ИНСТИТУТ СОЦИАЛЬНЫХ И ГУМАНИТАРНЫХ ЗНАНИЙ

И.О. Антонов

ЗАЩИТА ИНФОРМАЦИИ

Казань
2010

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ РФ
ИНСТИТУТ СОЦИАЛЬНЫХ И ГУМАНИТАРНЫХ ЗНАНИЙ
КАФЕДРА УГОЛОВНОГО ПРАВА И ПРОЦЕССА

И.О. Антонов

ЗАЩИТА ИНФОРМАЦИИ

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Казань
2010

УДК
ББК
А

Рекомендовано к изданию учебно-методическим советом
Института социальных и гуманитарных знаний

Рецензенты:
Кафедра национальной экономики и права Казанского государственного технического университета им. А.Н. Туполева;
Ю.И. Селивановская – к.ю.н., доцент кафедры уголовного права и процесса НОУ «Институт социальных и гуманитарных знаний»

Антонов И.О.
А Защита информации: Учебно-методический комплекс / И.О. Антонов. – Казань: РИЦ «Школа», 2010. – с.
ISBN

Учебно-методический комплекс составлен в соответствии с требованиями государственного образовательного стандарта высшего профессионального образования по специальности 021100 «Юриспруденция». Дисциплина входит в блок специальных дисциплин и является обязательной для изучения.

Предназначен для студентов и преподавателей юридических факультетов высших учебных заведений.

УДК
ББК

ISBN

СОДЕРЖАНИЕ

Введение.....
Объем дисциплины и виды учебной работы.....
Тематический план занятий.....
Рабочая программа учебной дисциплины.....
Краткий курс лекций.....
Самостоятельная работа студентов.....
Контроль знаний студентов.....
Литература.....

ВВЕДЕНИЕ

Цели и задачи дисциплины

В процессе изучения курса «Защита информации» у будущих юристов должно сформироваться представление о современных формах, методах, способах и средствах, используемых в деятельности по защите информации.

Преподавание дисциплины «Защита информации» студентам юридического факультета предполагает достижение следующих целей:

1) формирование основных представлений о современных возможностях организации защиты информации и, прежде всего, правовых возможностях;

2) раскрытие структуры и содержания дисциплины, ее базовых категорий, принципов и методов.

Освоение студентами дисциплины позволяет решить следующие задачи:

а) формирование адекватных представлений о роли информации, информационных ресурсов, информационных систем в жизни современного общества и о значимости их эффективной защиты для обеспечения безопасности человека, гражданина, общества и государства;

б) формирование у будущих юристов базовых знаний, умений и навыков в создании оптимальной системы защиты ценной информации.

Требования к уровню освоения содержания дисциплины

Студенты, завершившие изучение данного курса, должны:

– знать основные и производные понятия дисциплины «Защита информации»;

– уметь логично, последовательно, аргументированно отвечать на вопросы в объеме тематического содержания курса;

– ознакомиться с правовыми актами, регламентирующими деятельность по защите информации;

– выработать навыки самостоятельного решения правовых, организационных, инженерно-технических, программно-аппаратных и иных задач в практической деятельности по защите информации.

ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Объем часов по формам обучения	
	Очная	Заочная
№ семестров	3	7
Всего часов по дисциплине	40	40
Лекции	18	8
Практические и семинарские занятия	–	–
Самостоятельная работа	22	32
Форма контроля	Зачет	Зачет

ТЕМАТИЧЕСКИЙ ПЛАН ЗАНЯТИЙ

Дневная форма обучения

№ п/п	Название темы	Объем часов		
		Лекции	Семинары и практические занятия	Самост. работа
1	Предмет, основные понятия и система дисциплины «Защита информации»	2	–	3
2	Принципы защиты информации	2	–	3
3	Правовое регулирование зашиты информации в Российской Федерации	2	–	3
4	Субъекты защиты информации	2	–	3
5	Общая характеристика угроз информационной безопасности	2	–	3
6	Административно-организационный аспект защиты информации	4	–	3
7	Базовые положения инженерно-технической и программно-аппаратной защиты информации	4	–	4
ИТОГО		18	–	22
Итоговый контроль		Зачет		

Заочная форма обучения

№	Название темы	Объем часов		
		Лекции	Семинары и практ. занятия	Самост. работа
1	Предмет, основные понятия и система дисциплины «Защита информации»	1	–	4
2	Принципы защиты информации	1	–	5
3	Правовое регулирование зашиты информации в Российской Федерации	2	–	5
4	Субъекты защиты информации	1	–	5
5	Общая характеристика угроз информационной безопасности	1	–	5
6	Административно-организационный аспект защиты информации	1	–	4
7	Базовые положения инженерно-технической и программно-аппаратной защиты информации	1	–	4
ИТОГО		**8**	**–**	**32**
Итоговый контроль		**Зачет**		

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Предмет, основные понятия и система дисциплины «Защита информации»

Предмет и задачи дисциплины. Понятие информации, информационных ресурсов и информационных систем. Свойства информации. Информационная безопасность. Угрозы информационной безопасности.

Соотношение предмета дисциплины с другими учебными курсами. Соотношение с правовыми дисциплинами. Защита информации и информационное право. Соотношение с общей теорией безопасности. Соотношение с информатикой.

Система курса. Общие положения дисциплины. Правовой, административно-организационный, инженерно-технический и программно-аппаратный аспекты защиты информации.

Тема 2. Принципы защиты информации

Понятие принципа защиты информации. Система принципов защиты информации. Принцип законности. Принцип уважения прав и свобод человека и гражданина. Принцип соблюдение баланса интересов человека, общества и государства. Принципы комплексности, своевременности и непрерывности. Принцип эшелонирования. Принцип надежности (равнопрочности). Принципы обоснованности и специализация. Принцип взаимодействия и координации. Принцип совершенствования. Принцип соответствия уровня защиты степени ценности информации. Принцип экономической целесообразности. Принцип персональной ответственности.

Тема 3. Правовое регулирование зашиты информации в Российской Федерации

Информационное право как основа деятельности по защите информации. Методы и принципы информационного права.

Предмет правового регулирования. Государственный уровень правового регулирования деятельности по защите информации. Значение Конституции РФ и федеральных законов. Федеральный закон «Об информации, информационных технологиях и защите информации». Указы Президента РФ. Нормативные акты Правительства РФ в сфере защиты информации. Ведомственные нормативные акты. Правовое регулирование защиты государственной тайны.

Локальный уровень правового регулирования. Правовое регулирование защиты служебной, коммерческой и банковской тайны.

Тема 4. Субъекты защиты информации

Понятие субъектов защиты информации, их функции и классификации. Субъект защиты информации как лицо, обладающее правами и

обязанностями по защите информации. Комплекс прав и обязанностей субъектов защиты информации. Права и обязанности собственника, владельца и пользователя информационных ресурсов. Российская Федерация, субъекты РФ, государственные органы и должностные лица государственных органов как субъекты защиты информации. Юридические и физические лица как обладатели прав и обязанностей по защите информации.

Тема 5. Общая характеристика угроз информационной безопасности

Понятие и классификации угроз информационной безопасности. Источники угроз информационной безопасности. Информационные, программно-математические, физические и радиоэлектронные угрозы. Угрозы конфиденциальности данных и программ. Угрозы целостности данных, программ, аппаратуры. Угрозы доступности данных. Угрозы отказа от выполнения трансакции.

Тема 6. Административно-организационный аспект защиты информации

Программно-целевой метод в деятельности по защите информации. Концепция защиты информации. Концепция защиты информации OPSEC. Программа по защите информации.

Организационные мероприятия программы. Подбор персонала. Психологические методики отбора. Биографический метод. Организация и поддержание пропускного режима. Контроль за работой персонала. Увольнение сотрудников. Служебное расследование по факту потери контроля за ценной информации.

Основные операционные технологические схемы обработки конфиденциальных документов.

Тема 7. Базовые положения инженерно-технической и программно-аппаратной защиты информации

Понятие инженерно-технической и программно-аппаратной защиты информации. Системы контроля и управления доступом. Физические средства защиты. Инженерные сооружения.

Основные сервисы безопасности. Идентификация и аутентификация. Протоколирование и аудит.

Шифрование. Криптография. Методы шифрования. Симметричный и асимметричный методы шифрования. Контроль целостности. Экранирование.

Стеганография.

Анализ защищенности. Сканеры защищенности. Сетевые сканеры. Антивирусная защита. Обеспечение отказоустойчивости. Обеспечение безопасного восстановления.

КРАТКИЙ КУРС ЛЕКЦИЙ[1]

Тема 1. Предмет, основные понятия и система дисциплины «Защита информации»

1. Понятие информации, информационных ресурсов и информационных систем

При изучении курса «Защита информации» необходимо иметь представление о базовых категориях дисциплины.

Информация – сведения (сообщения, данные) независимо от формы их представления. Помимо данного официального определения (ФЗ РФ «Об информации, информационных технологиях и защите информации»), существует великое множество других определений, в которых предприняты попытки определить сущность такой категории, как информация. Например, «информация – это мера сложности объекта» (А. Колмогоров).

Информация обладает следующими свойствами:

– ценность;
– достоверность;
– своевременность;
– защищенность;
– общественная природа;
– языковая природа;
– неотрывность от языка и носителя;
– дискретность;
– независимость от создателя;
– старения;
– рассеивания.

---

[1] В основе краткого конспекта лекций работы: Бачило И.Л. Информационное право: учебник для вузов. М.: Юрайт-Издат, Высш. обр., 2009; Галатенко В.А. Основы информационной безопасности / под ред. В.Б. Бетелина. М.: Интернет-Университет информационных технологий, 2003; Грень И.В. Компьютерная преступность. Минск: Новое знание, 2007; Джеймс Л. Фишинг. Техника компьютерных преступлений / пер. с англ. Р.В. Гладицкого. М.: НТ Пресс, 2008; Информационное право: учебник / Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. – М.: Норма: ИНФРА-М, 2010; Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учеб. пособие. М.: ФОРУМ, 2009; Копылов В.А. Информационное право. – М.: Юристъ, 2002; Корнеев И.К., Степанов Е.А. Защита информации в офисе: учебник. М.: Проспект, 2009; Куприянов А.И**.** Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. М.: Академия, 2006; Правовое обеспечение информационной безопасности: учебник / под общ. ред. В.А. Минаева, А.П. Фисуна, С.В. Скрыля, С.В. Дворянкина, М.М. Никитина, Н.С. Хохлова. М.: Маросейка, 2008; Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009; Донцов Д. Как защитить компьютер от ошибок, вирусов, хакеров. СПб.: Питер, 2008; Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов / под ред. В.Н. Черкасова. Саратов: СЮИ МВД России, 2006.

Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если законодательством не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Доступ к информации – возможность получения информации и ее использования.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

2. Понятие защиты информации

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

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

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

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

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

2) своевременное обнаружение фактов несанкционированного доступа к информации;

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

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

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

6) постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Безопасность информации – это проведение единой политики защитных мероприятий, а также система мер правового, организационного, инженерно-технического и программно-аппаратного характера.

3. Предмет и задачи дисциплины «Защита информации»

Дисциплина «Защита информации» является комплексной. Она призвана исследовать закономерности, явления, отношения, возникающие и развивающиеся в сфере правомерного ограничения доступа к ценной информации, обеспечения ее безопасности от вредоносных воздействий.

Задачи курса «Защита информации»:

1. Научная разработка структурных элементов курса.

2. Разработка практических рекомендаций по защите информации на основе теоретических изысканий.

3. Адаптация, приспособление достижений других наук для решения задач по защите информации.

4. Изучение зарубежного опыта и использование его в РФ для решения задач по эффективной защите информации.

Предмет курса «Защита информации» тесно связан с общей теорией безопасности, юридическими науками, информатикой, наукой управления, физикой, математикой, техническими дисциплинами и др.

Тема 2. Принципы защиты информации

1. Понятие принципа защиты информации

Принципом деятельности по защите информации можно назвать основополагающую идею, руководящее начало, в котором отражается сущность деятельности по защите информации.

Соблюдение принципов защиты информации позволяет достигать значимых результатов в деятельности с наименьшими затратами ресурсов и с наибольшей эффективностью.

Определяющими для принципов деятельности по защите ценной информации являются принципы правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

2. Система принципов защиты информации

Системный подход к построению системы защиты информации, означающий оптимальное сочетание взаимосвязанных организационных, программных, аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

К принципам деятельности по защите информации можно отнести:

– принцип законности (соблюдение норм международного права, Конституции РФ и законодательства РФ при осуществлении деятельности по обеспечению информационной безопасности);

– принцип недопущения ограничений прав и свобод граждан, за исключением случаев, прямо предусмотренных законом (уважения прав и свобод человека);

– принцип сбалансированности (соблюдение баланса интересов субъектов, их взаимная ответственность);

– принцип системности;

– принцип открытости;

– принцип реальности выдвигаемых задач (с учетом имеющихся ресурсов);

– принцип сочетания централизованного управления силами и средствами обеспечения безопасности с делегированием части полномочий;

– принцип непрерывного развития системы (способы реализации угроз информации в ИС непрерывно совершенствуются, а потому обеспечение безопасности ИС не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования СИБ, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа);

– принцип специализации (привлечение для защиты специализированных организаций и профессионально подготовленных специалистов);

– принцип многозональности средств защиты;

– принцип надежности (равнопрочности);

– принцип соответствия уровня защиты степени ценности информации.

Зарубежный и отечественный опыт показывает, что для обеспечения выполнения столь многогранных требований безопасности система защиты информации должна удовлетворять определенным принципиальным условиям:

1) охватывать весь технологический комплекс информационной деятельности;

2) быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;

3) быть открытой для изменения и дополнения мер обеспечения

безопасности информации;

4) быть нестандартной, разнообразной: при выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей;

5) быть простой для технического обслуживания и удобной для эксплуатации пользователями;

6) быть надежной: любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;

7) быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы.

Тема 3. Правовое регулирование зашиты информации в Российской Федерации

1. Информационное право как основа деятельности по защите информации

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации.

Информационные правоотношения – это отношения, возникающие по поводу сбора, обработки, накопления, хранения, поиска, распространения, использования информации, информационных ресурсов и регулируемые нормами информационного законодательства (информационным правом).

Указанные отношения возникают при осуществлении информационных процессов, в том числе и при осуществлении защиты информации.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

При создании правовой основы деятельности по защите информации 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 должны затрагивать все уровни законодательства России. Например, конституционно должны быть закреплены и оформлены права граждан, организаций, государства на информацию и последовательно обеспечены во всех законах – о собственности, правах граждан, гражданстве, предпринимательстве и т.д.

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

Нормативные правовые акты в области защиты информации 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 систем защиты информации и систем ее обработки, установление гарантий и т.д. Кроме федерального законодательства вопросы информатизации должны быть учтены в законодательстве субъектов РФ.

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

Обязательной составной частью рассматриваемой структуры системы законодательства является правоохранительное законодательство, включающее нормы об ответственности за правонарушение при работе с информацией.

2. Государственный уровень правового регулирования деятельности по защите информации

Деятельность по защите информации на государственном уровне правового регулирования рассматривается в правовом аспекте через установление и раскрытие сущности института «тайны» (государственной, служебной, коммерческой, банковской, персональных данных и т.д.).

Тайна – это сфера объективной реальности, скрытая от нашего восприятия либо понимания. Все то, что на данный момент не осознано человеческим интеллектом, или нечто уже известное, но с определенной целью скрытое от других людей, – тайна.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Служебная тайна – информация ограниченного распространения, несекретная, касающаяся деятельности организации, ограничения на распространение которой диктуются служебной необходимостью.

Таким образом, к служебной тайне, за исключением информации, составляющей государственную тайну, относится информация о деятельности государственных органов и должностных лиц, представляющая не коммерческий, а государственный интерес, а также иная конфиденциальная информация, составляющая частную, коммерческую тайну организаций, полученная государственным органом в пределах своей компетенции для выполнения возложенных на него функций.

Следовательно, информация может быть отнесена к служебной тайне, если она отвечает следующим требованиям:

1. Отнесена федеральным законом к служебной информации.
2. О деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости.
3. Является конфиденциальной информацией другого субъекта (коммерческая тайна, банковская тайна, тайна частной жизни и т.п.).
4. Не является государственной тайной и не подпадает под перечень информации, составляющей государственную тайну.
5. Получена представителем государственного органа или органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и в порядке, установленных федеральным законодательством, и имеет действительную ценность в силу неизвестности ее третьим лицам.

Коммерческая тайна – конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну, – это научно-техническая, технологическая, производственная, финансово-экономическая

или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критериям правовой охраны):

– не попадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;

– к ней нет свободного доступа на законном основании;

– обладатель информации принимает определенные меры к ее охране.

Профессиональная тайна – это охраняемая законом конфиденциальная информация, доверенная или ставшая известной лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которой может повлечь за собой вред правам и законным интересам другого лица, доверившего эту информацию, и предоставляет ему право на защиту в соответствии с законодательством Российской Федерации.

Существует несколько обобщающих признаков профессиональной тайны.

Первым признаком, при котором информация относится к конкретному виду тайны, выступает профессия, в силу которой лицу доверяется или становится известной конфиденциальная информация.

Второй признак – конфиденциальная информация доверяется лицу, исполняющему профессиональные обязанности, добровольно по выбору владельца этой информации и, как правило, затрагивает частную жизнь последнего.

Третий признак – лицо, которому в силу его профессии была доверена информация, обязано по закону обеспечить ее сохранность как профессиональной тайны под страхом наступления ответственности в соответствии с действующим законодательством.

Профессиональная тайна имеет некоторые особенности, которые можно разделить не два вида:

– профессиональная тайна в чистом виде, обусловленная характером деятельности;

– профессиональная тайна, составную часть которой образуют доверенные личные тайны граждан (адвокатская, врачебная, банковская, нотариальная, усыновления, журналистского расследования, представительства и т.п.).

Сведениями конфиденциального характера являются:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных разговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

3. Локальный уровень правового регулирования

Обеспечение выполнения установленных правовых норм осуществляется путем такой регламентации производственной деятельности объекта защиты информации и его работников, которая позволяет, обязывает или заставляет на нормативно-правовой основе выполнять требования по защите информации. С этой целью правовые нормы защиты информации закладываются в нормативные документы объекта защиты информации, которые регулируют организацию и технологию выполнения работ, взаимоотношения служащих, условия приема и увольнение сотрудников, правила трудового распорядка и др.

При этом решение вопросов защиты информации обеспечивается либо установленной технологией выполнения работ, исключающей утрату носителей информации и несанкционированного доступа к информации или к ее носителям, либо путем введения прямых правил, регулирующих организацию защиты информации.

Например, основные мероприятия по организации правомерного доступа сотрудников к сведениям, составляющим коммерческую тайну, как правило, излагаются в виде раздела положения о коммерческой тайне объекта защиты информации. Однако в случае необходимости может быть разработана специальная инструкция, детализирующая процедуру доступа.

Оба документа могут составляться с различной степенью детализации, зависящей от специфики деятельности организации, однако ряд положений, отражающих права и обязанности сторон, возникающие в связи с допуском к конфиденциальной информации, должен быть включен в нее непременно.

В них устанавливается механизм реализации норм конституционного права, гражданского, трудового и иного законодательства в процессе защиты конфиденциальной информации.

Они учитываются сторонами при заключении трудовых договоров и контрактов. Их нарушение может служить основанием для наложения дисциплинарных взысканий на работника администрацией организации либо

предъявления судебных исков одной из сторон.

В частности, инструкция должна содержать указания на то, что допуск граждан к конфиденциальной информации осуществляется в добровольном порядке и предусматривает:

– принятие на себя обязательств о нераспространении доверенных им сведений, составляющих конфиденциальность информации;

– согласие на частичные временные ограничения их прав в соответствии с условиями трудового договора;

– письменное согласие на проведение в отношении них проверочных мероприятий соответствующими службами организации либо иной частной коммерческой службой по договору с организацией (выявление биографических и других характеризующих личность данных в пределах, установленных ст. 3 Закона РФ «О частной детективной и охранной деятельности в Российской Федерации»);

– обязательство гражданина представлять кадровому аппарату сведения о возникновении оснований для отказа к допуску к конфиденциальной информации;

– определение видов, размеров и порядка предоставления льгот в качестве компенсации за исполнение указанных выше обязательств и ограничения прав (взаимные обязательства организации и лица, получающего допуск, фиксируются в трудовом договоре).

Инструкция должна содержать исчерпывающий перечень оснований для отказа гражданину в допуске к конфиденциальной информации:

– признание его судом недееспособным, ограниченно дееспособным, нахождение его под судом и следствием за тяжкие и особо тяжкие преступления, наличие у него неснятой судимости за преступления;

– наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих конфиденциальную информацию;

– выявление в результате проверочных мероприятий таких данных, которые свидетельствуют о деятельности оформляемого лица или обстоятельствах, создающих угрозу разглашения сведений, составляющих конфиденциальную информацию;

– уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Тема 4. Субъекты защиты информации

1. Понятие субъекта защиты информации

Субъект защиты информации – это лицо, которое обладает комплексом прав и обязанностей в сфере правомерной защиты ценной информации.

Данный комплекс прав и обязанностей обусловлен установленным Федеральным законом РФ «Об информации, информационных технологиях и защите информации» статусом «обладатель информации» (лицо, самостоятельно создавшее информацию либо получившее на основании

закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам).

Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

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

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

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Полномочия по защите информации ограничиваются целым рядом институтов, среди которых особое место занимает «общедоступная информация».

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

2. Виды субъектов защиты информации и их правомочия

Среди субъектов защиты информации выделяют физических лиц и юридических лиц, государственные органы и органы местного самоуправления.

Физические лица и юридические лица вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

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

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

Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

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

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

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

Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

В случае если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

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

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

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

Тема 5. Общая характеристика угроз информационной безопасности

1. Понятие угроз информационной безопасности

Под угрозой безопасности конфиденциальной информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. К существующим относятся угрозы, реализация которых наносит ущерб объекту защиты и которые могут быть в принципе реализованы.

Угрозы безопасности конфиденциальной информации целесообразно разделять по фактору возникновения, виду нарушения, объекту воздействия, виду деструктивного действия, способу реализации.

Для конфиденциальной информации опасность представляют угрозы ее утечки по техническим каналам, угрозы, связанные с несанкционированным доступом, и угрозы «заражения» компьютерными вирусами.

Обеспечение информационной безопасности достигается системой мер, направленных на:

– предупреждение угроз. Предупреждение угроз – это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

– выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

– обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;

– локализацию последствий и принятие мер по ликвидации угрозы или конкретных преступных действий;

– ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными методами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты: физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения и добывания информации о готовящихся противоправных актах.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность.

Выявление угроз имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции. Особое внимание в этом виде деятельности должно отводиться изучению собственных сотрудников. Среди них могут быть и недовольные, и неопытные, и «внедренные».

Обнаружение угроз – это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированно го доступа к источникам коммерческих секретов.

Пресечение или локализация угроз – это действия, направленные на устранение действующей угрозы и конкретных преступных действий.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного от подрыва здания, и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

– предотвращение разглашения и утечки конфиденциальной информации;

– воспрещение несанкционированного доступа к источникам конфиденциальной информации;

– сохранение целостности, полноты и доступности информации;

– соблюдение конфиденциальности информации;

– обеспечение авторских прав.

Защита от разглашения сводится в общем плане к разработке перечня сведений, составляющих коммерческую тайну предприятия. Эти сведения должны быть доведены до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять коммерческую тайну. Одним из важных мероприятий является система контроля за сохранностью коммерческих секретов.

2. Виды угроз информационной безопасности

Основными угрозами информационной безопасности являются ее разглашение, утечка и несанкционированный доступ к источникам информации. Каждому из условий неправомерного овладения конфиденциальной информацией можно поставить в соответствие

определенные каналы, определенные способы защитных действий и определенные классы средств защиты или противодействия.

Все множество потенциальных угроз информационной безопасности по природе их возникновения можно разделить на две пары классов:

– естественные угрозы – угрозы, вызванные воздействиями на систему, ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека;

– искусственные угрозы – угрозы, вызванные деятельностью человека;

– преднамеренные – в случае, если они связаны с корыстными устремлениями людей;

– непреднамеренные – в случае, если они вызваны ошибками в действиях персонала, проектировании системы, ее элементов, ошибками в программном обеспечении.

Угрозы подразделяются информационной безопасности на:

– пассивные угрозы, которые направлены в основном на несанкционированное использование информационных ресурсов АИС, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.;

– активные угрозы имеют целью нарушение нормального функционирования АИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, искажение сведений в базе данных, разрушение программного обеспечения компьютеров, нарушение работы линий связи и т.д. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Умышленные угрозы подразделяются на внутренние и внешние:

– внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом;

– внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями).

Естественно предположить, что каждому виду угроз присущи свои специфические способы, силы и средства.

Тема 6. Административно-организационный аспект защиты информации

1. Сущность организационной защиты конфиденциальной информации

Сущностью организационной защиты информации является необходимость в проведении мероприятий по защите информации, которая является составной частью деятельности предприятий, организаций и учреждений и осуществляется во взаимодействии с другими мерами по защите конфиденциальной информации, составляющей определенный вид тайны.

В способы защиты информации входит комплекс организационных, организационно-технических, административно-правовых, воспитательных и других проводимых органами защиты мер по надежному закрытию каналов утечки секретных сведений.

Организационные мероприятия – это мероприятия ограничительного характера, сводящиеся в основном к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самого субъекта защиты информации путем использования простейших организационных мер

2. Методы и формы организационной защиты конфиденциальной информации

Методами организационной защиты информации являются:

1) При необходимости обеспечения режима секретности:

• ограничение доступа личного состава на режимные объекты и их элементы, а также к работам и служебным документам ограниченного доступа;

• обеспечение сохранности носителей информации, содержащих сведения, составляющие тайну, путем введения определенных норм и правил, регламентирующих порядок их хранения и обращения с ними;

• обучение работников учреждений и организаций по вопросам защиты тайны и соблюдения ими указанных норм и правил.

2) При организации противодействия техническим средствам:

• скрытие работы технических средств;

• защита информации при использовании технических средств передачи информации.

3) При организации скрытого управления:

• организация защиты (закрытие) информации, циркулирующей в системе управления;

• обучение работников учреждений и организаций по вопросам защиты тайны и соблюдение ими норм и правил, регламентирующих порядок пользования средствами связи, а также хранения секретных носителей информации и обращения с ними.

4) При использовании работ по обеспечению безопасности информации:

• проведение комплекса мероприятий и применение специальных средств по защите от несанкционированного доступа;

• специальная защита информации от технических средств разведки.

Формами организационной защиты информации могут являться:

1. Издание приказов руководителя организации и учреждения о порядке защиты от утечки информации и сведений ограниченного распространения.

2. Принятие обязательств сотрудников организаций и учреждений о защите служебной информации.

3. Ознакомление с обязательствами сотрудников организаций и

учреждений, допущенных к информации ограниченного распространения.

4. Разработка должностной инструкции сотрудников организаций и учреждений, с ограничением прав и обязанностей с персональной ответственностью.

5. Определение тематики работ, по которым составляются договора, подлежащие согласованию со службой безопасности или отделом (группой) по защите информации.

6. Соответствие помещений, предназначенных для ведения работ, установленным правилам.

7. Порядок хранения документов, содержащих закрытую информацию.

8. Порядок хранения ключей.

9. Порядок охраны офиса или здания в целом.

10. Ведение дел и журналов, их регистрация и учет.

11. Ведение карточек, пропусков на сотрудников.

12. Учет магнитных носителей информации, печатей, штампов.

13. Порядок учета входящей и исходящей информации, документов.

14. Порядок уничтожения документов, содержащих служебную информацию.

3. Программно-целевой метод в деятельности по защите информации

Программно-целевой метод в деятельности по защите информации является единственным, способным обеспечить необходимую эффективность данного вида деятельности.

В общем плане организационные мероприятия предусматривают проведение следующих действий:

– определение границ охраняемой зоны (территории);

– определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;

– определение «опасных», с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений;

– выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников;

– реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому распространению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам:

– технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, и др.;

– технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Таким образом, процесс организации защиты конфиденциальной информации можно представить в виде следующих этапов (концепция защиты информации OPSEC):

Первый этап: анализ объекта защиты.

Определение того, что необходимо защищать. На этом этапе проводится анализ по следующим направлениям:

• какая информация нуждается в защите;

• наиболее важные (критические) элементы защищаемой информации;

• определяется срок жизни критической информации (время, необходимое конкуренту для реализации полученной информации);

• определяются ключевые элементы информации (индикаторы), отражающие характер охраняемой информации;

• классифицируются индикаторы по функциональным подразделениям объекта защиты информации.

Второй этап: выявление угроз.

1) Определяется субъект интереса к защищаемой информации.

2) Оцениваются методы, применяемые конкурентами для получения этой информации, а также вероятные направления использования слабых мест в существующей системе обеспечения безопасности в каждом конкретном случае.

3) Разрабатывается система мероприятий по пресечению действий злоумышленников.

Третий этап: анализ эффективности принятых и постоянно действующих подсистем обеспечения безопасности.

Определяются возможные специфические источники информации, анализ которых может привести к выявлению таких индикаторов (статьи в прессе, пресс-релизы, телефонные разговоры с излишней информацией в ходе переговоров, а также установившиеся стереотипы, шаблоны в повседневной работе и процедурах и т.п.).

Четвертый этап: на основе проведенных на первых трех этапах

аналитических исследований определяются необходимые дополнительные меры по обеспечению безопасности, что составляет содержание четвертого этапа. При этом перечень дополнительных защитных мер, позволяющих «закрыть» выявленные уязвимые направления, сопровождается оценкой затрат, связанных с применением каждой меры.

На **пятом этапе** рассматриваются представленные предложения по всем необходимым мерам безопасности и проводится расчет их стоимости и эффективности.

Шестой этап – реализация принятых дополнительных мер безопасности, с учетом установленных приоритетов.

Седьмой этап заключается в осуществлении контроля и доводке реализуемых мер безопасности. При этом проверяется эффективность принятых мер, выявляются оставшиеся незащищенными или вновь возникшие уязвимые места. Реализуемые меры доводят до оптимального уровня, вводится постоянный контроль за их функционированием.

Осуществляется систематический контроль за исполнением организационно-распорядительных документов и инструкций по защите конфиденциальной информации.

Тема 7. Базовые положения инженерно-технической и программно-аппаратной защиты информации

1. Понятие инженерно-технической и программно-аппаратной защиты информации

Системный подход к построению системы защиты, означающий оптимальное сочетание взаимосвязанных организационных, программных, аппаратных, физических и других свойств в настоящее время является самым эффективным.

Вся совокупность технических средств подразделяется на ***аппаратные*** и ***физические.***

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с программным обеспечением (ПО) самой ИС.

При защите информации рекомендуется использовать программные и технические средства защиты информации, сертифицированные в системе

сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01.БИ00.

К проведению работ по аттестации объектов защиты могут привлекаться организации, имеющие соответствующие лицензии на право проведения работ в данной области или аккредитованные в качестве органов по аттестации объектов информатизации по требованиям безопасности информации.

Под **техническим способом защиты информации** понимаются различные аппаратные способы защиты информации.

Технические средства включают в себя:

– фильтры, экраны на аппаратуру;

– ключ для блокировки клавиатуры;

– устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т.д.;

– электронные ключи на микросхемах.

Под **программным способом защиты информации** понимается разработка специального программного обеспечения, которое бы не позволяло постороннему человеку, не знакомому с этим видом защиты, получать информацию из системы.

Программные средства включают в себя:

– парольный доступ – задание полномочий пользователя;

– блокировка экрана и клавиатуры с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilites;

– использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом.

Под **криптографическим способом защиты информации** подразумевается ее шифрование при вводе в компьютерную систему.

2. Современная компьютерная безопасность

Обеспечение безопасности информации на объектах информатизации является сложной задачей.

Опасность злоумышленных несанкционированных действий над конфиденциальной информацией приняла особенно угрожающий характер с развитием компьютерных сетей.

Международная организация стандартизации (МОС) определяет следующие сервисы безопасности:

1. Аутентификация (подтверждение подлинности).
2. Обеспечение целостности.
3. Засекречивание данных.
4. Контроль доступа.
5. Защита от отказов.

Среди механизмов безопасности сетей, предусмотренных МОС, обычно выделяют следующие основные:

• шифрование;

• контроль доступа;

• цифровая подпись.

Шифрование применяется для реализации служб засекречивания и используется в ряде других служб.

Механизмы контроля доступа обеспечивают реализацию одноименной службы безопасности, осуществляют проверку полномочий объектов сети, т.е. программ и пользователей, на доступ к ресурсам сети. При доступе к ресурсу через соединение, контроль выполняется в точке инициализации связи, в промежуточных точках, а также в конечной точке.

Самым распространенным и одновременно самым ненадежным методом аутентификации является парольный доступ. Более совершенными являются пластиковые карточки и электронные жетоны. Наиболее надежными считаются методы аутентификации по особым приметам личности, так называемые биометрические методы.

Цифровая подпись используется для реализации служб аутентификации и защиты от отказов. По своей сути она призвана служить электронным аналогом реквизита «подпись», используемого на бумажных документах. Механизм цифровой подписи базируется на использовании способа шифрования с открытым ключом. Знание соответствующего открытого ключа дает возможность получателю электронного сообщения однозначно опознать его отправителя.

Дополнительными механизмами безопасности, предусмотренными МОС, являются следующие:

• обеспечение целостности данных;
• аутентификация;
• подстановка трафика;
• управление маршрутизацией;
• арбитраж.

Основным источником угрозы несанкционированного проникновения является канал подключения к внешней сети, например, к Интернету. Вероятность реализации угрозы зависит от множества факторов, поэтому говорить о едином способе защиты в каждом конкретном случае не представляется возможным. Распространенным вариантом защиты является применение межсетевых экранов, или брандмауэров.

Брандмауэр (файервол) – барьер между двумя сетями: внутренней и внешней, обеспечивает прохождение входящих и исходящих пакетов в соответствии с правами, определенными администратором сети. Брандмауэр устанавливается у входа в корпоративную сеть, и все коммуникации проходят через него.

Возможности межсетевых экранов позволяют определить и реализовать правила разграничения доступа, как для внешних, так и для внутренних пользователей корпоративной сети, скрыть, при необходимости, структуру сети от внешнего пользователя, блокировать отправку информации по «запретным» адресам, контролировать использование сети и т.д. Вход в корпоративную сеть становится усложненным, прежде всего, для злоумышленника.

В зависимости от характера информации, обрабатываемой в том или ином сегменте сети, и от способа взаимодействия между сегментами реализуют один из следующих вариантов.

В *первом варианте* не устанавливается никакого разграничения информационных потоков, т.е. защита практически отсутствует. Такой вариант оправдан в случаях, когда ни в одном из взаимодействующих сегментов не хранится и не обрабатывается критичная информация или когда сегменты сетевой информационной системы содержат информацию одинаковой важности и находятся в одном здании, в пределах контролируемой зоны.

Во *втором варианте* разграничение достигается средствами коммуникационного оборудования (маршрутизаторы, переключатели и т.п.). Такое разграничение не позволяет реализовать защитные фикции в полном объеме, поскольку, во-первых, коммуникационное оборудование изначально не рассматривается как средство зашиты и, во-вторых, требуется детальное представление о структуре сети и циркулирующих в ней информационных потоках.

В *третьем вариан*те предполагается применение брандмауэров. Данный способ применяется, как правило, при организации взаимодействия между сегментами через сеть Интернет, когда уже установлены брандмауэры, предназначенные для контроля потоками информации между информационной системой и сетью Интернет.

Наиболее критичными ресурсами корпоративной сети являются серверы, а основным способом вмешательства в нормальный процесс их функционирования является проведение атак с использованием уязвимых мест в аппаратном и программном обеспечении. Атака может быть реализована как из внешней сети, так и из внутренней. Основная задача заключается не столько в своевременном обнаружении и регистрации атаки, сколько в противодействии ей.

Наиболее мощными инструментами зашиты, предназначенными для оперативного реагирования на подобные нападения, являются специальные системы, наподобие системы RealSecure, производимой американской корпорацией Internet Security Systems Inc., которые позволяют своевременно обнаружить и предотвратить наиболее известные атаки, проводимые по сети.

До настоящего времени большинство автоматизированных систем ориентируется только на встроенные защитные механизмы сетевых операционных систем. При правильном администрировании такие механизмы обеспечивают достаточную защиту информации на серверах корпоративной сети.

3. Основные понятия криптографии и стеганографии

Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Защита информации с использованием криптографических методов достигается преобразованием информации при помощи шифрования и/или

выработки имитовставки. Зашифрованное сообщение называют ***шифротекстом (ciphertext).*** Процесс, при котором из шифротекста извлекается открытый текст, называют **дешифровкой *(decryption).*** Обычно в процессе шифровки и дешифровки используется некий **ключ *(key)*** и алгоритм, которые обеспечивают невозможность дешифрования без знания этого ключа.

Метод, применяемый в криптографии для шифровки или дешифровки информации, называют **шифром *(cipher).*** Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано, только если известен ключ. Как уже отмечалось ранее, ключ, используемый для дешифровки, может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают. Алгоритмы с использованием ключа делятся на два класса: *симметричные* (или алгоритмы с секретным ключом) и *асимметричные* (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки. Широко известными симметричными алгоритмами являются DES, AES и IDEA, к наиболее популярным асимметричным алгоритмам можно отнести RSA.

Симметричные алгоритмы подразделяют на *потоковые шифры* и *блочные шифры.* Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором бит данных и шифруют этот набор как единое целое. Асимметричные шифры (также именуемые алгоритмами с открытым ключом или в более общем плане – криптографией с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют *открытым ключом,* ключ для дешифрования – *закрытым ключом* или *секретным ключом.*

Еще одним важным элементом при изучении понятия криптографии является понятие криптографической системы – семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют защищаемый открытый текст в шифрограмму и обратно.

К современным криптографическим системам защиты информации предъявляются следующие требования:

1. Зашифрованное сообщение должно поддаваться чтению только при наличии ключа.
2. Число операций, необходимых для определения использованного

ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей.

3. Число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и не выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений).

4. Знание алгоритма шифрования не должно влиять на надежность защиты.

5. Незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа.

6. Структурные элементы алгоритма шифрования должны быть неизменными.

7. Дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте.

8. Длина шифрованного текста должна быть равной длине исходного текста.

9. Не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования.

10. Любой ключ из множества возможных должен обеспечивать надежную защиту информации.

11. Алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Современные алгоритмы шифровки или дешифровки достаточно сложны и их невозможно проводить вручную. В таких условиях процесс криптографического закрытия данных осуществляется программно или аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Основная задача высшего образования заключается в формировании творческой личности специалиста, способного к саморазвитию, самообразованию, инновационной деятельности. Решение этой задачи вряд ли возможно только путем передачи знаний в готовом виде от преподавателя к студенту. Необходимо перевести студента из пассивного потребителя знаний в активного их творца, умеющего сформулировать проблему, проанализировать пути ее решения, найти оптимальный результат и доказать его правильность. Происходящая в настоящее время реформа высшего образования связана по своей сути с переходом от парадигмы обучения к парадигме образования. В этом плане следует признать, что самостоятельная работа студентов является не просто важной формой образовательного процесса, а должна стать его основой.

Самостоятельная работа студентов – способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процессе преподавателей**.**

Формами самостоятельной работы являются:

1. Работа с конспектами лекций, рекомендованной литературой, поиск новейших достижений по системе Интернет.

2. Подготовка к практическим занятиям.

КОНТРОЛЬ ЗНАНИЙ СТУДЕНТОВ

В конце изучения курса у всех студентов проверяется и оценивается преподавателем письменное решение тестовых заданий. Результаты решения тестовых заданий студенты вписывают в специальную таблицу.

Фамилия студента			Номер группы		
1			6		
2			7		
3			8		
4			9		
5			10		

Студенты, не выполнившие тестовые задания по блоку самостоятельной работы, не допускаются к сдаче зачета.

1. Свойство информации, позволяющее при ее передаче, обработке, хранении скрыть ее смысловое содержание, а также делающее доступным смысловое содержание информации только авторизованным пользователям, неодушевленным объектам и процессам, – это:

а) целостность;

б) доступность;

в) конфиденциальность;

г) целесообразность.

2. Способность использовать или вступать в контакт с информацией либо ресурсами в информационной системе – это:

а) гарантия;

б) достоверность;

в) доступ;

г) привилегия.

3. Наука, изучающая криптографические преобразования (включает в себя два направления – криптографию и криптоанализ) – это:

а) криминология;

б) криптология;

в) кармология;

г) криминалистика.

4. Расположите в правильной последовательности этапы организации защиты ценной информации согласно концепции OPSEC:

а) создание программы по защите ценной информации;

б) утверждение программы по защите ценной информации у руководства;

в) анализ объекта защиты;

г) выявление угроз информационной безопасности;

д) реализация программы;

е) корректировка реализуемой программы по защите ценной информации;

ж) анализ информационных ресурсов.

5. Промежуток времени с момента, когда появляется возможность использовать слабое место в защите информации и до момента, когда слабое место ликвидируется, – это:

а) атака;

б) идентификационный период;

в) окно опасности;

г) попытка реализации угрозы.

6. Субъект, который устанавливает порядок предоставления информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивает условия доступа к ней (информации), – это:

а) владелец информационных ресурсов;

б) собственник информационных ресурсов;

в) пользователь информационных ресурсов;

г) программист.

7. Метод шифрования информации, при использовании которого один и тот же ключ используется для зашифровки и расшифровки данных, – это:

а) ассиметричный метод шифрования;

б) симметричный метод шифрования;

в) корректный метод шифрования;

г) некорректный метод шифрования.

8. Сервис безопасности, позволяющий субъекту назвать себя (сообщить свое имя), а второй стороне убедиться в том, что субъект является тем, за кого он себя выдает, – это:

а) туннелирование;

б) анализ защищенности;

в) экранирование;

г) идентификация и аутентификация.

9. Специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования, – это:

а) программные средства защиты;

б) криптографические средства защиты;

в) стеганографические средства защиты;

г) аппаратные средства защиты.

10. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, – это:

а) обладатель информации;

б) пользователь информации;
в) собственник информации.

Вопросы к зачету

1. Предмет и задачи дисциплины.
2. Информационная безопасность. Угрозы информационной безопасности.
3. Соотношение предмета дисциплины «Защита информации» с другими учебными курсами.
4. Система курса «Защита информации»
5. Правовой, административно-организационный, инженерно-технический и программно-аппаратный аспекты защиты информации.
6. Система принципов защиты информации.
7. Принцип законности и принцип уважение прав и свобод человека и гражданина.
8. Принцип соблюдение баланса интересов человека, общества и государства.
9. Принципы комплексности, своевременности и непрерывности.
10. Принцип эшелонирования.
11. Принцип надежности (равнопрочности).
12. Принцип совершенствования.
13. Принцип экономической целесообразности.
14. Информационное право как основа деятельности по защите информации.
15. Государственный уровень правового регулирования деятельности по защите информации.
16. Правовое регулирование защиты государственной тайны
17. Локальный уровень правового регулирования.
18. Правовое регулирование защиты коммерческой и банковской тайны.
19. Понятие субъектов защиты информации, их функции и классификации.
20. Комплекс прав и обязанностей субъектов защиты информации.
21. Российская Федерация, субъекты РФ, государственные органы и должностные лица государственных органов как субъекты защиты информации.
22. Юридические и физические лица как обладатели прав и обязанностей по защите информации.
23. Понятие и классификации угроз информационной безопасности.
24. Информационные, программно-математические, физические и радиоэлектронные угрозы.
25. Угрозы конфиденциальности данных и программ.
26. Угрозы целостности данных, программ, аппаратуры.
27. Угрозы доступности данных.
28. Программно-целевой метод в деятельности по защите информации.
29. Концепции защиты информации. Концепция защиты информации OPSEC.

30. Организационные мероприятия программы по защите информации.
31. Служебное расследование по факту потери контроля за ценной информацией.
32. Основные операционные технологические схемы обработки конфиденциальных документов.
33. Понятие инженерно-технической и программно-аппаратной защиты информации.
34. Системы контроля и управления доступом.
35. Идентификация и аутентификация.
36. Протоколирование и аудит.
37. Шифрование и стеганография.
38. Экранирование.
39. Анализ защищенности.
40. Антивирусная защита.

ЛИТЕРАТУРА

Основная:

1. Бачило И.Л. Информационное право: учебник для вузов. – М.: Юрайт-Издат, Высш обр., 2009.
2. Галатенко В.А. Основы информационной безопасности / под ред. В.Б. Бетелина – М.: Интернет-Университет информационных технологий, 2003.
3. Грень И.В. Компьютерная преступность. – Минск: Новое знание, 2007.
4. Джеймс Л. Фишинг. Техника компьютерных преступлений / пер. с англ. Р.В. Гладицкого. – М.: НТ Пресс, 2008.
5. Дзлиев М.И., Урсул А.Д. Основы обеспечения безопасности России: учеб. пособие. – М.: Экономика, 2003.
6. Диев С. Организация и современные методы защиты информации. – М.: БДЦ, 1998.
7. Домашев А., Попов В., Правиков Д., Прокофьев И., Щербаков А. Программирование алгоритмов защиты информации. – М.: Нолидж, 2000.
8. Доронин А. Экономическая и информационная безопасность. – Тула, 1997.
9. Защита информации. – М.: Мир безопасности, 1998.
10. Информационное право: учебник / Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. – М.: Норма: ИНФРА-М, 2010.
11. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учеб. пособие. – М.: ФОРУМ, 2009.
12. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: Полигон, 2000.
13. Копылов В.А. Информационное право. – М.: Юристъ, 2002.
14. Корнеев И.К., Степанов Е.А. Защита информации в офисе: учебник. – М.: Проспект, 2009.
15. Кузнецов И.Н. Учебник по информационно-аналитической работе. – М.: Яуза, 2001.
16. Куприянов А. И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – М.: Академия, 2006.
17. Партыка Т.Л., Попов И.И. Информационная безопасность: учеб. пособие. – М.: ФРУМ: ИНФРА, 2002.
18. Правовое обеспечение информационной безопасности: учебник / под общ. ред. В.А. Минаева, А.П. Фисуна, С.В. Скрыля, С.В. Дворянкина, М.М. Никитина, Н.С. Хохлова. – М.: Маросейка, 2008.
19. Северин В. Правовое обеспечение информационной безопасности предприятия. – М.: Городец, 2000.
20. Соловьев Э. Коммерческая тайна и ее защита. – М.: Главбух, 1995.

21. Фисун А.П., Касилов А.Н., Глоба Ю.А., Савин В.И., Белевская Ю.А. Право и информационная безопасность: учеб. пособие // под ред. А.П. Фисуна и Ю.А. Белевской. – М.: Приор-издат, 2005.

22. Халяпин Д.Б., Ярочкин В.И. Основы защиты информации: учеб. пособие. – М.: ИПКИР, 1994.

23. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009.

24. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003.

25. Ярочкин В.И. Безопасность информационных систем. – М.: Ось-89, 1996.

26. Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000.

Дополнительная:

1. Абрамов В. Информационно-аналитическая работа частных структур безопасности. – М.: Каскад. 1997.

2. Абрамов В. Подбор, проверка, изучение и расстановка кадров. – М.: Арсин Лтд, 1998.

3. Антонов И.О. Коммерческая тайна: понятие, правовое регулирование и организация защиты. Методические рекомендации. – Казань: Форт-Диалог, 1996.

4. Антонов И.О., Романов В.И. Обеспечение экономической безопасности субъекта предпринимательской деятельности: учеб. пособие. – Казань: МАРПО, 2001.

5. Ацапина Л.А. Коммерческая тайна как объект гражданских прав: автореф. дис. ... к.ю.н. – М., 2005.

6. Донцов Д. Как защитить компьютер от ошибок, вирусов, хакеров. – СПб.: Питер, 2008.

7. Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов / под ред. В.Н. Черкасова. – Саратов: СЮИ МВД России, 2006.

8. Крылов В.В. Информационные компьютерные преступления. – М.: ИГ ИНФРА-М – НОРМА, 1997.

9. Куваева М.В., Чуфаровский Ю.В., Шиверский А.А. Коммерческая информация: способы получения и защиты. – М.: Юристъ. 1996.

10. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. – СПб., 2000.

11. Лысов А., Остапенко А. Телефон и безопасность (проблемы защиты информация в телефонных сетях). – СПб.: Лаборатория ППШ, 1997.

12. Максимов Ю., Сонников В., Петров В., Паршуткин А., Еремеев М. Шпионские штучки-4. Технические методы и средства защиты информации. – М.: АСТ, СПб.: Полигон, 2000.

13. Мирских И.Ю. Коммерческая тайна как вид конфиденциальной информации: трудоправовой и цивилистический аспекты: автореф. дис. ... к.ю.н. – Пермь, 2005.

14. Поздняков Е.Н. Защита объектов (рекомендации для руководителей и сотрудников служб безопасности). – М.: Банковский деловой центр, 1997.

15. Петраков А.В. Защита и охрана личности, собственности, информации. – М.: Радио и связь, 1997.

16. Прасолов А. Информационная безопасность бизнеса // Охранная деятельность. – 2005. – № 3–4.

17. Промохов Ю. О вирусах // Мир безопасности. – 2000. – № 10 (83).

18. Современные информационные технологии в юридической деятельности: учеб.-метод. комплекс для студентов юрид. фак. – Волгоград: ВА МВД РФ, 2006.

19. Соколов А., Степанюк О. Шпионские штучки-5. Методы информационной защиты объектов и компьютерных сетей. – М.: АСТ, СПб.: Полигон, 2000.

20. Соколов А.В. Шпионские штучки: новое и лучшее. – СПб.: Полигон, 2000.

21. Халяпин Д. Чем заткнуть длинное ухо // Мир безопасности. – 1998. – № 3 (55).

22. Халяпин Д. Визуально-оптический канал утечки информации. // Мир безопасности. – 1998. – № 7 (59).

23. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. – М.: Ось-89, 2000.

Учебное издание

АНТОНОВ Игорь Олегович

ЗАЩИТА ИНФОРМАЦИИ

Корректор *Орлова М.Л.*
Технический редактор
Компьютерная верстка

Подписано в печать . Формат .
Бумага офсетная. Гарнитура New Roman. Печать .
Усл. печ. л. . Уч.-изд. л. . Тираж 100 экз. Заказ № .