiVirus. Выполните обновление антивирусной базы и проверьте компьютер на наличие вирусов.

6. Посетите web-страницу http://www.sarc.eom//avcenter/vinfodb. html онлайн-экспедиции вирусов на сайте компания Symantec. На этой странице можно просмотреть, чем заражен тот или иной файл и как удалить этот вирус.

5. Вопросы для самопроверки

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?

2. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.

3. Какие вирусы называются резидентными и в чем особенность таких вирусов?

4. Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ?

5. Опишите схему функционирования загрузочного вируса.

6. Опишите схему функционирования файлового вируса.

7. Опишите схему функционирования загрузочно-файловых вирусов.

8. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?

9. Каковы причины появления компьютерных вирусов. Приведите примеры широко известных вирусов.

10. Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?

11. Каковы пути проникновения вирусов в компьютер и признаки заражения компьютера вирусом?

99763008. Каковы способы обнаружения вирусов и антивирусной профилактики?

99763009. Перечислите основные меры по защите от компьютерных вирусов.

99763010. Опишите назначение антивирусных программ различных типов.

15. Назовите примеры современных антивирусных программ и опишите их особенности.

Рекомендуемая литература

1. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. - М.:СОЛОН-Р, 2001. - 461 с.

В энциклопедии собрана исчерпывающая информация по проблеме компьютерных вирусов, от создания до обнаружения и уничтожения. Приведены примеры написания и уничтожения COM-,EXE-,Boot-, Internet- и макровирусов, как нерезидентных, так резидентных и полиморфных. Основное преимущество данной книги в ее практическом применении.

2. **http://www.avp.ru** - сервер антивирусной лаборатории Евгения Касперског 6.0, на котором имеется возможность бесплатно и быстро проверить файлы на наличие вирусного кода. В разделе «Триальные версии» вы можете познакомиться с антивирусными продуктами Лаборатории Касперского перед приобретением.

3. **http://www.viruslist.com/virusHst.asp** - раздел сервера антивирусной лаборатории Евгения Касперского, содержащий огромное число описаний вирусов и демонстраций вызываемых вирусами эффектов, классификацию вирусов, общие методы обнаружения и удаления компьютерных вирусов.

4. **http://www.dials.ru** - сервер антивирусной лаборатории «ЛабораторияДанилова» и «ДиалогНаука». На данном сервере вы можете:найти информацию о программах сканер Doctor Web; резидентный сторож SpIDer Guard; ревизор дисков ADinf и универсальный лекарь ADinf Cure Module, выполнить через Интернет бесплатно удаленную проверку ваших файлов на наличие вирусов с помощью последней версии антивирусного сканера Doctor Web, а также получить некоммерческие версии антивирусных продуктов, дополнения для программы Doctor Web и документацию.

5. **http://www.adinf.ru** - WEB-сайт разработчиков антивируса ADinf.

6. **http://www.symantec.ru** - Российское Интернет-представительство компании Symantec, производящей антивирусный пакет Norton Anti Virus.