Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

Институт отраслевой экономики и управления

Р. А. Мнацаканян

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие по изучению дисциплины
для студентов по программе специалитета 38.05.01. Экономическая
безопасность

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

УДК 004.056.5

Рецензент
кандидат экономических наук, доцент кафедры экономии и финансов ФГБОУ ВО «Калининградский государственный технический университет»
Т. В. Романова

Мнацаканян, Р. А.
Информационная безопасность: учебно-методическое пособие по изучению дисциплины для студентов по программе специалитета 38.05.01 Экономическая безопасность / Р.А. Мнацаканян. – Калининград: ФГБОУ ВО «КГТУ», 2022. - 79 с.

В учебно-методическом пособии приведен тематический план по дисциплине и даны методические указания по её самостоятельному изучению, подготовке к практическим занятиям, задания и методические указания по выполнению контрольной работы, подготовке и сдаче экзамена, выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины «Информационная безопасность» специальности 38.05.01 Экономическая безопасность.
Табл. 7, рис. 7, список лит. – 22 наименования

Учебно-методическое пособие рассмотрено и одобрено для опубликования в качестве локального электронного методического материала кафедрой экономической теории и инструментальных методов 01.04.2022 г., протокол № 8

Учебно-методическое пособие по изучению дисциплины рекомендовано к изданию в качестве локального электронного методического материала для использования в учебном процессе методической комиссией ИНОТЭКУ 31.08.2022 г., протокол № 8

УДК 004.056.5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Дисциплина "Информационная безопасность" формирует у обучающихся способность решать стандартные задачи профессиональной деятельности на основе применения информационных ресурсов, технологий, методов и средств с учётом основных требований, предъявляемых к экономической безопасности.

Настоящее учебно-методическое пособие представляет собой комплекс систематизированных материалов по самостоятельному изучению дисциплины "Информационная безопасность".

Учебная дисциплина "Информационная безопасность" является фундаментальной экономической дисциплиной опирающаяся на знания, приобретенные в результате освоения таких дисциплин, как, "Экономическая теория", "Информационные технологии", "Общая экономическая безопасность", "Экономическая безопасность организации (предприятия)", "Экономическая безопасность России" и вариативной части образовательной программы специалитета по специальности 38.05.01 Экономическая безопасность, специализация "Экономико-правовое обеспечение экономической безопасности".

Учебно-методическое пособие составлено в соответствии с утвержденной рабочей программой дисциплины "Информационная безопасность" программой подготовки в специалитете 38.05.01. Экономическая безопасность.

Преподавание дисциплины "Информационная безопасность" строится исходя из требуемого уровня базовой подготовки специалистов по программе 38.05.01 Экономическая безопасность.

Целью изучения дисциплины "Информационная безопасность" является формирование у студентов необходимых теоретических и практических знаний и навыков в области информационной безопасности при проектировании, внедрении и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС).

Задачи дисциплины "Информационная безопасность":

- дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности ВС/ИС;

- сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

Планируемые результаты освоения дисциплины "Информационная безопасность" заключаются в том, что студент должен:

***знать*:**

- предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ;

- основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия;

- иметь полное представление о значение информационной безопасности для современного бизнеса, о перспективах развития технологий обеспечения информационной безопасности;

***уметь*:**

- анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ;

- использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры;

- применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ;

- ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ;

***владеть*:**

- способностью применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации ИБ;

- способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия;

- организовывать и проводить аудит ИБ;

- использовать современные инструментальные средства анализа рисков и разработки политики ИБ.;

- навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.

Общая трудоемкость дисциплины составляет 4 зачетных единиц (зет), т. е. 144 академических часа аудиторных (лекционных, лабораторных и практических (семинарских) занятий и самостоятельной учебной работы специалиста, в т. ч. связанной с промежуточной и итоговой аттестацией по дисциплине.

Студенты заочной формы обучения во внеаудиторное время выполняют контрольную работу в соответствии с заданием и методическими указаниями, приведенными в четвертом разделе настоящего пособия.

Распределение трудоемкости освоения дисциплины по семестрам ОП, видам учебной работы студента, а также формы контроля приведены ниже в таблицах 1, 2.

В этом же семестре выполняется контрольная работа и проводится итоговая аттестация в форме экзамена.

Структура учебно-методического пособия по изучению дисциплины включает пять раздела.

Таблица 1 - Объем (трудоёмкость освоения) в очной форме обучения и структура дисциплины

Номер и наименование темы	**Объем учебной работы, ч**		
	Лекции	**ЛЗ**	**ПЗ**
Семестр – 7, трудоемкость – 4 ЗЕТ (144 ч)			
1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия.	3	3	3
2. Защищенная информационная система. Уровни и структура ИБ.	4	4	4
3. Модели и стандарты в сфере ИБ и управления рисками ИБ.	5	5	5
4. Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры.	5	5	5
Подготовка к сдаче и сдача экзамена	-	-	-
Всего в седьмом семестре	17	17	17
	51		

Таблица 2 - Объем (трудоёмкость освоения) в заочной форме обучения и структура дисциплины

Номер и наименование темы	**Объем учебной работы, ч**		
	Лекции	**ЛЗ**	**ПЗ**
Семестр – 9, трудоемкость – 4 ЗЕТ (144 ч)			
1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия.	0,5	1	1
2. Защищенная информационная система. Уровни и структура ИБ.	0,5	1	1
3. Модели и стандарты в сфере ИБ и управления рисками ИБ.	0,5	1	1
4. Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры.	0,5	1	1
Подготовка к сдаче и сдача экзамена	-	-	-
Всего в девятом семестре	2	4	4
	10		

В первом разделе приводится тематический план, соответствующий содержанию изучаемой дисциплины, даются методические указания по её самостоятельному изучению.

Во втором разделе учебно-методического пособия представлены методические указания для подготовки к практическим занятиям.

В третьем разделе учебно-методического пособия представлены задания и методические указания по выполнению контрольной работы для студентов заочной формы обучения.

В четвертом разделе представлены методические указания по подготовке к промежуточной аттестации по дисциплине, которая проводится в форме экзамена.

В пятом разделе представлены методические указания по выполнению самостоятельной работы по дисциплине.

В конце учебного пособия указаны рекомендуемые источники по изучению дисциплины.

1 Тематический план по дисциплине и методические указания по её изучению

Содержательно структура дисциплины представлена четырнадцатью тематическими блоками (темами):

Тема 1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия

Содержание темы

Цель и задачи дисциплины, место дисциплины в структуре образовательной программы. Понятие и сущность информационной безопасности для субъектов экономики. Объективная необходимость управления информационной безопасностью. Практические примеры нарушения информационной безопасности и их последствия для государства, бизнеса, личности. Современная концепция информационной безопасности. Цели и концептуальные основы защиты информации. Ключевые положения корпоративной концепции информационной безопасности. Нормативно-правовые акты в области информационной безопасности в РФ: акты федерального законодательства; методические документы государственных органов России; стандарты информационной безопасности. Международный опыт правового обеспечения информационной безопасности. Сравнительная характеристика международного и российского законодательства в сфере ИБ.

Методические указания

Цель темы – дать базовое представление о современных требованиях к обеспечению информационной безопасности и определить необходимость повышения уровня информационной безопасности на предприятии.

В результате изучения темы будут получены знания, позволяющие рассматривать информационную безопасность, как необходимый элемент деятельности как коммерческих и некоммерческих предприятий, так и государственных структур, обеспечивающий их информационные ресурсы конфиденциальностью, целостностью и работоспособностью.

В процессе изучения темы следует уяснить, что информационная безопасность – это невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой.

Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена. Формирование информационного общества концептуально и практически означает формирование мирового информационного пространства.

Информационное пространство (инфосфера) - сфера человеческой деятельности связанная: с созданием, преобразованием и потреблением информации.

Информационная война - информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство - форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность - проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться

информационный терроризм, то есть деятельность, проводимая в политических целях.

Информационное воздействие - акт применения информационного оружия.

Информационное оружие - комплекс технических и других средств, методов и технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;

- вмешательство в работу его систем управления и информационных сетей, систем связи и т. п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;

- распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;

- воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства над противником или ослабления проводимых им информационных воздействий.

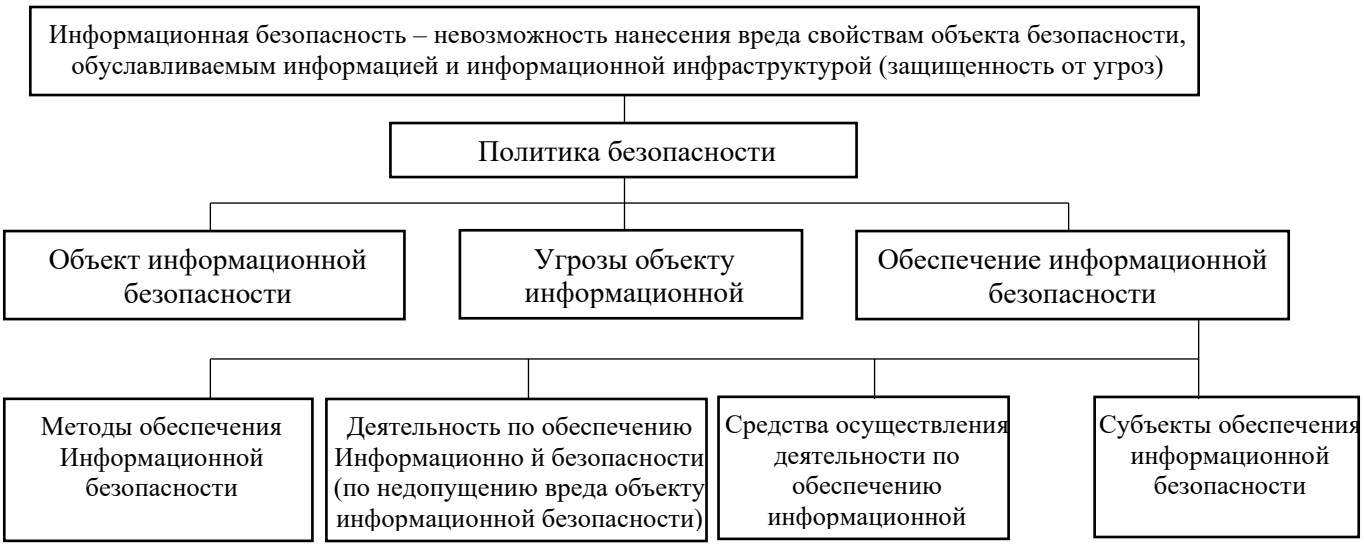

Рисунок 1 - Структура понятия «Информационная безопасность»

Под *угрозой безопасности информации* понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Объектом информационной безопасности может быть коммерческое предприятие. Тогда содержание "информационной безопасности" будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными. Интересы проявляются через объекты, способные служить для их удовлетворения, и действия, предпринимаемые для обладания этими объектами. Соответственно интересы как объект безопасности могут быть представлены совокупностью информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение информацией или сокрытие информации. Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз.

Система обеспечения безопасности информации включает подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Основные предметные направления *защиты информации* - охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

Под *системой безопасности* понимается организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Система защиты информации представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размерам ущерба располагаются кражи и подлоги, в большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами.

Концепция информационной безопасности — это система взглядов на проблему обеспечения информационной безопасности, взаимоувязывающая правовые, организационные и программно-аппаратные меры защиты и основанная на анализе защищенности информационной системы в разрезе видов угроз и динамики их развития.

Из анализа действующего законодательства вытекает, что правовой защите подлежит главным образом документированная информация (документ), зафиксированная на материальном носителе с реквизитами, т.е. информация, облеченная в форму, позволяющую ее идентифицировать.

При этом неправомерный доступ к компьютерной информации считается преступлением, если:

- компьютерная информация охраняется законом, а именно отвечает нормам Закона "Об информации, информатизации и защите информации" (в частности ст. 2 и 5 Закона);

- неправомерный доступ привел к уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или сети (ст. 272 УК).

Государственные и коммерческие структуры, которые подверглись нападениям, не хотят афишировать их последствия и недостаточную

эффективность своих систем защиты. Поэтому совершаемые преступления далеко не всегда становятся достоянием гласности. Не следует думать, что информационные преступления является лишь отечественной национальной спецификой.

Как уберечь информацию от потерь и несанкционированного доступа заинтересованных лиц? Можно предложить следующий набор административных мер:

- структурировать работу организации;

- формализовать потоки документов и упорядочить их хранение;

- регламентировать правила работы с документами;

- исключить доступ к корпоративной информации сотрудников организации после уведомления их об увольнении.

При разработке организационных мер необходимо помнить, что существует как минимум три способа потери данных: с использованием личного контакта, средств компьютерной техники и технических каналов передачи данных.

Выбор контрмер и управление рисками

При разработке концепции Информационной Безопасности организации необходимо выработать стратегию управления рисками различных классов.

Возможно несколько подходов:

- уклонение от риска;

- уменьшение риска;

- изменение характера риска;

- принятие риска.

Закон «О государственной тайне» от 21.07.93 г. № 5485-1 – основной нормативный руководящий документ. Этот Закон содержит ряд статей и регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Нормативно-правовые акты в области информационной безопасности в РФ:

- Федеральный закон от 27 июля 2006 г. « 149-ФЗ «Об информации, информационных технологиях и о защите информации».

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г.).

- Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (с изменениями от 8 ноября 2007 г.).

- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (с изменениями от 2 февраля, 18 декабря 2006 г., 24 июля 2007 г.).

- Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895).

- Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

- Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации».

Весьма совершенным в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года) Глава 28 - "Преступления в сфере компьютерной информации".

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Зарубежное законодательство в области информационной безопасности. Ключевую роль играет американский "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145),

January 8, 1988). Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

В законодательстве ФРГ имеется весьма развернутый (44 раздела) Закон о защите данных (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)). Он целиком посвящен защите персональных данных.

Методические материалы по теме 1

В ходе работы по теме студенту следует использовать лекционный материал; материалы, рассмотренные на практическом занятии; рекомендованную литературу; все материалы в соответствующем разделе дисциплины в ЭИОС КГТУ.

Ссылки на рекомендуемые источники по теме 1: [2-11].

Тема 2. Защищенная информационная система. Уровни и структура ИБ

Содержание темы

Понятие и виды защищаемой информации в соответствии с законом РФ «Об информации, информационных технологиях и защите информации». Классификации защищаемой информации. Содержание, объём и ценность защищаемой информации. Модель угроз информационной безопасности как описание существующих угроз ИБ, их актуальности, возможности реализации и последствий. Обязательный учёт в модели всех актуальных угроз на всех стадиях их жизненного цикла. Процедура построения модели угроз информационной безопасности, состоящая из нескольких последовательных шагов. Пересмотр и обновление модели информационной безопасности на основе постоянно меняющихся данных. Определение защищенной информационной системы. Трехуровневая модель параметров оценки защищенности ИС. Модель защищенных информационных систем. Порядок

разработки и структурные элементы программы информационной безопасности. Перечень и основное содержание действующих в РФ организационно распорядительных документов в сфере ИБ и практика их применения. Политика ИБ как комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов. Порядок разработки Политики ИБ.

Методические указания

Цель темы - получить представление о защищенной информационной системе. Исследовать уровни и структуру информационной безопасности.

В результате изучения темы будут получены знания о:

- видах защищаемой информации;
- моделях угроз и информационной безопасности;
- понятии защищенной информационной системы;
- программе информационной безопасности;
- организационно-распорядительных документах в сфере информационной безопасности;
- политике информационной безопасности.

В процессе изучения темы следует уяснить, что защищенная информационная система – это система, использующая достаточные аппаратные и программные средства, для обеспечения одновременно достоверную обработку информации разной степени секретности различными пользователями или группами пользователей без нарушения прав доступа, целостности и конфиденциальности данных и информации, и поддерживающая свою работоспособность в условиях воздействия на нее совокупности внешних и внутренних угроз.

В соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006) защищаемая информация – это информация, являющаяся предметом собственности и

подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Виды защищаемой информации:

- Государственная тайна
- Персональные данные/GDPR
- Коммерческая тайна
- Автоматизированные системы управления технологическими процессами (АСУ ТП)
- Государственные и муниципальные ИС
- Информация для служебного пользования
- Открытые информационные ресурсы

Классификация защищаемой информации может осуществляться по принадлежности, степени секретности и по содержанию.

Классификация информации по категориям доступа.

Рисунок 2 - Классификация информации по категориям доступа

Защищаемая информация неоднородна по содержанию, объему и ценности. Следовательно, защита будет рациональной в том случае, когда

уровень защиты, а, следовательно, затраты, соответствуют количеству и качеству информации. Если затраты на защиту информации выше ее цены, то уровень защиты неоправданно велик, если существенно меньше, то возможно уничтожение, хищение или модернизация информации, приводящие к значительному ущербу. Для обеспечения рациональной защиты возникает необходимость структурирования конфиденциальной информации, т. е. разделения ее на так называемые информационные элементы.

Стандарт СТО БР ИББС – 1.0-2010 определяет модель угроз информационной безопасности следующим образом: это «описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба».

Адекватные модели угроз информационной безопасности позволяют выявить существующие угрозы, разработать эффективные контрмеры, повысив тем самым уровень ИБ, и оптимизировать затраты на защиту (сфокусировав её на актуальных угрозах).

Рисунок 3 – Модели угроз

У различных информационных систем, а также объектов одной информационной системы может быть разный спектр угроз, определяемый особенностями конкретной информационной системы и её объектов и характером возможных действий источника угрозы.

Проектирование системы информационной безопасности информационной системы с учетом всей важности вопроса является сложным процессом, который должен учитывать многие факторы: программные, технические, организационные и правовые. Система обеспечения информационной безопасности разрабатывается с целью достижения приемлемого уровня защиты информационной системы от случайных или преднамеренных действий различного происхождения, и ее разработка включает в себя следующие основные этапы:

1) оценку текущего состояния информационной безопасности информационной системы;

2) описание модели угроз информационной безопасности;

3) формирование рекомендаций по совершенствованию системы обеспечения информационной безопасности.

модель угроз может иметь два варианта реализации:

- самостоятельный проект информационной безопасности информационной системы;

- интегрированный компонент безопасности в проекте информационной системы.

Для построения модели угроз информационной безопасности информационной системы используются методики и каталоги угроз из официального стандарта ГОСТ Р 51275-2006, методических документов ФСТЭК, Стандартов Банка России.

Концепция "Защищенные информационные системы" включает в себя ряд законодательных инициатив, научных, технических и технологических решений, готовность государственных организаций и компаний использовать

их для того, чтобы люди, используя устройства на базе компьютеров и ПО, чувствовали себя так же комфортно и безопасно.

В "Оранжевой книге" надежная информационная система определяется как "система, использующая достаточные аппаратные и программные средства, для обеспечения одновременно достоверную обработку информации разной степени секретности различными пользователями или группами пользователей без нарушения прав доступа, целостности и конфиденциальности данных и информации, и поддерживающая свою работоспособность в условиях воздействия на нее совокупности внешних и внутренних угроз".

Таблица 3 - Трехуровневая модель параметров оценки защищенности ИС.

Система целей	**Средства**	**Исполнение**
Общая цель: • Защищенные информационные системы	*Установки:* • защищенность • конфиденциальность • целостность • готовность к работе • точность • управляемость • безотказность • прозрачность • удобство пользования	*Обеспечение:* • законы, нормы • характер ведения бизнеса • контракты, обязательства • внутренние принципы • международные, отраслевые, и внутренние стандарты
Цели: • безопасность • безотказность • деловое взаимодействие	*Подтверждения:* • внутренняя оценка • аккредитация • внешний аудит	*Реализация*: • методы взаимодействия с внешней и внутренней средой • методы работ • анализ рисков • методы разработки, внедрения, • эксплуатации и сопровождения • обучение персонала

В процессе функционирования защищенной информационной системы (ЗИС) предприятия возникает огромное количество событий безопасности. Даже правильно настроенное отдельно взятое средство защиты в сутки может регистрировать сотни «нештатных» событий, но из них лишь малый процент

представляет действительную опасность. В централизованной системе защиты обязательно настраивается аудит событий на всех автоматизированных рабочих местах (АРМ) и сетевом оборудовании с занесением информации в журнал безопасности на сервере для дальнейшего анализа. Просмотром этого журнала занимается администратор безопасности. На основании полученных данных он создает и корректирует правила безопасности для каждого конкретного устройства или программы. Этот механизм имеет как минимум 2 слабых места:

1. Наличие человеческого фактора;

2. Отсутствие унифицированности описания ошибок, генерируемых различными СЗИ, уязвимостей, настроек безопасности.

Согласно методике ФСТЭК России, актуальность угроз определяется следующим образом:

1) Рассчитываются вероятность реализации и опасность угрозы. Вероятность ($У_2$) может принимать значения: 0 (маловероятная), 2 (низкая вероятность), 5 (средняя вероятность) и 10 (высокая вероятность). Опасность угрозы принимает значения: «низкая», «средняя» и «высокая». Оба параметра определяются экспертным путем.

2) Вычисляется коэффициент реализуемости угрозы $У$ по формуле

$$У=(У_1+У_2)/20,$$

где $У_1$ – показатель исходной защищенности ИС (обратный опасности угрозы), зависящий от ее технических и эксплуатационных характеристик. Он может принимать значения 0 (для высокой степени исходной защищенности), 5 (для средней степени) и 10 (для низкой степени).

По значению коэффициента реализуемой угрозы $У$ формируется вербальная интерпретация реализуемости угрозы: «низкая» (от 0 до 0,3), «средняя» (от 0,3 до 0,6), «высокая» (от 0,6 до 0,8) и «очень высокая» (больше 0,8).

Рассчитав возможность реализации угрозы $У$ и ее опасность, можно определить ее актуальность по таблице 4.

Таблица 4 – Определение актуальности угрозы

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Конечные данные о расчетах актуальности угроз безопасности, рассматриваемой ИС, сводятся в таблицу.

Органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ, является ФСТЭК России. Это закреплено указом Президента Российской Федерации от 25.11.2017 г. № 569 «О внесении изменений в Положение о ФСТЭК России», утвержденное Указом Президента Российской Федерации от 16.08.2004 г. № 1085. Специалисты ведомства серьезно подошли к поставленной задаче и уже к концу зимы разработали и ввели нормативную базу, необходимую для категорирования потенциальных объектов КИИ и создания систем их защиты. Состав указанной нормативной базы приведен в таблице далее.

Политика информационной безопасности — комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых на предприятии для обеспечения его информационной безопасности.

Как правило, создание ПИБ начинается с постановки целей, которые должны быть достигнуты с помощью данного документа. Количество целей и конкретные формулировки остаются на усмотрение руководства. Но, не следует впадать в излишнюю детализацию (например, "снижение рисков вирусного заражения" или "соответствие стандарту СТО БР ИББС" – лучше оставить для нижестоящих документов).

Таблица 5 - Состав нормативной базы ФСТЭК России в области обеспечения информационной безопасности КИИ

Постановления Правительства	• № 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (далее — Правила категорирования) • № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
Приказы ФСТЭК России	• № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»; • № 229 от 11.12.2017 г. «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; • № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (далее — Приказ № 235); • № 236 от 21.12.2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»; • № 239 от 25.12.2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — Требования по безопасности КИИ).

Основная цель политики информационной безопасности – установление фарватера (тренда) защиты информации, который станет базисом для всех остальных документов, в том числе рассказывающих доступным языком пользователям, почему необходимо защищать информацию (для этого хорошо подходит политика (регламент) по работе с конфиденциальной информацией или с корпоративными ресурсами).

Следующий важный пункт – область действия политики. В идеале ПИБ должна охватывать всю организацию, дочерние предприятия, филиалы и подразделения. Если это по каким-то причинам невозможно, то в ПИБ

необходимо предусмотреть раздел по контролю непротиворечивости ПИБ различных элементов организации.

Далее – содержание политики. При создании ПИБ небольших размеров можно быть уверенным, что ее прочитают. Если организация не строго формалистская, то в политику необходимо включить принципы обеспечения ИБ. Однако дословное бездумное копирование принципов из международных стандартов (законность, комплексность, преемственность и т. д.) "убьет" документ. Скорее всего, дальше его никто читать не будет.

Обязательно уделите внимание следующим принципам:

- непрерывность – для установления непрерывного контроля над защищаемыми объектами и их окружением;
- системность, что позволит охватить все сферы деятельности организации;
- своевременность – для получения гибкости в противодействии актуальным и потенциальным угрозам;
- контроль;
- экономическая целесообразность, которая позволит вам обосновывать достигнутые результаты или требуемые инвестиции.

В заключение политике необходимо уделить внимание самому процессу управления информационной безопасностью. Здесь должен быть дан старт процессу, который будет описан в отдельном документе. Необходимо обозначить его главные этапы, например по Демингу – планирование, действие, контроль, совершенствование.

Это минимально необходимое содержание политики. Его можно бесконечно дополнять, например правовыми основаниями, рисками и угрозами, нарушителями, основными подсистемами системы защиты.

Методические материалы по теме 2

В ходе работы по теме студенту следует использовать лекционный материал; материалы, рассмотренные на практическом занятии; рекомендованную литературу; все материалы в соответствующем разделе дисциплины в ЭИОС КГТУ.

Ссылки на рекомендуемые источники по теме 2: [2-9, 11].

Тема 3. Модели и стандарты в сфере ИБ и управления рисками ИБ

Содержание темы

Понятие и виды информационных рисков. Математические методы их оценки. Технологии (методики) управления информационными рисками. Российский и международный опыт стандартизации в области информационной безопасности. Международные стандарты ISO. Необходимость стандартизации обеспечения безопасности данных. Общая характеристика проблемы синтеза систем защиты информации для информационных систем. Исследование предметной области с целью создания математической модели системы защиты информации (СЗИ). Общая характеристика математических методов оценки и обоснования требований к СЗИ.

Методические указания

Цель темы - получить представление о моделях и стандартах в сфере ИБ и управления рисками ИБ.

В результате изучения темы будут получены знания о:

- управлении информационными рисками;

- стандартизации в сфере информационной безопасности;

- математических моделях систем и процессов защиты информации;

- сервисах ИБ и защите от инсайдеров.

В процессе изучения темы следует уяснить, что информационные риски – это вероятность ущерба вследствие применения компанией или предприятием

информационных технологий и для их минимизации созданы различные модели и стандарты.

Понятие информационного риска не имеет четкого и устойчивого определения, на сегодняшний день. В теории и на практике пока не выработано единого подхода к их дефиниции. Условно можно выделить следующие подходы к трактовке термина «информационный риск»:

1) Информационный риск является тождественным угрозе безопасности информации и трактуется как потенциальное событие, вследствие которого может быть удалена или искажена информация, нарушена ее доступность или конфиденциальность. Управление информационными рисками в данном случае эквивалентно информационной безопасности.

2) Информационный риск подразумевает возможность наступления для организации ущерба или убытков. Каждый из двух подходов опирается на негативный характер риска, его связь исключительно с отрицательными последствиями. В то же время нельзя говорить о наличии противоречий описанных подходов между собой.

На практике способы выявления IT-рисков ничем не отличаются от способов определения любых других рисков: составляются карты рисков, проводится сбор экспертных мнений и т. п.

Для оценки рисков используются количественные и качественные методы оценки. Математическое моделирование относится к группе количественных методов. Качественные методы позволяют дать комплексную оценку вероятности наступления риска и ущерба от его реализации, однако недостатком является то, что необходимо привлекать компетентных экспертов. Количественные методы являются, в свою очередь более трудоемкими, но позволяют определить несколько альтернатив для принятия решений. К количественным методам относят следующие виды расчетных методов:

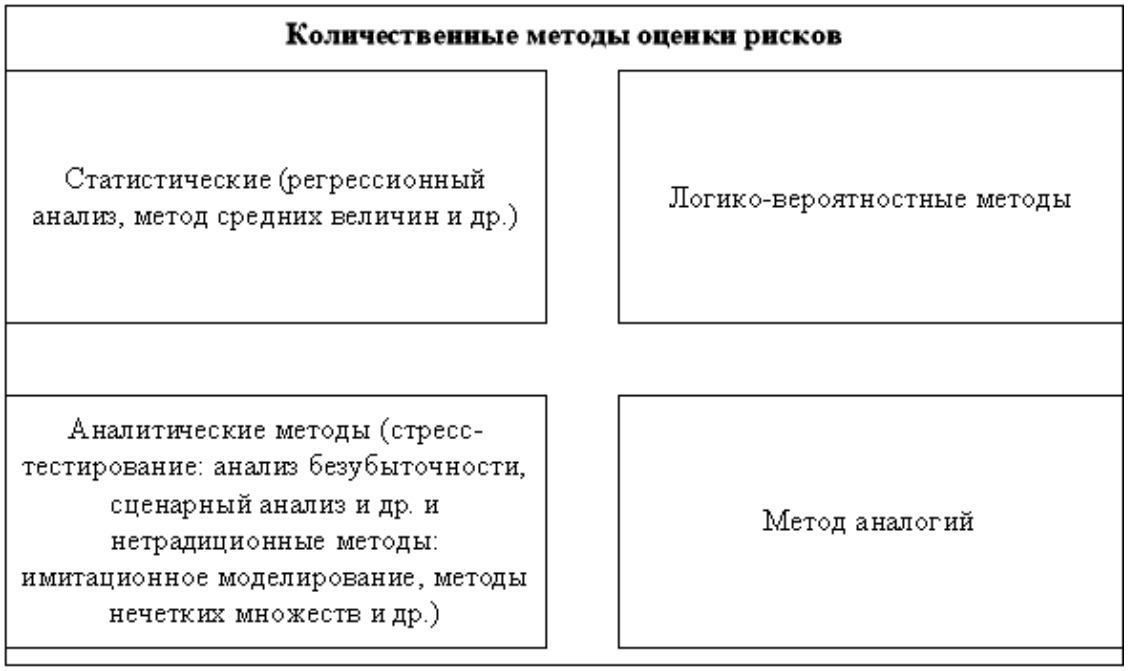

Рисунок 4 – Количественные методы оценки рисков

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином «управление информационными рисками» обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативно правовой базы в области защиты информации и собственной корпоративной политики безопасности. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

К качественным методикам управления рисками на основе требований ISO 17999 относятся методики COBRA и RA Software Tool.

К количественным методикам управления рисками относятся методики CRAMM и MethodWare.

Любое обеспечение информационной безопасности нуждается в контроле и проверке, которая не может быть произведена только лишь методом индивидуальной оценки, без учета международных и государственных стандартов.

Формирование стандартов информационной безопасности происходит после четкого определения ее функций и границ.

Стандартизация в области информационной безопасности (ИБ) выгодна и профессионалам, и потребителям продуктов и услуг ИБ, так как позволяет установить оптимальный уровень упорядочения и унификации, обеспечить взаимозаменяемость продуктов ИБ, а также измеряемость и повторяемость результатов, полученных в разных странах и организациях. Для профессионалов — это экономия времени на поиск эффективных и зарекомендовавших себя решений, а для потребителя - гарантия получения результата ожидаемого качества.

Стандартизация, в зависимости от состава участников, бывает международной, региональной или национальной, при этом международная стандартизация (наравне с официальными органами стандартизации, такими как ISO) включает в себя стандартизацию консорциумов (например, IEEE или SAE), а национальная стандартизация бывает государственной или отраслевой.

Компании, которые беспокоятся о защите собственной конфиденциальной информации и сертифицируют товары и услуги по системе ISO 9001, должны стремиться организовать собственную систему менеджмента информационной безопасности (СМИБ) на основе ISO/IEC 27000–2016 или более ранних версий, если внедрение СМИБ началось до введения новой редакции стандарта.

Согласно модели менеджмента ISO 9001, процесс создания и внедрения системы включает четыре этапа, которые обозначаются аббревиатурой PDCA.

В России наиболее полные собственные стандарты СМИБ разработала банковская сфера. Документы, утвержденные в итоге как Стандарт Центрального банка России по информационной безопасности, вобрали лучшие мировые практики, включая методики оценки рисков CRAMM и OCTAVE.

Оценки параметров СЗИ в условиях высокой степени неопределенности условий ее функционирования должны вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и таким образом непрерывно совершенствующихся на основе оптимального выбора исходных данных.

При синтезе оптимальных систем защиты исходными должны явиться следующие два положения:

• выбор математически вычисляемого критерия оптимальности в соответствии с архитектурой системы защиты и технологией обработки информации на объекте;

• четкая математическая формулировка задачи, учитывающая все априорные сведения и позволяющая решить ее в соответствии с принятым критерием.

Итогом решения задачи синтеза оптимальной системы защиты и его конечной целью должны быть четыре содержательных результата:

• архитектура системы защиты;

• количественная оценка качества ее функционирования;

• оценка практической чувствительности разработанных моделей к отклонениям от априорных данных;

• физическая реализуемость синтезируемых систем защиты в современных системах обмена данными (соответствие технологии обработки информации уровню ее защиты).

Математическая модель представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей и ответных мер. Расчетные количественные значения параметров

модели характеризуют функциональные (аналитические, алгоритмические или численные) зависимости, описывающие процессы взаимодействия нарушителей с системой защиты и возможные результаты действий.

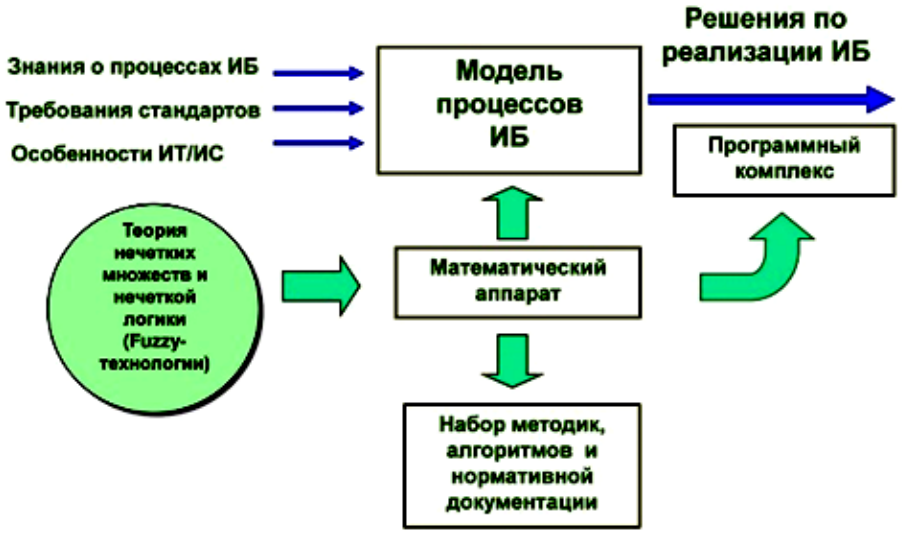

Рисунок 5 - Место математических моделей в реализации защиты информации

Именно такой вид моделей чаще всего используется для количественных оценок уязвимости объекта, построения алгоритма защиты оценки рисков и эффективности принятых мер.

Пример модели процесса защиты, строящийся в терминах теории нечетких множеств и нечеткой логики представлен ниже.

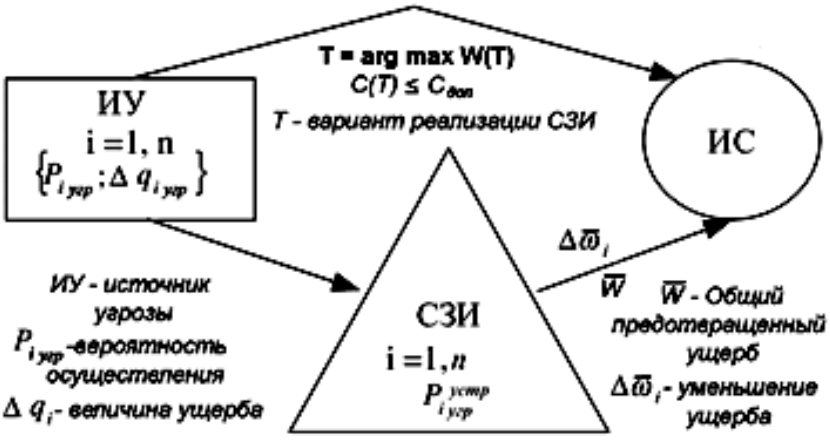

Рисунок 6 - Модель процесса защиты

Одним из эффективных методов выбора варианта модели является метод экспертных оценок. Для проведения экспертизы по распоряжению ЛПР

создается рабочая группа, которая организует деятельность экспертов, составляющих экспертную группу.

Надежная СЗИ должна обеспечивать такое построение и функционирование защитных механизмов, чтобы общая политика безопасности постоянно проводилась в жизнь, несмотря на уязвимости коммуникационных путей и параллельную, асинхронную работу компонентов.

Базовой основой реализации эффективной работы сервисов безопасности является рациональная архитектура распределенной ВС/ИС и полностью соответствующая ей система защиты информации.

Инсайдеры – лица, имеющие доступ к внутренней информации о корпорации, которая в большей степени является конфиденциальной. Чаще всего штатные работники предприятия, случайно, ошибочно или умышленно превышающие свои полномочия при работе с информацией, следствием чего является нарушение ее целостности, доступности и/или конфиденциальности.

Стандартный набор сервисов безопасности для защиты от инсайдеров:

- идентификация / аутентификация пользователя;
- управление доступом;
- контроль доступа;
- протоколирование / аудит;
- контроль целостности;
- контроль защищенности;
- экранирование;
- туннелирование;
- шифрование;
- обнаружение отказов и оперативное восстановление.

Наиболее эффективной формой защиты от инсайдеров является совокупность сервисов информационной безопасности.

Методические материалы по теме 3

В ходе работы по теме студенту следует использовать лекционный материал; материалы, рассмотренные на практическом занятии; рекомендованную литературу; все материалы в соответствующем разделе дисциплины в ЭИОС КГТУ.

Ссылки на рекомендуемые источники по теме 3: [1-9, 11].

Тема 4. Технологии и методы реализации ИБ, комплексная защита информационной инфраструктуры

Содержание темы

Криптография. Методы криптографического преобразования информации. Обобщённая схема криптографической системы. Законопроект «О безопасности критической информационной инфраструктуры». Защита от таргетированных атак, что должно обеспечивать эшелонированную систему защиты информации. Средства и виды антивирусных средств защиты. Внешние и внутренние угрозы информационной безопасности предприятия. Особенности и задачи корпоративных систем защиты информации. Комплексная защита информации в корпоративных сетях: задачи, средства и стоимость решений.

Методические указания

Цель темы - получить представление о технологии и методах реализации информационной безопасности и о комплексной защите информационной инфраструктуры.

В результате изучения темы будут получены знания о:

- криптографических методах защиты информации;
- защите информационной инфраструктуры от атак;
- антивирусных средствах защиты;
- комплексной защиты информационной инфраструктуры и ресурсов;
- оценке эффективности СЗИ.

В процессе изучения темы следует уяснить, что любое коммерческое и некоммерческое предприятие, а также государство в своей деятельности постоянно сталкиваются с внешними и внутренними угрозами информационной безопасности, что подталкивает их к более подробному изучению технологий и методов реализации ИБ для формирования комплексной защиты информационной инфраструктуры.

Криптографическое преобразование — это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоемкостью меньше заранее заданной.

Криптография делится на два класса: криптография с симметричными ключами и криптография с открытыми ключами.

В криптографии с симметричными ключами (классическая криптография) абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных.

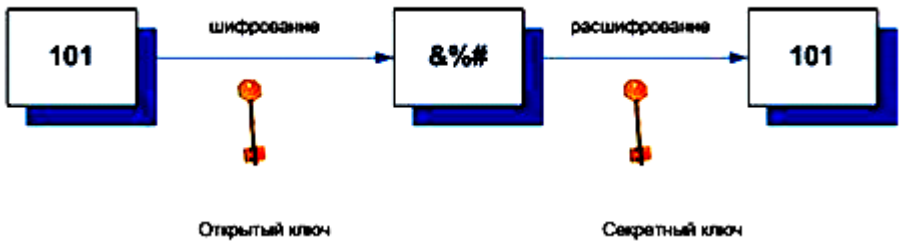

Рисунок 7 - Схема шифрования в криптографии с открытыми ключами

Реализация схемы ЭЦП связанна с вычислением хэш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма. Хэш-функция является однонаправленной функцией, т. е. по хэш-значению невозможно восстановить исходные данные. Хэш-функция чувствительна к всевозможным искажениям данных. Кроме того,

очень трудно отыскать два набора данных, обладающих одним и тем же значением хэш-функции.

Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. В целях настоящей статьи под информационными ресурсами Российской Федерации понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

1) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено

функционирование значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры и этими требованиями предусматриваются:

1) планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Таргетированная (или целевая) атака — это заранее спланированный удаленно управляемый в реальном времени процесс непрерывной и несанкционированной активности в инфраструктуре атакуемой системы.

В состав эшелонированной системы защиты информации от таргетированных атак обычно входят:

- средства выявления и блокирования атак и сетевых аномалий на периметре сети (включая DDoS-атаки);
- средства выявления сетевых аномий внутри сети заказчика;
- средства противодействия таргетированным атакам на web-приложения;
- средства противодействия таргетированным атакам на СУБД.

Указанные средства комбинируются с классическими системами межсетевого экранирования и IPS. Вся совокупность средств должна функционировать в рамках единых политик информационной безопасности и предоставлять события ИБ для централизованного корреляционного анализа в рамках SIEM-системы.

Обнаружение таргетированной атаки — очень сложная и комплексная задача. Факт проникновения в систему может оставаться незамеченным долгое время. В связи с этим очень сложно оценить общее число атак, проводимых по всему миру.

Использование антивирусных программ является основным средством защиты информации от компьютерных вирусов.

Выделяют следующие виды антивирусных программ: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

В настоящее время разделение антивирусных программ на виды не является жестким, многие антивирусные программы совмещают различные функции. Производители антивирусных программ начали создавать не просто программы антивирусы, а комплексные средства для борьбы с вирусами. Одна из наиболее популярных и наиболее универсальных антивирусных программ — DoctorWeb, антивирус Касперского Personal Pro, Norton Antivirus Professional Edition. Это универсальные и перспективные антивирусные программы, сочетающие функции антивирусного сканера, резидентного сторожа и доктора.

Создание комплексной системы защиты информации (КСЗИ) отражает системный подход к обеспечению информационной безопасности (ИБ)

компании, предотвращению хищений и утечек информации ограниченного доступа, а также оптимизирует работу ИТ-системы предприятия, снижает капитальные и операционные затраты компании.

Основные цели средств защиты информации – обеспечение стабильного функционирования компаний и предупреждение угроз безопасности информации.

К задачам КСЗИ относятся:

- своевременное обнаружение и устранение угроз информационной безопасности;
- ограничение возможности несанкционированного перехвата сведений по каналам передачи;
- создание копий баз данных, критичных для предприятия, на случай их утраты;
- учет текущего состояния IT-инфраструктуры и прогноз изменений внешней и внутренней среды;
- восстановление информационных систем при повреждении.

Внешние угрозы (кибератаки) – реальная опасность, которая затрагивает интеллектуальную и физическую собственность организаций. Распространенная форма киберпреступности – применение специальных программ. Они способны нарушить целостность секретных документов.

Как показывает практика, большую часть инцидентов провоцируют внутренние угрозы. Хищение интеллектуальной собственности, утечки коммерческой тайны и ущерб информационной системе могут нанести действия сотрудников. Такие действия могут быть совершены из корыстных соображений (злонамеренные), по неосторожности (случайные) или из-за некомпетентности человека.

Основными методами защиты информации являются:

1. Антивирусная защита.
2. Шифрование (криптографические средства).

3. Защита информации внутри сети (использование Virtual Private Network).

4. Proxy servers.

5. Межсетевые экраны (брандмауэры).

Методические материалы по теме 4

В ходе работы по теме студенту следует использовать лекционный материал; материалы, рассмотренные на практическом занятии; рекомендованную литературу; все материалы в соответствующем разделе дисциплины в ЭИОС КГТУ.

Ссылки на рекомендуемые источники по теме 4: [2-9, 11].

2 Методические указания для подготовки к практическим занятиям

Целью проведения практических (семинарских) занятий является закрепление теоретических знаний, полученных на лекциях и самостоятельном изучении дисциплины "Информационная безопасность", для выработки профессиональных умений и навыков, сформулированных в рабочей программе дисциплины.

Практическими (семинарскими) занятиями предусматривается сочетание индивидуальных и групповых форм работы, выполнение практических заданий с использованием ситуационных задач, анализа макроэкономических показателей и др.

Занятие по теме 1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;

2. Дискуссия по пройденному материалу;

3. Работа с тестом.

Вопросы:

1. Информационное пространство (инфосфера);
2. Информационная война;
3. Информационное противоборство;
4. Информационная преступность;
5. Информационное воздействие;
6. Информационное оружие;
7. Угроза безопасности информации;
8. Информационная безопасность;
9. Объект информационной безопасности;
10. Компьютерная безопасность;
11. Безопасность данных;
12. Безопасность коммуникаций;
13. Политика безопасности;
14. Угроза безопасности информации;
15. Защита информации (ЗИ);
16. Система защиты информации (СЗИ);
17. Виды обеспечения СЗИ;
18. Классы угроз информационной безопасности;
19. Концепция Информационной Безопасности;
20. Правовая основа Концепции;
21. Что подлежит правовой защите;
22. Организационные меры по предотвращению нарушений безопасности информации;
23. Подходы по выработке стратегии управления рисками;
24. Основные цели обеспечения информационной безопасности экономических систем;
25. Основные задачи обеспечения информационной безопасности экономических систем;

26. Нормативно-правовые акты в области информационной безопасности в РФ.

Занятие по теме 2. Защищенная информационная система. Уровни и структура ИБ

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;

2. Дискуссия по пройденному материалу.

Вопросы:

1. Защищаемая информация;

2. Отличительные признаки защищаемой информации;

3. Государственная тайна;

4. Персональные данные;

5. Что такое GDPR;

6. Принципы GDPR;

7. Коммерческая тайна;

8. Автоматизированная система управления технологическим процессом;

9. Документы с грифом «Для служебного пользования»;

10. Открытые информационные ресурсы;

11. Характеристики безопасной ИС;

12. Классификация защищаемой информации;

13. Классификация информации по категориям доступа;

14. Ценность информации;

15. Шаги процедуры построения модели угроз информационной безопасности;

16. Моделирование сценариев угроз;

17. Защищенная информационная система;

18. Модель ЗИС;

19. Состав нормативной базы ФСТЭК России в области обеспечения информационной безопасности КИИ;

20. Политика информационной безопасности (ПИБ);

21. Этапы создания ПИБ.

Занятие по теме 3. Модели и стандарты в сфере ИБ и управления рисками ИБ

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;

2. Дискуссия по пройденному материалу.

Вопросы:

1. Информационный риск;

2. Проблемные аспекты оценки информационных рисков;

3. Виды информационных рисков;

4. Проблемы страхования информационных рисков;

5. Категории IT-рисков;

6. Процесс минимизации ИТ-рисков;

7. Выявление IT-рисков;

8. Методы количественной оценки рисков;

9. Статистические методы;

10. Логико-вероятностные методы;

11. Метод аналогий;

12. Аналитическая группа методов;

13. Виды количественных показателей риска;

14. Формула функции для оценки динамики исследуемого параметра;

15. График плотности вероятности;

16. Основные черты функции нормального распределения;

17. Применение метода VaR в оценке риска;

18. Статистические способы оценки риска;

19. Применение элементов теории игр;

20. Качественные методики управления рисками

21. COBRA

22. RA Software Tool

23. Количественные методики управления рисками

24. CRAMM

25. Методика Method Ware

26. Необходимость стандартизации обеспечения безопасности данных;

27. Международные стандарты в области ИБ;

28. системы менеджмента информационной безопасности;

29. Создание СМИБ с учетом стандартов;

30. Российские СМИБ;

31. Преимущества СМИБ;

32. Исходные положения при синтезе оптимальных систем защиты;

33. Итоги решения задачи синтеза оптимальной системы защиты и его конечная цель;

34. Математическая модель процессов в СЗИ;

35. Пример модели процесса защиты;

36. Выбор модели реализации СЗИ;

37. Архитектурная безопасность;

38. Инсайдеры;

39. Стандартный набор сервисов безопасности.

Занятие по теме 4. Технологии и методы реализации ИБ, комплексная защита информационной инфраструктуры

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;

2. Дискуссия по пройденному материалу.

Вопросы:

1. Криптографическое преобразование;
2. Криптография с симметричными ключами;
3. Криптография с открытыми ключами;
4. Свойства криптографии с открытыми ключами;
5. Реализация схемы электронной цифровой подписи (ЭЦП);
6. Схема формирования подписи электронного документа (ЭД);
7. Комбинированный метод;
8. Сертификация открытых ключей;
9. ФЗ «О безопасности критической информационной инфраструктуры»;
10. Таргетированная (или целевая) атака;
11. Их цели;
12. Классификация таргетированных атак;
13. Этапы таргетированных атак;
14. Объект воздействия таргетированных атак;
15. Источники таргетированных атак;
16. Анализ риска таргетированных атак;
17. Система защиты должна обеспечивать;
18. Состав эшелонированной системы защиты информации от таргетированных атак;
19. Альтернативные возможности защиты информации;
20. Результаты внедрения;
21. Используемы технологии;
22. Компьютерный вирус;
23. Классификация вирусов;
24. Виды антивирусных программ;
25. Комплексная система защиты информации;
26. Цели и задачи комплексной системы защиты информации;

27. Принципы создания комплексной системы защиты информации;

28. Основные функции КСЗИ по обеспечению ИБ;

29. Основные модули КСЗИ;

30. Внешние угрозы информационной безопасности;

31. Внутренние угрозы информационной безопасности;

32. Выгоды при внедрении комплексной системы защиты информации;

33. К организационным методикам относятся;

34. Основными методами защиты информации являются.

3 Задания и методические указания по выполнению контрольной работы

3.1 Общие сведения, выбор варианта

В соответствии с рабочей программой дисциплины "Информационная безопасность" студенты заочной формы обучения выполняют контрольную работу.

Контрольная работа является одним из способов оценки результатов освоения дисциплины и направлена на самостоятельное решение конкретной задачи, сформулированной в задании на её выполнении.

Контрольная работа состоит из двух разделов. Первый раздел представляет собой письменное изложение двух теоретических вопросов, а второй – решение задач.

Контрольная работа сдается путем прикрепления в ЭИОС ИНОТЭКУ КГТУ в соответствующую рубрику, созданную преподавателем по данной дисциплине. Срок сдачи: не позднее начала зачетно-экзаменационной сессии, установленную графиком учебного процесса.

Критерии оценивания контрольной работы аналогичен критерию оценивания экзамена по дисциплине и представлен в разделе 4.

Выбор варианта для ***теоретических вопроса*** осуществляется в соответствии со списком студентов при помощи таблицы.

Таблица 6 – Выбор варианта для теоретических вопросов

Номер студента по списку	Теоретические вопросы
1	1,18
2	2,19
3	3,20
4	4,21
5	5,22
6	6,23
7	7,24
8	8,25
9	9,26
10	10,27
11	11,28
12	12,29
13	13,30
14	14,31
15	15,32
16	16,33
17	17,34
18	18,35
19	3,33
20	4,32

Для ***задач*** выбор варианта осуществляется по последней цифре номера по списку. Задачи решить с использованием MS EXCEL.

3.2 Методические указания по выполнению контрольной работы

Объем контрольной работы следует ограничить 10-15 страницами, оформление производится в соответствии с требованиями, принятыми в ИНОТЭКУ КГТУ.

Работу следует разбить на следующие **структурные разделы:**

- содержание;
- введение;
- теоретические вопросы;
- решение задач;
- заключение.

В конце работы должен быть приведен **список использованных источников**, состоящий не менее чем из 5 наименований.

3.3 Тематика контрольных работ с заданиями на их выполнение

Теоретические вопросы

1. Объективная необходимость управления информационной безопасностью.

2. Современная концепция информационной безопасности.

3. Цели и концептуальные основы защиты информации.

4. Понятие и сущность информационной безопасности для субъектов экономики.

5. Классификации защищаемой информации.

6. Ключевые положения корпоративной концепции информационной безопасности.

7. Методические документы государственных органов России; стандарты информационной безопасности.

8. Международные стандарты ISO по защите информации.

9. Модель угроз информационной безопасности как описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

10. Пересмотр и обновление модели информационной безопасности на основе постоянно меняющихся данных.

11. Трехуровневая модель параметров оценки защищенности ИС.

12. Политика ИБ как комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов.

13. Понятие и виды информационных рисков.

14. Общая характеристика математических методов оценки и обоснования требований к СЗИ.

15. Криптография как наука о методах обеспечения конфиденциальности и аутентичности информации.

16. Законопроект «О безопасности критической информационной инфраструктуры».

17. Внешние и внутренние угрозы информационной безопасности информационной безопасности предприятия.

18. Необходимость стандартизации обеспечения безопасности данных.

19. Практические примеры нарушения информационной безопасности и их последствия для государства, бизнеса, личности.

20. Сравнительная характеристика международного и российского законодательства в сфере ИБ.

21. Обязательный учёт в модели всех актуальных угроз на всех стадиях их жизненного цикла.

22. Процедура построения модели угроз информационной безопасности, состоящая из нескольких последовательных шагов.

23. Порядок разработки и структурные элементы программы информационной безопасности.

24. Порядок разработки Политики ИБ.

25. Математические методы оценки информационных рисков.

26. Технологии (методики) управления информационными рисками.

27. Исследование предметной области с целью создания математической модели системы защиты информации (СЗИ).

28. Методы криптографического преобразования информации.

29. Обобщённая схема криптографической системы.

30. Порядок и этапы защиты от таргетированных атак для обеспечения эшелонированной системы защиты информации.

31. Средства и виды антивирусных средств защиты.

32. Комплексная защита информации в корпоративных сетях: задачи, средства и стоимость решений.

33. Реализация методики оценки информационных рисков.

34. Постановка проблемы синтеза систем защиты информации для информационных систем.

35. Особенности и задачи корпоративных систем защиты информации.

Задачи

1. Определить время перебора всех паролей с параметрами.

Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

После каждого из m неправильно введенных паролей идет пауза в v секунд

Вариант	n	k	s	m	v
0	33	10	100	0	0
1	26	12	13	3	2
2	52	6	30	5	10
3	66	7	20	10	3
4	59	5	200	0	0
5	118	9	50	7	12
6	128	10	500	0	0
7	150	3	200	5	3
8	250	8	600	7	3
9	500	5	1000	10	10

2. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

Вариант	n	t	s
0	33	100	100
1	26	120	13
2	52	60	30
3	66	70	20
4	59	50	200
5	118	90	50
6	128	100	500
7	150	30	200
8	250	80	600
9	500	50	1000

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

Вариант	k	t	s
0	5	100	100
1	6	120	13
2	10	60	30
3	7	70	20
4	9	50	200
5	11	90	50
6	12	100	500
7	6	30	200
8	8	80	600
9	50	50	1000

4. Зашифровать свою ФИО с использованием шифра Цезаря.

5. Зашифровать свою ФИО с использованием шифра Вижинера.

6. Сделать QR-код для своей страницы в соц. сетях.

4 Методические указания по подготовке к промежуточной аттестации

Промежуточная (заключительная) аттестация по дисциплине проводится в форме экзамена в седьмом семестре для очной формы обучения и в девятом семестре для заочной формы обучения.

К экзамену допускаются студенты:

- положительно аттестованные по результатам проведенного тестирования;

- получившие положительную оценку по результатам работы в текущем семестре на семинарских, практических и лабораторных занятиях;

- получившие положительную оценку по контрольной работе (для студентов заочного обучения).

Критерии оценивания контрольной работы аналогичен критерию оценивания экзамена по дисциплине, и представлен ниже.

Экзаменационная оценка («отлично», «хорошо», «удовлетворительно» или «неудовлетворительно») является экспертной и зависит от уровня освоения специалистом тем дисциплины.

Критерии оценивания экзамена по дисциплине:

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную (процентную) систему и правило перевода оценок в пятибалльную систему.

Таблица 7 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40 %	**41-60 %**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3. Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно- корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи

Система оценок / Критерий	2	3	4	5
	0-40 %	**41-60 %**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
4. Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

К оценочным средствам для промежуточной аттестации по дисциплине, проводимой в форме экзамена, соответственно относятся вопросы для проведения промежуточной аттестации (экзамена).

Перечень контрольных вопросов

1. Объективная необходимость управления информационной безопасностью.

2. Современная концепция информационной безопасности.

3. Цели и концептуальные основы защиты информации.

4. Понятие и сущность информационной безопасности для субъектов экономики.

5. Классификации защищаемой информации.

6. Ключевые положения корпоративной концепции информационной безопасности.

7. Нормативно-правовые акты в области информационной безопасности в РФ: акты федерального законодательства

8. Методические документы государственных органов России; стандарты информационной безопасности.

9. Международные стандарты ISO по защите информации.

10. Содержание, объём и ценность защищаемой информации.

11. Модель угроз информационной безопасности как описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

12. Пересмотр и обновление модели информационной безопасности на основе постоянно меняющихся данных.

13. Трехуровневая модель параметров оценки защищенности ИС.

14. Политика ИБ как комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов.

15. Понятие и виды информационных рисков.

16. Общая характеристика математических методов оценки и обоснования требований к СЗИ.

17. Криптография как наука о методах обеспечения конфиденциальности и аутентичности информации.

18. Законопроект «О безопасности критической информационной инфраструктуры».

19. Внешние и внутренние угрозы информационной безопасности информационной безопасности предприятия.

20. Необходимость стандартизации обеспечения безопасности данных.

21. Практические примеры нарушения информационной безопасности и их последствия для государства, бизнеса, личности.

22. Международный опыт правового обеспечения информационной безопасности.

23. Сравнительная характеристика международного и российского законодательства в сфере ИБ.

24. Обязательный учёт в модели всех актуальных угроз на всех стадиях их жизненного цикла.

25. Процедура построения модели угроз информационной безопасности, состоящая из нескольких последовательных шагов.

26. Пересмотр и обновление модели информационной безопасности на основе постоянно меняющихся данных.

27. Порядок разработки и структурные элементы программы информационной безопасности.

28. Порядок разработки Политики ИБ.

29. Математические методы оценки информационных рисков.

30. Технологии (методики) управления информационными рисками.

31. Исследование предметной области с целью создания математической модели системы защиты информации (СЗИ).

32. Методы криптографического преобразования информации.

33. Обобщённая схема криптографической системы.

34. Порядок и этапы защиты от таргетированных атак для обеспечения эшелонированной системы защиты информации.

35. Средства и виды антивирусных средств защиты.

36. Модель защищенных информационных систем.

37. Комплексная защита информации в корпоративных сетях: задачи, средства и стоимость решений.

38. Реализация методики оценки информационных рисков.

39. Постановка проблемы синтеза систем защиты информации для информационных систем.

40. Особенности и задачи корпоративных систем защиты информации.

5 Методические указания по выполнению самостоятельной работы по дисциплине

5.1 Общие положения

Самостоятельная работа студентов в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических

занятиях, а также для индивидуального изучения дисциплины в соответствии с программой и рекомендованной литературой. Самостоятельная работа выполняется в виде подготовки домашнего задания или сообщения по отдельным вопросам, реферативного обзора.

Контроль качества самостоятельной работы может осуществляться с помощью устного опроса на практических занятиях, проведения тестирования.

Устные формы контроля помогут оценить владение студентами жанрами научной речи (дискуссия, диспут, сообщение, доклад и др.), в которых раскрывается умение студентов передать нужную информацию, грамотно использовать языковые средства, а также ораторские приемы для контакта с аудиторией. Письменные работы помогают преподавателю оценить владение источниками, научным стилем изложения, для которого характерны: логичность, точность терминологии, обобщенность и отвлеченность, насыщенность фактической информацией.

Самостоятельная работа предусмотрена в следующих формах:

1) Освоение теоретического учебного материала, в том числе подготовка к практическим занятиям (форма контроля – тестирование, контроль на практических занятиях, РГР).

2) Выполнение контрольной работы – для студентов заочной формы обучения (форма контроля – защита контрольной работы).

5.2 Задания для самодиагностики в рамках самостоятельной работы студента

Тестовые задания используются для оценки освоения всех тем дисциплины студентами всех форм обучения.

Тестирование обучающихся проводится на занятиях после рассмотрения на лекциях, соответствующих тем или самостоятельно с использованием системы компьютерного тестирования «INDIGO».

Тестирование производится методом случайной выборки (27 вопросов) в системе тестирования «INDIGO» и предусматривает выбор правильного(ых) ответа(ов) на поставленный вопрос из предлагаемых вариантов. Оценка по

результатам тестирования зависит от уровня освоения студентом тем дисциплины и соответствует следующему диапазону (%):

- от 0 до 55 – неудовлетворительно;
- от 56 до 70 – удовлетворительно;
- от 71 до 85 – хорошо;
- от 86 до 100 – отлично.

Положительная оценка («зачтено») выставляется студенту при получении от 56 до 100 % верных ответов.

5.3 Примерный перечень тестовых заданий по вариантам

Вариант 1

1. К негосударственным относятся информационные ресурсы

а) созданные, приобретенные за счет негосударственных учреждений и организаций; б) созданные, приобретенные за счет негосударственных предприятий и физических лиц; в) полученные в результате дарения юридическими или физическими лицами

2. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется

а) достоверной;

б) конфиденциальной;

в) документированной;

г) коммерческой тайной

3. Под информационной безопасностью понимается…

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;

в) нет правильного ответа

4. К организационно-административному обеспечению информации относятся:

а) взаимоотношения исполнителей;

б) подбор персонала;

в) регламентация производственной деятельности

5. Информацию с ограниченным доступом делят:

а) государственную тайну;

б) конфиденциальную информацию;

в) достоверную информацию

6. Доступность – это

а) возможность за приемлемое время получить требуемую информационную услугу;

б) логическая независимость;

в) нет правильного ответа

7. Угроза – это

а) процесс определения отвечает на текущее состояние разработки требованиям данного этапа;

б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) потенциальная возможность определенным образом нарушить информационную безопасность

8. Атака – это

а) потенциальная возможность определенным образом нарушить информационную безопасность;

б) попытка реализации угрозы;

в) программы, предназначенные для поиска необходимых программ.

9. Основными источниками внутренних отказов являются:

а) ошибки при конфигурировании системы;

б) отказы программного или аппаратного обеспечения;

в) выход системы из штатного режима эксплуатации

10. Ошибка – это

а) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния;

б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций;

в) негативное воздействие на программу

11. Вредоносная программа – это

а) упорядочение абстракций, расположение их по уровням;

б) программа, специально разработанная для нарушения нормального функционирования систем;

в) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

12. СЗИ (система защиты информации) делится:

а) ресурсы автоматизированных систем;

б) организационно-правовое обеспечение;

в) человеческий компонент

13. Из перечисленного:

1) оповещение о попытках нарушения защиты;

2) идентификация;

3) аутентификация;

4) учет носителей информации;

5) управление потоками информации — подсистема управления доступом системы защиты информации должна обеспечивать

а) 2, 3, 5; б) 3, 4, 5; в) 1, 2, 5; г) 1, 2, 3

14. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это

а) аутентификация;

б) идентификация;

в) аудит;

г) авторизация

15. Достоинством модели политики безопасности на основе анализа угроз системе является

а) динамичность;

б) числовая вероятностная оценка надежности;

в) высокая степень надежности;

г) простой механизм реализации

16. Что относится к организационным мероприятиям:

а) хранение документов;

б) проведение тестирования средств защиты информации;

в) пропускной режим

Вариант 2

1. По принадлежности информационные ресурсы подразделяются на

а) государственные, коммерческие и личные;

б) государственные, не государственные и информацию о гражданах;

в) информацию юридических и физических лиц;

г) официальные, гражданские и коммерческие

2. Целостность – это

а) целостность информации;

б) непротиворечивость информации;

в) защищенность от разрушения

3. Какие трудности возникают в информационных системах при конфиденциальности?

а) сведения о технических каналах утечки информации являются закрытыми;

б) на пути пользовательской криптографии стоят многочисленные технические проблемы;

в) все ответы правильные

4. По доступности информация классифицируется на

а) открытую информацию и государственную тайну;

б) конфиденциальную информацию и информацию свободного доступа;

в) виды информации, указанные в остальных пункта;

г) информацию с ограниченным доступом и общедоступную информацию

5. Источник угрозы – это

а) потенциальный злоумышленник;

б) злоумышленник;

в) нет правильного ответа

6. Сбой – это

а) объект-метод;

б) неправильное выполнение элементом одной или нескольких функций происходящее вследствие специфического состояния;

в) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

7. Какие события должны произойти за время существования окна опасности?

а) должно стать известно о средствах использования пробелов в защите;

б) должны быть выпущены соответствующие заплаты;

в) заплаты должны быть установлены в защищаемой ИС

8. Защита информации – это

а) процесс разработки структуры базы данных в соответствии с требованиями пользователей;

б) комплекс мероприятий, направленных на обеспечение информационной безопасности.

в) небольшая программа для выполнения определенной задачи.

9. Криптографические средства – это

а) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования;

б) специальные программы и системы защиты информации в информационных системах различного назначения;

в) механизм, позволяющий получить новый класс на основе существующего

10. Из перечисленного:

1) оповещение о попытках нарушения защиты;

2) идентификация;

3) аутентификация;

4) учет носителей информации;

5) управление потоками информации — подсистема регистрации и учета системы защиты информации должна обеспечивать

а) 1,4; б) 2,3; в) 3,4; г) 1,2

11. С помощью открытого ключа информация

а) транслируется;

б) расшифровывается;

в) копируется;

г) зашифровывается

12. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется

а) мониторингом средств защиты;

б) минимизацией риска;

в) управлением риском;

г) оптимизацией средств защиты

13. Что относится к ресурсам автоматизированной системы СЗИ (системы защиты информации)?

а) лингвистическое обеспечение;

б) техническое обеспечение;

в) все ответы правильные

14. Из перечисленного:

1) анализ потенциального злоумышленника;

2) оценка возможных затрат;

3) оценка возможных потерь;

4) анализ потенциальных угроз — процесс анализа рисков при разработке системы защиты ИС включает

а) 3, 4; б) 1, 2; в) 1, 3; г) 2, 4

15. Из перечисленного:

1) эффективность;

2) корректность;

3) унификация;

4) конфиденциальность — аспектами адекватности средств защиты являются

а) 1, 3; б) 1, 2; в) 3, 4; г) 2, 4

16. Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это

а) принцип многоуровневой защиты;

б) принцип минимизации привилегий;

в) принцип простоты и управляемости ИС;

г) принцип максимизации привилегий

Вариант 3

1. Информация - это

а) сведения, поступающие от СМИ;

б) только документированные сведения о лицах, предметах, фактах, событиях;

в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

г) только сведения, содержащиеся в электронных базах данных

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники;

б) хакеры;

в) атакующие;

г) контрагенты (лица, работающие по договору)

3. Какая информация подлежит защите?

а) информация, циркулирующая в системах и сетях связи;

б) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

в) только информация, составляющая государственные информационные ресурсы;

г) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

4. От чего зависит информационная безопасность?

а) от компьютеров;

б) от поддерживающей инфраструктуры;

в) от информации

5. Из перечисленного:

1) степень прогнозируемости;

2) природа происхождения;

3) предпосылки появления;

4) источники угроз;

5) размер ущерба — параметрами классификации угроз безопасности информации являются

а) 1, 5; б) 3, 4, 5; в) 2, 3, 4; г) 1, 2, 3

6. Конфиденциальность – это

а) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов;

б) защита от несанкционированного доступа к информации;

в) описание процедур

7. Где применяются средства контроля динамической целостности?

а) при анализе потока финансовых сообщений;

б) при обработке данных;

в) при выявлении кражи, дублирования отдельных сообщений

8. К какому виду угроз относится присвоение чужого права?

а) нарушение права собственности;

б) нарушение содержания;

в) внешняя среда

9. Окно опасности – это…

а) формализованный язык для описания алгоритма решения задачи пользователя на компьютере;

б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;

в) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

10. Правовое обеспечение безопасности информации – это…

а) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации;

б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) нет правильного ответа

11. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

а) ограниченной компетенцией злоумышленника;

б) за определенное время;

в) фиксированными затратами;

г) фиксированным ресурсом

12. Что самое главное должно продумать руководство при классификации данных?

а) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным;

б) необходимый уровень доступности, целостности и конфиденциальности;

в) оценить уровень риска и отменить контрмеры;

г) управление доступом, которое должно защищать

13. Из перечисленных программных закладок:

1) вирусные;

2) троянские;

3) программно-аппаратные;

4) загрузочные;

5) драйверные;

6) прикладные — по методу внедрения в компьютерную систему различают

а) 2, 3, 4, 5; б) 3, 4, 5, 6; в) 1, 2, 4, 6; г) 1, 2, 3, 6

14. Черви – это

а) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И. С. и их выполнения;

б) код, обладающий способностью к распространению путем внедрения в другие программы;

в) программа действий над объектом или его свойствами

15. Административные действия в СУБД позволяют выполнять привилегии

а) безопасности;

б) чтения;

в) тиражирования;

г) доступа

16. Соответствие средств безопасности решаемым задачам характеризует

а) эффективность;

б) корректность;

в) адекватность;

г) унификация

Вариант 4

1. Основные составляющие информационной безопасности:

а) целостность;

б) достоверность;

в) конфиденциальность

2. Целостность можно подразделить:

а) статическую;

б) динамичную;

в) структурную

3. Угрозы можно классифицировать по нескольким критериям:

а) по спектру ИБ;

б) по способу осуществления;

в) по компонентам И.С.

4. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы – это

а) идентификация;

б) авторизация;

в) аудит;

г) аутентификация

5. Отказ – это

а) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций;

б) некоторая последовательность действий, необходимых для выполнения конкретного задания;

в) структура, определяющая последовательность выполнения и взаимосвязи процессов

6. Какова минимальная длина безопасного пароля, состоящего из одних только строчных английских букв?

а) 15;

б) 12;

в) 10;

г) 6

7. Инсайдер — это

а) бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер;

б) система предотвращения вторжений — программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них;

в) член какой-либо группы людей, имеющий доступ к секретной, скрытой или какой-либо другой закрытой информации или знаниями, недоступной широкой публике;

8. Вирус – это

а) небольшая программа для выполнения определенной задачи;

б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов;

в) код, обладающий способностью к распространению путем внедрения в другие программы

9. Троянские программы — это

а) программы-вирусы, которые распространяются самостоятельно;

б) все программы, содержащие ошибки;

в) часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба;

г) текстовые файлы, распространяемые по сети

10. Степень защищённости информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования – это

а) уязвимость информации;

б) надёжность информации;

в) защищённость информации;

г) безопасность информации

11. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

а) криптология;

б) стеганография;

в) криптоанализ;

г) криптография

12. Из перечисленного:

1) протоколирование;

2) тестирование программ;

3) аутентификация;

4) обработка угроз;

5) резервное копирование — группами требований к документированию системы защиты информации являются

а) 2, 3, 4; б) 3, 4, 5; в) 1, 2, 3; г) 1, 2, 4

13. Требования к техническому обеспечению системы защиты

а) аппаратурные и физические;

б) управленческие и документарные;

в) процедурные и раздельные;

г) административные и аппаратурные

14. Достоинством модели политики безопасности на основе анализа угроз системе является

а) высокая степень надежности;

б) числовая вероятностная оценка надежности;

в) динамичность;

г) простой механизм реализации

15. Контроль за соблюдением инструкции по работе с компьютерной техникой осуществляет?

а) системный администратор;

б) генеральный директор предприятия;

в) пользователь;

г) начальник службы безопасности

16. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;

б) Когда риски не могут быть приняты во внимание по политическим соображениям;

в) Когда необходимые защитные меры слишком сложны;

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

Вариант 5

1. Для чего создаются информационные системы?

а) обработки информации;

б) получения определенных информационных услуг;

в) все ответы правильные

2. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

а) актуальностью информации;

б) доступностью;

в) качеством информации;

г) целостностью

3. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности;

б) обрабатывать большой объем программной информации;

в) нет правильного ответа

4. Конфиденциальную информацию можно разделить:

а) предметную;

б) служебную;

в) глобальную

5. По каким компонентам классифицируется угрозы доступности:

а) отказ пользователей;

б) отказ поддерживающей инфраструктуры;

в) ошибка в программе

6. Основными источниками внутренних отказов являются:

а) отступление от установленных правил эксплуатации;

б) разрушение данных;

в) все ответы правильные

7. Правовое обеспечение безопасности информации делится:

а) международно-правовые нормы;

б) национально-правовые нормы;

в) все ответы правильные

8. К случайным не относится угроза:

а) ошибка персонала;

б) ошибка автоматизированных систем;

в) форс-мажор;

г) программы закладки

9. Программой-закладной называют вирус

а) размножающий себя на ПК;

б) приводящий к временному изменению ссылок на программы;

в) выдающий себя за какую-либо полезную программу;

г) активируется при нажатии сочетании клавиш

10. Организационные требования к системе защиты

а) административные и процедурные;

б) административные и аппаратурные;

в) управленческие и идентификационные;

г) аппаратурные и физические

11. Наукой, изучающей математические методы защиты информации путем ее преобразования, является

а) криптоанализ;

б) криптология;

в) стеганография;

г) криптография

12. Какие средства используется на инженерных и технических мероприятиях в защите информации:

а) аппаратные;

б) криптографические;

в) физические

13. Процесс имитации хакером дружественного адреса называется

а) «крэком»;

б) проникновением;

в) взломом;

г) «спуфингом»

14. Цель процесса внедрения и тестирования средств защиты —

а) определить уровень расходов на систему защиты;

б) выявить нарушителя;

в) гарантировать правильность реализации средств защиты;

г) выбор мер и средств защиты

15. За соблюдением ИБ на сетевой инфраструктуре отвечает

а) начальник службы информационной безопасности;

б) директор;

в) системный администратор;

г) начальник службы безопасности

16. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков;

б) анализ затрат / выгоды;

в) результаты ALE;

г) выявление уязвимостей и угроз, являющихся причиной риска

Вариант 6

1. Шаблон проекта экономической информационной системы – это

а) форма ввода данных;

б) интерфейс экономической информационной системы;

в) типовой проект экономической информационной системы;

г) база данных экономической информационной системы.

2. Взаимодействие с глобальными ресурсами других организаций определяет уровень операционной системы

а) системный;

б) внешний;

в) приложений;

г) сетевой

3. По доступности информация классифицируется на

а) открытую информацию и государственную тайну;

б) конфиденциальную информацию и информацию свободного доступа;

в) виды информации, указанные в остальных пункта;

г) информацию с ограниченным доступом и общедоступную информацию

4. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство

а) восстанавливаемость;

б) детермированность;

в) целостность;

г) доступность

5. Отказ, ошибки, сбой – это:

а) природные угрозы;

б) преднамеренные угрозы;

в) случайные угрозы

6. Программные средства – это…

а) специальные программы и системы защиты информации в информационных системах различного назначения;

б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла;

в) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

7. Удаление вируса при помощи антивируса, запущенного с локальной машины — это способ защиты

а) комплексный;

б) фрагментальный;

в) целостный;

г) административный

8. Безусловной атакой является атака, когда

а) пользователь принес вирус на дискете;

б) пользователь открыл зараженное письмо, которое парализовало работу на компьютере;

в) злоумышленник открыто похитил диск с информацией, оставленный без присмотра;

г) на ПК обнаружен вирус, передающий информацию в Интернет

9. Первым этапом разработки системы защиты ИС является

а) анализ потенциально возможных угроз информации;

б) изучение информационных потоков;

в) стандартизация программного обеспечения;

г) оценка возможных потерь

10. Удачная криптоатака называется

а) раскрытием шифра;

б) проникновением;

в) взломом;

г) вскрытием

11. Какие существуют грани вредоносного программного обеспечения (ПО)?

а) вредоносная функция;

б) внешнее представление;

в) способ распространения

12. На flash-носителе обнаружен вирус, подобный вирус обнаружен на сервере в профиле пользователя. Кто будет нести ответственность за нарушение ИБ?

а) пользователь;

б) директор фирмы;

д) системный администратор;

г) начальник службы безопасности

13. Для создания базы данных пользователь должен получить привилегию от:

а) администратора сервера баз данных;

б) системного администратора;

в) сетевого администратора;

г) старшего пользователя своей группы

14. Надежность СЗИ определяется

а) усредненным показателем;

б) самым слабым звеном;

в) количеством отраженных атак;

г) самым сильным звеном

15. Недостатком многоуровневых моделей безопасности является

а) сложность представления широкого спектра правил обеспечения безопасности;

б) отсутствие полного аудита;

в) отсутствие контроля за потоками информации;

г) невозможность учета индивидуальных особенностей субъекта

16. Основополагающие документы для обеспечения безопасности внутри организации:

а) трудовой договор сотрудников;

б) должностные обязанности руководителей;

в) коллективный договор

СПИСОК ИСТОЧНИКОВ

Основная

1. Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. - Москва: Прометей, 2018. - 173 с. (ЭБС «Университетская библиотека онлайн»).

2. Кияев, В. И. Безопасность информационных систем: курс / В. Кияев, О. Граничин. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. (ЭБС «Университетская библиотека онлайн»).

3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров. - Санкт-Петербург: Изд-во Политехнического ун-та, 2014. - 322 с. (ЭБС «Университетская библиотека онлайн»).

4. Богомолов, В. А. Экономическая безопасность: учеб. пособие / В. А. Богомолов, Н. Д. Эриашвили, Е.Н. Барикаев [и др.]. - 2-е изд., перераб. и доп. - Москва: ЮНИТИ-ДАНА, 2012. - 296 с. (ЭБС «Университетская библиотека онлайн»).

Дополнительная

5. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие для вузов / В. И. Аверченков. - 3-е изд., стер. - Москва: Изд-во «Флинта», 2016. - 269 с. (ЭБС «Университетская библиотека онлайн»).

6. Аверченков, В. И. Служба защиты информации: организация и управление: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стер. - Москва: Изд-во «Флинта», 2016. - 186 с. (ЭБС «Университетская библиотека онлайн»).

7. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учеб. пособие / Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с. (ЭБС «Университетская библиотека онлайн»).

8. Петренко, В. И. Теоретические основы защиты информации: учеб. пособие / В.И. Петренко. - Ставрополь: СКФУ, 2015. - 222 с. (ЭБС «Университетская библиотека онлайн»).

9. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учеб. пособие / В. А. Сердюк. - Москва: Изд. дом Высшей школы экономики, 2015. - 574 с. (ЭБС «Университетская библиотека онлайн»).

10. Скрипник, Д. А. Общие вопросы технической защиты информации / Д. А. Скрипник. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. (ЭБС «Университетская библиотека онлайн»).

11. Сычев, Ю. Н. Основы информационной безопасности: учеб.-практ. пособие / Ю. Н. Сычев. - Москва: Евразийский открытый институт, 2010. - 328 с. (ЭБС «Университетская библиотека онлайн»).

Интернет-ресурсы:

12. "Росстат" [Электронный ресурс]. – Электрон. дан. – Режим доступа: www.gks.ru.

13. Журнал "Защита информации. Инсайд" [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.inside-zi.ru.

14. Журнал "Специальная техника" [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.st.ess.ru.

15. Журнал по исследованию рисков [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://taylorandfrancis.com/

16. КонсультантПлюс: офиц. сайт [Электронный ресурс]. – Электрон. дан. – Режим доступа: www.consultant.ru.

17. Образовательная среда КГТУ [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://eios.klgtu.ru/

18. Образовательный портал [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://economics.edu.ru.

19. Открытая ассоциация по риск-менеджменту [Электронный ресурс]. – Электрон. дан. – Режим доступа: www.primacentral.org

20. Средства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации. [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.analitika.info.

21. Федеральная служба безопасности Российской Федерации [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.fsb.ru.

22. Центр по лицензированию, сертификации и защите [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://clsz.fsb.ru.

Локальный электронный методический материал

Роберт Альбертович Мнацаканян

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Редактор Э. С. Круглова

Уч.-изд. л. 5,5 Печ. л. 5,0

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1