Федеральное государственное бюджетное образовательное учреждение
высшего образования
"КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ"

Институт отраслевой экономики и управления

Р. А. Мнацаканян

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ СУБЪЕКТА ЭКОНОМИКИ

Учебно-методическое пособие по изучению дисциплины для студентов
по направлению подготовки 38.05.01 Экономическая безопасность

Калининград
Издательство ФГБОУ ВО "КГТУ"
2023

УДК 004.056.5

Рецензент
кандидат экономических наук, доцент кафедры экономики и финансов ИНОТЭКУ ФГБОУ ВО "Калининградский государственный технический университет" Т. В. Романова

Мнацаканян, Р. А.
Обеспечение информационной и технической безопасности субъекта экономики: учеб.-метод. пособие по изучению дисциплины для студентов специальности 38.05.01 Экономическая безопасность / Р. А. Мнацаканян. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. - 47 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 к промежуточной аттестации, выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины "Обеспечение информационной и технической безопасности субъекта экономики" по специальности 38.05.01 Экономическая безопасность.
Табл. 3, список лит. – 22 наименования

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой экономической безопасности 31.08.2023 г., протокол № 01
Учебно-методическое пособие по изучению дисциплины рекомендовано к изданию в качестве локального электронного методического материала для использования в учебном процессе методической комиссией ИНОТЭКУ ФГБОУ ВО «КГТУ» 22.09.2023 г., протокол № 11

УДК 004.056.5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Дисциплина "Обеспечение информационной и технической безопасности субъекта экономики" является дисциплиной обязательной части учебного плана, формирующей у обучающихся способность решать стандартные задачи профессиональной деятельности на основе применения информационных ресурсов и технологий и с учётом основных требований информационной и технической безопасности.

Настоящее учебно-методическое пособие представляет собой комплекс систематизированных материалов по самостоятельному изучению дисциплины "Обеспечение информационной и технической безопасности субъекта экономики ".

Дисциплина "Обеспечение информационной и технической безопасности субъекта экономики" − фундаментальная экономическая дисциплина, опирающаяся на знания, приобретенные в результате освоения таких дисциплин, как "Информационные системы в экономике", "Управление организацией и технологии обеспечения безопасности", "Экономическая безопасность хозяйствующих субъектов", и является базой для получения знаний, умений и навыков, необходимых при изучении таких дисциплин и практик, как: "Информационная безопасность", "Мониторинг и предупреждение рисков экономической безопасности", "Отраслевая политика экономической безопасности в продовольственном секторе", "Стратегические аспекты экономической безопасности", "Финансовая безопасность", " Оценка и экспертиза инвестиционных проектов продовольственного сектора", "Экономическая безопасность в системе внешнеэкономических связей", "Диагностика экономической безопасности в продовольственном сектор", "Производственная практика"

Учебно-методическое пособие составлено в соответствии с утвержденной рабочей программой дисциплины "Обеспечение информационной и технической безопасности субъекта экономики" по специальности 38.05.01 Экономическая безопасность.

Целью освоения дисциплины "Обеспечение информационной и технической безопасности субъекта экономики" является формирование у студентов современных фундаментальных знаний в сфере построения информационных систем, обеспечивающих техническую поддержку безопасности субъекта экономики.

Задачами дисциплины "Обеспечение информационной и технической безопасности субъекта экономики " являются:

- изучение понятийного аппарата теории экономической безопасности субъектов экономики в части информационной и технической безопасности;
- основные положения нормативно-законодательной базы, регулирующей информационную безопасность субъектов экономики, а также требования к технической безопасности;
- умение классифицировать и анализировать угрозы информационной безопасности для субъектов экономики, защиту которых можно обеспечить за счёт современных технологий и технических средств;
- освоение этапов, методик, технологий и технических средств, необходимых для проведения аналитической работы в сфере безопасности информационных ресурсов субъектов экономики;
- изучение механизмов, методов и технических средств защиты информационных систем и их элементов с использованием современных информационных технологий, и технических средств, адаптированных к субъекту экономики;
- формирование концептуального подхода на уровне постановки задач для разработки и внедрения технических систем, обеспечивающих информационную безопасность субъекта экономики;
- формирование компетенции, необходимой для работы с различными информационными и техническими ресурсами и технологиями по обеспечению безопасности субъекта экономики, для выявления и предотвращения угроз экономической безопасности.

Планируемые результаты освоения дисциплины "Обеспечение информационной и технической безопасности субъекта экономики" заключаются в том, что студент должен:

***знать*:**

- категорию "субъект экономики" и его типологию;
- понятие "информационная безопасность" и требования, предъявляемые к ней, в том числе с позиции нормативно-законодательной базы, действующей в РФ, применительно к субъекту экономики;
- носители информации;
- классификацию средств защиты;
- понятия информационных ресурсов и технологий;
- требования информационной и технической безопасности субъекта экономики;
- основные положения международного стандарта ISO/IEC 15408 по оценке защищенности информационных систем;
- состав автоматизированной информационной системы;

- требования безопасности к информационным системам;
- особенности обеспечения информационной безопасности в компьютерных сетях;
- технический уровень обеспечения информационной безопасности субъекта экономики программно-техническим уровнями формирования режима информационной безопасности;

***уметь*:**

- распознавать ключевые угрозы и средства защиты информации;
- проводить аналитическую работу в сфере безопасности информационных ресурсов;
- с позиции системного подхода комплексно использовать, в том числе компьютерных систем (КС): организационно-правовой и инженерно-технической методы защиты информации, криптографические и программно-аппаратные методы и средства защиты информации;

***владеть*:**

- современными технологиями и техническими средствами обеспечения информационной безопасности субъекта экономики;
- механизмами обеспечения информационной и технической безопасности субъекта экономики;
- алгоритмами реализации программно-аппаратных методов и средств защиты ин формации для субъекта экономики.

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 и 2.

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

Номер и наименование темы	**Объем учебной работы, ч**	
	Лекции	**ПЗ**
Семестр – 6, трудоемкость – 2 ЗЕТ (72 ч)		
1. Проблема информационной и технической безопасности для субъектов экономики	2	2
2. Составляющие информационной и технической безопасности	2	2
3. Классификация угроз информационной и технической безопасности	2	2
4. Технологии, методы, технические средства, механизмы обеспечения информационной безопасности	6	6
5. Экономическая эффективность обеспечения информационной и технической безопасности субъекта экономики	4	4
Подготовка к сдаче и сдача зачета	-	-
Всего в шестом семестре	16	16
	32	

В этом же семестре проводится промежуточная аттестация в форме зачета.

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

Номер и наименование темы	**Объем учебной работы, ч**	
	Лекции	**ПЗ**
Семестр – 8, трудоемкость – 2 ЗЕТ (72 ч)		
1. Проблема информационной и технической безопасности для субъектов экономики	0,5	-
2. Составляющие информационной и технической безопасности	0,5	-
3. Классификация угроз информационной и технической безопасности	0,5	-
4. Технологии, методы, технические средства, механизмы обеспечения информационной безопасности	0,5	2
5. Экономическая эффективность обеспечения информационной и технической безопасности субъекта экономики	-	2
Подготовка к сдаче и сдача зачета	-	-
Всего в восьмом семестре	2	4
	6	

В восьмом семестре студентами заочной формы обучения выполняется контрольная работа и проводится промежуточная аттестация в форме зачета.

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

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 зачета. 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 пятью тематическими блоками (темами):

Тема 1. Проблема информационной и технической безопасности для субъектов экономики

Содержание темы

Цель и задачи дисциплины; Место дисциплины в структуре образовательной программы; Планируемые результаты освоения дисциплин.

Понятие и сущность; функции основных субъектов рыночной экономики; модели взаимодействия субъектов рыночных отношений.

Определения и толкования понятия и сущности информационной и технологической безопасности и её составляющих; информация как субъект управления; защита информации; информационная безопасность как составная часть информационных технологий; понятие компьютерной безопасности; пути решения проблемы информационной безопасности.

Методические указания

Цель темы - получить представление о жизнедеятельности "субъекта экономики" в системе экономических отношений и в информационной среде общества, а также информационной безопасности как составной части информационных технологий.

В результате изучения темы будут получены знания, позволяющие раскрыть сущность информационной безопасности и её составляющих, содержание информации как субъекте управления и определить пути решения проблемы информационной безопасности.

В процессе изучения темы следует обратить внимание на то, что информационная безопасность является составной частью информационных технологий.

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. Составляющие информационной и технической безопасности

Содержание темы

Принципы обеспечения безопасности: доступность, целостность, конфиденциальность информации. Система формирования режима информационной безопасности: задачи информационной безопасности общества и субъектов экономики; уровни формирования режима информационной безопасности (законодательно-правовой, административный, программно-технический).

Методические указания

Цель темы - получить представление о содержании и назначении составляющих информационной безопасности.

В результате изучения темы будут получены знания, позволяющие выявить специфические принципы обеспечения безопасности, а также особенности формирования режима информационной безопасности.

В процессе изучения темы следует особое внимание обратить на различные инструменты обеспечения режима информационной безопасности.

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. Классификация угроз информационной и технической безопасности

Содержание темы

Основные носители информации; обозначения, используемые в курсе; понятие информационной системы; безопасность информации; наиболее распространенные угрозы ин формационной безопасности и их классификация; способы воздействия угроз на информационные объекты.

Методические указания

Цель темы - получить представление о критериях и признаках классификации угроз информационной и технической безопасности.

В результате изучения темы будут получены знания, позволяющие идентифицировать угрозы информационной и технической безопасности по разным признакам структуризации.

В процессе изучения темы следует особое внимание обратить на способы воздействия угроз на информационные объекты.

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, методы, технические средства, механизмы обеспечения информационной безопасности

Содержание темы

Вредоносное программное обеспечение. Категории вредоносных программ. Признаки наличия вредоносного программного обеспечения. Классификация вредоносного программного обеспечения. Основные классы вирусов, способы заражения, особенности алгоритма вируса, механизмы распространения.

Аппаратные средствам защиты информации. Основные программные средства защиты информации. Примеры основных и вспомогательных аппаратных средств защиты информации. Информационная безопасность вычислительных сетей.

Методические указания

Цель темы - получить представление о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности.

В результате изучения темы будут получены знания отличать вредоносное программное обеспечение от нормальной, а также разных методах защиты информации.

В процессе изучения темы следует уяснить, что для борьбы с вирусами необходимо владеть инструментами, позволяющими вычислить способы заражения, алгоритмы самих вирусов и способы распространения

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: [1-11].

Тема 5. Экономическая эффективность обеспечения информационной и технической безопасности субъекта экономики

Содержание темы

Понятие экономической эффективности обеспечения информационной безопасности. Факторы, влияющие на уровень защиты информации. Определение и методики расчёта экономической эффективности защиты информации

Методические указания

Цель темы - получить представление о об инструментарии, позволяющему рассчитать экономическую эффективность обеспечения информационной безопасности субъекта экономики.

В результате изучения темы будут получены знания о методах расчета экономической эффективности обеспечения информационной безопасности субъекта экономики.

В процессе изучения темы следует уяснить, что можно использовать разные походы к расчету экономической эффективности обеспечения информационной безопасности субъекта экономики.

Методические материалы по теме 5

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 5: [1-9, 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 "Обеспечение информационной и технической безопасности субъекта экономики", 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 компьютерной техники.

Занятие по теме 1. Проблема информационной и технической безопасности для субъектов экономики

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций.
2. Работа с тестом.

Вопросы:

1. Функции основных субъектов рыночной экономики;
2. Модели взаимодействия субъектов рыночных отношений;
3. Понятие и сущность информационной безопасности и её составляющих;
4. Информация как субъект управления;
5. Защита информации;
6. Информационная безопасность как составная часть информационных технологий;
7. Компьютерная безопасность;
8. Пути решения проблемы информационной безопасности.

Занятие по теме 2. Составляющие информационной и технической безопасности

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций.
2. Работа с тестом.

Вопросы:

1. Принципы обеспечения безопасности;
2. Доступность информации;
3. Целостность информации;

4. Конфиденциальность информации;

5. Система формирования режима информационной безопасности;

6. Задачи информационной и технологической безопасности общества и субъектов экономики;

7. Уровни формирования режима информационной безопасности.

Занятие по теме 3. Классификация угроз информационной и технической безопасности

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций.

2. Работа с тестом.

Вопросы:

1. Основные носители информации;

2. Понятие информационной системы;

3. Безопасность информации;

4. Технической обеспечение информационной безопасности;

5. Угрозы информационной безопасности и их классификация;

6. Способы воздействия угроз на информационные объекты.

Занятие по теме 4. Технологии, методы, технические средства, механизмы обеспечения информационной безопасности

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций.

2. Работа с тестом.

Вопросы:

1. Категории вредоносных программ;

2. Признаки наличия вредоносного программного обеспечения;

3. Классификация вредоносного программного обеспечения;

4. Признаки наличия вредоносного программного обеспечения;

5. Основные классы вирусов;

6. Способы заражения;

7. особенности алгоритма вируса;

8. механизмы распространения;

9. Аппаратные средствам защиты информации;

10. Основные программные средства защиты информации;

11. Примеры основных и вспомогательных аппаратных средств защиты информации;

12. Информационная безопасность вычислительных сетей.

Занятие по теме 5. Экономическая эффективность обеспечения информационной и технической безопасности субъекта экономики

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций.

2. Работа с тестом.

Вопросы:

1. Понятие экономической эффективности обеспечения информационной и технической безопасности;

2. Факторы, влияющие на уровень защиты информации;

3. Методики расчёта экономической эффективности защиты информации.

3 Задания и методические указания по выполнению контрольной работы

3.1 Общие сведения, выбор варианта

В соответствии с рабочей программой дисциплины "Обеспечение информационной и технической безопасности субъекта экономики" 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 одного раздела. Он представляет собой письменное изложение двух теоретических вопросов.

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, установленной графиком учебного процесса.

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

Выбор варианта осуществляется в соответствии со списком студентов.

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 по вариантам с заданиями на их выполнение

Вариант 1.

1. Современные угрозы информационной безопасности в России.

2. На примере конкретного предприятия разработать SWOT-матрицу с перечнем и оценкой экономической безопасности субъекта экономики по критериям: "угрозы", "возможности", "сильные стороны", "слабые стороны".

Вариант 2.

1. Информационные ресурсы (информация) как объекты отношений субъектов экономики (физических и юридических лиц между собой и государством).

2. Привести методику количественного расчета экономического эффекта от мероприятий по обеспечению информационной безопасности экономического субъекта.

Вариант 3.

1. Финансовая грамотность как один из аспектов обеспечения безопасности индивида и домашнего хозяйства.

2. Разработать и охарактеризовать структуру "модель угроз" для предприятия (на конкретном примере).

Вариант 4.

1. Системный подход к обеспечению информационной безопасности.

2. Разработать структуру "Профиля защиты" предприятия для обеспечения его информационной безопасности (на конкретном примере).

Вариант 5.

1. Основные положения Стандарта ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".

2. Прокомментировать причины массовых ошибок в принятии финансовых решений экономических субъектов.

Вариант 6.

1. Информация как важнейший фактор производства и как товар.

2. Факторы, влияющие на уровень информационной безопасности субъекта экономики, и их количественная и качественная оценка (привести методику оценки).

Вариант 7.

1. Информационное противоборство, информационная преступность, информационное воздействие.

2. Модели взаимодействия субъектов рыночных отношений – изобразить графически и охарактеризовать.

Вариант 8.

1. Субъекты экономики в системе экономических отношений общества. Функции основных субъектов экономики.

2. Перечислить и охарактеризовать признаки наличия вредоносного программного обеспечения и какой ущерб оно наносит.

Вариант 9.

1. Информационная война и информационное оружие.

2. В чём проявляется информационный аспект финансовой безопасности домохозяйства?

Вариант 10.

1. Информация, относящаяся к коммерческой тайне. Законодательные акты РФ о коммерческой тайне.

2. Перечислить финансовые продукты, предназначенные для вкладчиков-физических лиц, в порядке возрастания риска.

Вариант 11.

1. Ответственность за нарушения в сфере информационной безопасности.

2. Количественно оценить и изобразить на графике зависимость уровня риска от стоимости системы защиты информации (на примере экономического субъекта).

Вариант 12.

1. Стандарты информационной безопасности: "Общие критерии".

2. Привести и пояснить смысл расчета экономического эффекта от эффективной системы защиты информации

Вариант 13.

1. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.

2. Привести и пояснить смысл формул расчета ущерба, наносимого незащищённой информационной системы субъекта экономики

Вариант 14.

1. Наиболее распространенные угрозы информационной безопасности экономическому субъекту, классификация угроз.

2. Привести и пояснить смысл формулы расчета риска для незащищенной информационной системы.

Вариант 15.

1. Принципы правовой защиты экономического положения человека как имманентного субъекта домохозяйства.

2. Привести и пояснить смысл формулы расчета экономической эффективности коэффициента защищённости системы информации.

Вариант 16.

1. Положение "Сертификация средств защиты информации по требованиям безопасности информации"

2. Основные программные средства защиты информации.

Вариант 17.

1. Механизмы распространения вирусов и способы заражения компьютерных сетей.

2. Изобразите графически информационную систему организации и поясните её функционирование (на конкретном примере). Какие факторы влияют на её уровень безопасности?

Вариант 18.

1. Система формирования режима информационной безопасности субъекта экономики.

2. С помощью каких статистических показателей можно проанализировать информационную и техническую безопасность субъекта экономики. Как они рассчитываются?

Вариант 19.

1. Система формирования режима технической безопасности субъекта экономики.

2. Изобразите структуру локальной информационной сети (на примере конкретной организации) и что необходимо для её защиты?

Вариант 20.

1. Идентификация и аутентификация как процедуры ограничения доступа случайных и незаконных субъектов

2. Почему большие масштабы бедности населения представляют угрозу национальным интересам и безопасности России?

4 Методические указания по подготовке к промежуточной аттестации

Промежуточная (заключительная) аттестация по дисциплине проводится в форме зачета**.**

К зачету допускаются студенты:

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

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

- положительно аттестованные по результатам проведенного тестирования.

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

Зачетная оценка ("зачтено", "не зачтено") выставляется по результатам выполнения практических работ студента в семестре и положительно оценённой контрольной работе.

Критерии оценивания зачета 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 3 – 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

Система оценок / Критерий	2	3	4	5
	0-40 %	**41-60 %**	**61-80 %**	**81-100 %**
	"неудовлетворительно"	**"удовлетворительно"**	**"хорошо"**	**"отлично"**
	"не зачтено"	**"зачтено"**		
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
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 зачета, соответственно относятся вопросы для проведения промежуточной аттестации (зачета).

Контрольные вопросы, при необходимости, могут быть использованы для проведения аттестации в форме зачета.

Перечень контрольных вопросов

1. Субъекты экономики в системе экономических отношений общества, их место, роль и функции в социально-экономической системе общества.
2. Общая модель взаимодействия субъектов экономики. Принципы и основные факторы взаимодействия.
3. Информация как важнейший фактор производства и как товар.
4. Информационные ресурсы (информация) как объекты отношений субъектов экономики (физических и юридических лиц между собой и государством).
5. Прогресс информационных технологий и необходимость обеспечения безопасности.
6. Основные понятия информатизации общества и информационной безопасности.

7. Экономическая информация как товар и объект безопасности.

8. Современные угрозы информационной безопасности в России.

9. Государственное регулирование информационной безопасности. Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

10. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".

11. ГОСТ 350922-96 О защите информации.

12. Ответственность за нарушения в сфере информационной безопасности.

13. Типы международных организаций в сфере информационной безопасности.

14. Системный подход к обеспечению информационной безопасности.

15. Объекты информационной безопасности в компании.

16. Обеспечивающие компоненты системы защиты информации.

17. Объектно-ориентированный подход к обеспечению информационной безопасности: сущность, преимущества и недостатки метода.

18. Перечень сведений, относящихся к коммерческой тайне. Объекты банковской тайны.

19. Принципы обеспечения информационной безопасности: конфиденциальность, целостность, доступность и их взаимосвязь.

20. Решение проблемы информационной безопасности.

21. Различие задач по обеспечению информационной безопасности для разных категорий субъектов экономики.

22. Уровни формирования режима информационной безопасности.

23. Сетевая безопасность. Аутентификация. Авторизация. Аутентичность.

24. Законодательные акты по защите информации.

25. Понятие информационной безопасности домохозяйства как субъекта экономики, методы и средства её обеспечения.

26. "Информационная безопасность" как "компьютерная безопасность".

27. Перечень и характеристика случайных угроз и преднамеренных угроз.

28. Способы воздействия угроз на информационные объекты.

29. Перечислить виды возможных нарушений информационной системы.

30. Действия и события, нарушающие информационную безопасность.

31. Основные виды каналов утечки информации.

32. Пути несанкционированного доступа к информации.

33. Стратегия и тактика злоумышленника при несанкционированном доступе.

34. Наиболее распространенные угрозы информационной безопасности и их классификация.

35. Способы воздействия угроз на информационные объекты.

36. Личностно-профессиональные характеристики сотрудников, способствующие реализации информационных угроз.

37. Вред от реализованной угрозы.

38. Вредоносные программы, их виды.

39. Признаки воздействия вирусов на компьютерную систему и механизмы их распространения.

40. Компьютерные преступления и их классификация.

41. Субъекты компьютерных преступлений.

42. Объективная сторона компьютерных преступлений.

43. Уголовно-правовой контроль над компьютерной преступностью в России.

44. Уголовно-правовая характеристика компьютерных преступлений.

45. Статьи 272, 273, 274 УК о компьютерных преступлениях.

46. Категории и виды вредоносных программ.

47. Меры предупреждения преступлений в сфере компьютерной информации.

48. Признаки воздействия вирусов на компьютерную систему.

49. Организация системы защиты информации в экономических системах.

50. Гарантия выбора и внедрения средств криптографической защиты информации.

51. Типовая методика испытаний объектов информатики по требованиям безопасности информации.

52. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.

53. Ранжирование финансовых институтов по степени риска для вкладчиков.

54. Методика расчёта экономической эффективности выбранных средств защиты информации.

55. Оценка эффективности инвестиций в информационную безопасность.

56. Аппаратные средства защиты информации.

57. Программные средства защиты информации.

58. Технические средства защиты информации

59. Комплексная система информационной безопасности субъектов экономики (на примере).

60. Финансовая грамотность как составляющая экономической безопасности индивида и домохозяйства.

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).

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 – знания основных финансовых и денежно-кредитных методов регулирования экономики (Приложение 1). ?

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. Собственниками информации могут быть (укажите правильные ответы):

а) государство; б) юридическое лицо; в) группа физических лиц; г) отдельное физическое лицо; д) домохозяйство.

2. Целостность информации для обеспечения информационной безопасности – это:

а) это гарантия получения требуемой информации или информационной услуги пользователем за определенное время; б) гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена; в) гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

3. Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением задач:

а) Обеспечением доступности информации; б) Обеспечением целостности информации; в) Обеспечением конфиденциальности информации.

4. Потенциальная возможность определенным образом нарушить информационную безопасность – это:

а) угроза; б) атака; в) взлом.

5. Источник угрозы безопасности информации:

а) Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации; б) Фактор, воздействующий на защищаемую информацию; в) Явление, действие или процесс, результатом которого могут

быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

6. Сертификация на соответствие требованиям по безопасности информации – это:

а) Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ; б) Прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации; в) Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами и условиями договоров.

7. Вирус — это:

а) отдельный файл, который размножается (воспроизводит себя), не заражая другие файлы; б) код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы); в) код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

8. Особенности алгоритма "вирусов-"червей":

а) Перехватывают обращения операционной системы к пораженным файлам или секторам и подставляют вместо себя незараженные участки; б) Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса; в) Не имеют ни одного постоянного участка кода, трудно обнаруживаемы, основное тело вируса зашифровано; г) Вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением com.

9. К аппаратным средствам защиты информации не относятся:

а) механические; б) электрические; в) электронные; г) программные; д) радиолокационные.

10. Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности, являются:

а) уязвимым местом; б) окном опасности; в) окном безопасности; г) источником угрозы.

11. Законодательный уровень информационной безопасности предусматривает:

а) формирование программы работ в области информационной безопасности и обеспечение ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел; б) контроль компьютерных сущностей -

оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности; в) направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности); г) минимизацию привилегий, которая предписывает выделять пользователям толь- ко те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно - уменьшить ущерб от случайных или умышленных некорректных действий.

12. К организационным методам обеспечения информационной безопасности в зависимости от способа их реализации относятся:

а) реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т. д.; б) которые подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей; в) по защите информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т. д.). Без использования программной составляющей практически невыполнимы никакие, в том числе и первые три группы методов (то есть в чистом виде организационные, технологические и аппаратные методы защиты, как правило, реализованы быть не могут — все они содержат программный компонент).

13. По расположению источника угрозы подразделяется на внутренние и внешние. К внутренним угрозам относятся (выбрать):

а) внедрение в атакуемые системы вредоносного программного обеспечения; б) нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности); в) невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.).

14. К программным средствам защиты информации не относится:

а) программы шифрования информации; б) программы защиты информационных ресурсов от несанкционированного изменения, использования и копирования; в) программы разграничения доступа

пользователей к ресурсам компьютерных систем; г) устройства для шифрования информации.

15. Средство защиты информации — это:

а) Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации; б) Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации; в) Средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

16. Фактор, воздействующий на защищаемую информацию – это:

а) Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации; б) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации; в) Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

17. Причины массовых ошибок в принятии финансовых решений экономических субъектов (выбрать правильное):

а) неумение адекватно оценивать риски; б) отсутствие долгосрочных стратегий семейного бюджета – чаще всего решения принимаются спонтанно, под действием примера, слухов или рекламы; в) недоступность профессионального финансового консультирования для подавляющего большинства граждан; г) "непрозрачность" для населения финансовой политики ключевых институтов и государственных решений, отсутствие разъяснительной работы; д) недобросовестная реклама потребительского кредита, ипотеки, финансовых услуг; е) всё перечисленное.

Вариант 2

1. Вставьте пропущенный термин. "Под информационной безопасностью будем понимать защищенность информации и …….[ответ] от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры":

а) поддерживающей инфраструктуры; б) человека; в) конфиденциальных данных.

2. Непосредственный вред от реализованной угрозы, называется:

а) воздействием угрозы; б) нанесением ущерба; в) уязвимым местом защиты; г) непреднамеренной ошибкой пользователя.

3. Принуждение как метод обеспечения защиты информации на предприятии – это:

а) метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.); б) метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму; в) метод защиты информации, который побуждает пользователей, и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм; г) метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

4. Программно-технический уровень формирования режима информационной безопасности включает подуровни:

а) физический; б) технический (аппаратный); в) программный.

5. Ошибки администрирования системы с точки зрения информационной безопасности являются:

а) уязвимым местом; б) окном опасности; в) окном безопасности; г) источником угрозы.

6. Окном опасности называется:

а) это потенциальная возможность определенным образом нарушить информационную безопасность; б) промежуток времени от момента, когда появляется возможность использовать слабое место, ассоциированным с данным уязвимым местом, и до момента, когда пробел ликвидируется; в) потенциальные злоумышленники; г) попытка реализации угрозы.

7. Возможность за приемлемое время получить требуемую информационную услугу называется:

а) доступностью информации; б) целостностью информации; в) предоставлением информации.

8. К аппаратным средствам обеспечения информационной безопасности относятся:

а) специальное программное обеспечение, используемое для защиты информации, например, антивирусный пакет и т. д.; б) схемы контроля информации по четкости, схемы доступа по ключу и т. д.; в) комплекс взаимокоординируемых мероприятий и технических мер, реализующих

практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.

9. Программно-математические способы воздействия угроз на информационные объекты включают:

а) уничтожение или разрушение средств обработки информации и связи; б) перехват информации в технических каналах ее возможной утечки; в) нарушение технологии обработки информации; г) уничтожение или модификацию данных в автоматизированных информационных системах.

10. Особенности алгоритма вирусов-призраков:

а) Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса; б) Изменяют содержимое дисковых секторов или файлов; в) Не имеют ни одного постоянного участка кода, трудно обнаруживаемы, основное тело вируса зашифровано; г) Перехватывают обращения операционной системы к пораженным файлам или секторам и подставляют вместо себя незараженные участки.

11. "червь" — это:

а) код, способный самостоятельно, т. е. без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы); б) код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы; в) код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы.

12. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:

а) утечкой; б) разглашением; в) взломом.

13. Эффективность информационного сервиса может измеряться как:

а) количество одновременно обслуживаемых пользователей; б) максимальное время обслуживания запроса; в) рентабельность работы сервиса.

14. К основным программным средствам защиты информации относится:

а) программы идентификации и аутентификации пользователей компьютерных сетей; б) программы аудита; в) программы уничтожения остаточной информации; г) программы тестового контроля защищенности компьютерных сетей.

15. Финансовая защищенность — это:

а) уровень экономической безопасности, при котором уровень пассивных доходов позволяет наращивать личный капитал.

б) уровень экономической безопасности, позволяющий поддерживать привычный уровень расходов при потере постоянного источника доходов на протяжении 6 (иногда 12) месяцев; в) самый простой уровень экономической безопасности домохозяйства, характеризующийся возможностью поддерживать привычный образ жизни;

16. Критерии экономической безопасности домохозяйства (выбрать):

а) удовлетворенность качеством жизни и уверенность в будущем; б) устойчивость к информационным, экономическим и политическим влияниям; в) защищённость базовых ценностей и интересов, источников духовного и материального благосостояния; г) контроль за соблюдением правовых и общественных норм защиты экономического положения человека д) удовлетворенность состоянием собственной экономической безопасности.

17. В современном мире сбережение и инвестирование является (*вставить пропущенное*) рациональным поведением, чем потребление.

а) менее; б) более; в) не.

Вариант 3

1. Экономические отношения: 1) объективно складывающиеся отношения между экономическими агентами при производстве, распределении, обмене и потреблении благ; 2) материально-опосредованные отношения, складывающиеся в процессе производства, обмена, распределения и потребления; 3) объективно складывающиеся отношения между людьми по поводу производства, распределения, обмена и потребления благ, в особенности — продуктов труда. Сделайте правильный выбор.

а) 1,2,3; б) 1; в) 1,3; г) 2.

2. Основными носителями информации являются:

а) открытая печать (газеты, журналы, отчеты, реклама и т. д.); б) люди; в) средства связи (радио, телевидение, телефон, пейджер и т. д.); г) документы (официальные, деловые, личные и т. д.); д) электронные, магнитные и другие носители, пригодные для автоматической обработки данных.

3. Информация – это (выбрать ответ):

а) разъяснение, представление, понятие о чём-либо; б) знания, сведения необходимые для принятия решений; в) это вся совокупность сведений об окружающем нас мире, о всевозможных протекающих в нем процессах, которые могут быть восприняты живыми организмами, электронными машинами и другими информационными системам; г) все утверждения правильные.

4. Модель угроз (безопасности информации) — это:

а) Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; б) Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации; в) Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы; г) Недостаток или слабое место в информационной системе.

5. К уровням формирования режима информационной безопасности относятся:

а) законодательно-правовой; б) административный (организационный); в) программно-технический.

6. Конфиденциальность информации для обеспечения информационной безопасности – это:

а) гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; б) гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена; в) это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

7. Мониторинг безопасности информации

а) Периодический независимый и документированный процесс получения свидетельств аудита и объект ивой оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности; б) Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение; в) Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

8. К программным средствам защиты информации относятся:

а) законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений; б) схемы контроля информации по четкости, схемы доступа по ключу и т. д.; в) специальное

программное обеспечение, используемое для защиты информации, например, антивирусный пакет и т. д.

9. Внедрение компьютерных вирусов относится к способу воздействия угроз на информационные объекты:

а) к информационным способам; б) к физическим способам; в) к радиоэлектронным способам; г) к программно-математическим способам.

10. Особенности алгоритма "паразитических" вирусов:

а) Вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением com; б) Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса; в) Не имеют ни одного постоянного участка кода, трудно обнаруживаемы, основное тело вируса зашифровано; г) Изменяют содержимое дисковых секторов или файлов.

11. Препятствие как метод обеспечения защиты информации на предприятии – это:

а) метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.); б) метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия; в) метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия; г) метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

12. Возможность за приемлемое время получить требуемую информационную услугу называется:

а) доступностью информации; б) целостностью информации; в) предоставлением информации.

13. Типы защиты сети можно разбить на четыре основные категории: 1) физическая безопасность; 2) защита пользователей; 3) защита файлов; 4) защита от вторжения извне.

Найдите соответствие: а) Любому компьютеру, является ли он сервером в сети, рабочей станцией, ноутбуком или общедоступным терминалом в уличном киоске, необходимо обеспечить физическую защиту; б) предоставление менеджеру доступа к тем ресурсам, в которых он нуждается; не предоставлять (и даже не показывать) ему те ресурсы, которые ему не требуются для работы. К таким ресурсам относятся наиболее конфиденциальная информация компании и личные данные сотрудников, имеющих доступ; в) два аспекта: управление доступом к файлу; защита целостности файла (нарушитель, преднамеренно проникнувший в систему, может извлечь, изменить или

уничтожить информацию в файлах, поэтому необходим ввод некоторых ограничений на обработку файлов, содержащих важную информацию); г) Защита реализуется процедурами идентификации, установления подлинности и регистрации обращений. Идентификация и подтверждение подлинности могут осуществляться в процессе работы неоднократно, чтобы исключить возможность входа в систему нарушителя, выдающего себя за истинного пользователя.

14. К вспомогательным программным средствам защиты информации относится:

а) программы идентификации и аутентификации пользователей компьютерных сетей; б) программы шифрования информации; в) программы уничтожения остаточной информации (в блоках оперативной памяти временных файлах и т.п.) г) программы защиты информационных ресурсов (системного и прикладного программного обеспечения баз данных компьютерных средств обучения и т.п.) от несанкционированного изменения использования и копирования.

15. Средство контроля эффективности защиты информации — это:

а) Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации; б) Средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации; в) Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

16. Финансовая независимость — это:

а) уровень экономической безопасности, при котором уровень пассивных доходов позволяет наращивать личный капитал; б) уровень экономической безопасности, позволяющий поддерживать привычный уровень расходов при потере постоянного источника доходов на протяжении 6 (иногда 12) месяцев; в) самый простой уровень экономической безопасности домохозяйства, характеризующийся возможностью поддерживать привычный образ жизни.

17. К составляющим сетевой безопасности непосредственно не относится понятие:

а) Целостность данных; б) Конфиденциальность данных; в) Доступность данных; г) Глобальная связанность.

Вариант 4

1. Домашнее хозяйство – это экономическая единица, которая:

а) стремится к максимизации прибыли; б) самостоятельно принимает решения; в) стремится к максимальному удовлетворению своих потребностей.

2. Информационная среда — это (какое из определений является более общим):

а) совокупность информационных условий существования субъекта (это наличие информационных ресурсов и их качество, развитость информационной инфраструктуры); б) совокупность технических и программных средств хранения, обработки и передачи информации, а также социально-экономических и культурных условий реализации процессов информатизации; в) сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации, включает в себя всю знаковую среду, которая окружает людей в современном обществе.

3. Уязвимость информационной системы:

а) Явление, действие или процесс, результатом которого могут быть утечка, искажение, защищаемой информации; б) Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации; в) Действие или процесс, результатом которого могут быть уничтожение защищаемой информации, блокирование доступа к ней.

4. Информационная безопасность – это:

а) защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации; б) есть составная часть информационных технологий; в) свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

5. По способу осуществления угрозы можно классифицировать по следующим критериям:

а) (случайные/преднамеренные действия природного/техногенного характера); б) данные, программы, аппаратура, поддерживающая инфраструктура; в) внутри/вне рассматриваемой ИС; г) доступность, целостность, конфиденциальность

6. Анализ информационного риска:

а) Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение; б) Общий процесс анализа информационного риска и его оценивания; в) Систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей

реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

7. Авторизация (*Authorization*) – это:

а) предоставление определенному пользователю прав на выполнение некоторых действий; б) процедура проверки идентификационных данных пользователя (чаще всего, логина и пароля) при доступе к информационной системе; в) процедура проверки идентификационных данных пользователя (чаще всего, логина и пароля) при доступе к информационной системе.

8. К информационным способам воздействия угроз на информационные объекты не относятся:

а) нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации; б) программно-математические; в) несанкционированный доступ к информационным ресурсам; г) манипулирование информацией (дезинформация, сокрытие или сжатие информации).

9. Особенности алгоритма макровируса:

а) Пишутся не в машинных кодах, а на WordBasik, живут в документах Word, переписывают себя в Normal.dot; б) Не имеют ни одного постоянного участка кода, трудно обнаруживаемы, основное тело вируса зашифровано; в) Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса; г) Вирусы, не изменяющие файлы, создают для EXE-файлов файлы - спутники с расширением com.

10. Вредоносные утилиты:

а) не представляют угрозы непосредственно компьютеру, на котором исполняются; б) это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах"; в) разработаны для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома компьютеров и других вредоносных действий.; г) не выполняют вредоносных действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя.

11. К методам обеспечения безопасности экономического объекта не относится метод а) Препятствия; б) Управление доступом; в) Программный; г) Маскировка; д) Регламентация.

12. Побуждение как метод обеспечения защиты информации на предприятии – это:

а) метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности; б) метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм; в) метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму; г) метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

13. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:

а) доступностью информации б) целостностью информации в) предоставлением информации г) конфиденциальностью информации

14. К основным аппаратным средствам защиты информации не относится:

а) устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.); б) устройства для шифрования информации; в) устройства для воспрепятствования несанкционированному включению рабочих станции и серверов (электронные замки и блокираторы); г) устройства сигнализации о попытках несанкционированных действий пользователей компьютерных сетей.

15. При рассмотрении вопросов, связанных с информационной безопасностью, в современных условиях, необходимо учитывать следующие факторы (выбрать правильное):

а) глобальную связанность; б) разнородность корпоративных информационных систем; в) распространение технологии "клиент/сервер"; г) всё перечисленное.

16. Предметом обеспечения экономической безопасности домохозяйства является:

а) выявление и мониторинг факторов, негативно влияющих на состояние их экономической безопасности; б) страхование личных экономических рисков; в) развитие индивидами в рамках домохозяйства собственных физических способностей, интеллектуальных и профессиональных знаний для обеспечения собственного уровня и качества жизни, противодействия экономическим угрозам; г) формирование экономических предпосылок использования

домохозяйством собственных ресурсов со стороны фирмы для обеспечения соответствующего уровня доходов.

17. Основными показателями экономической эффективности системы защиты информации считаются (указать правильное):

а) коэффициент защищенности; б) экономическая эффективность; в) экономический эффект.

Вариант 5

1. Рынок продуктов — это:

а) экономическая ситуация, складывающаяся на рынке продуктов и характеризующаяся уровнями спроса и предложения; б) место, где товары и услуги фирм покупаются и продаются; в) экономическая ситуация, складывающаяся на рынке ресурсов и характеризующаяся уровнями спроса и предложения; г) место, где ресурсы и услуги поставщиков ресурсов продаются и покупаются.

2. Информационная среда –

а) весь набор условий для технологической переработки и эффективного использования знаний в виде информационного ресурса; б) совокупность технических и программных средств хранения, обработки и передачи информации, а также социально-экономических и культурных условий реализации процессов информатизации; в) совокупность информационных условий существования субъекта (это наличие информационных ресурсов и их качество, развитость информационной инфраструктуры); г) все определения корректны.

3. Доступность информации для обеспечения информационной безопасности — это:

а) гарантия получения требуемой информации или информационной услуги пользователем за определенное время; б) неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации; в) гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

4. По расположению источника угроз, угрозы можно классифицировать по следующим критериям:

а) доступность, целостность, конфиденциальность; б) данные, программы, аппаратура, поддерживающая инфраструктура; в) случайные/преднамеренные действия природного/техногенного характера; г) внутри/вне рассматриваемой ИС.

5. К внешним угрозам информационной безопасности относятся (исключите неверный источник):

а) распространение вредоносного программного обеспечения; б) воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем; в) воздействие на персонал предприятия с целью получения конфиденциальной информации; г) воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций; д) угрозы, инициируемые персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию.

6. Вредоносная программа:

а) Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации; б) Недостаток или слабое место в информационной системе; в) Воздействие, вызывающе нарушение нормального функционирования (сбой в работе) технических средств автоматизированных информационных систем; г) Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

7. Аутентичность в передаче и обработке данных – это:

а) предоставление определенному пользователю прав на выполнение некоторых действий; б) процедура проверки идентификационных данных пользователя (чаще всего, логина и пароля) при доступе к информационной системе; в) целостность информации, подлинность того, что данные были созданы законными участниками информационного процесса, и невозможность отказа от авторства.

8. Окно опасности, когда возможны успешные атаки на ИС, возникает, когда должны произойти следующие события:

а) должно стать известно о средствах использования пробела в защите; б) должны быть выпущены соответствующие заплаты; в) заплаты должны быть установлены в защищаемой ИС.

9. Установка программных и аппаратных закладных устройств относится к способу воздействия угроз на информационные объекты:

а) к информационным способам; б) к программно-математическим способам; в) к информационным способам; г) к физическим способам.

10. Особенности алгоритма вирусов-"спутников":

а) Изменяют содержимое дисковых секторов или файлов; б) Не имеют ни одного постоянного участка кода, трудно обнаруживаемы, основное тело вируса зашифровано; в) Вирусы, не изменяющие файлы, создают для EXE-

файлов файлы-спутники с расширением com; г) Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса.

11. К средствам обеспечения безопасности экономического объекта не относится

а) Физические; б) Аппаратные; в) Программные; г) Законодательные; д) Управление доступом.

12. Маскировка как метод обеспечения защиты информации на предприятии:

а) метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму; б) метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности; в) метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм; г) метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

13. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба, называются:

а) обнаружение угроз; б) пресечения и локализация угроз; в) ликвидация угроз.

14. К программным методам обеспечения информационной безопасности в зависимости от способа их реализации относятся:

а) реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т. д.; б) которые подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей; в) включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации; г) по защите информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т. д.). Без использования программной составляющей

практически невыполнимы никакие, в том числе и первые три группы методов (то есть в чистом виде организационные, технологические и аппаратные методы защиты, как правило, реализованы быть не могут — все они содержат программный компонент).

15. Использование технологии "клиент/сервер" с точки зрения информационной безопасности имеет следующие особенности (выбрать правильное):

а) каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности); б) каждый сервис имеет свою трактовку понятий субъекта и объекта; в) каждый сервис имеет специфические угрозы; г) каждый сервис нужно по-своему администрировать; д) средства безопасности в каждый сервис нужно встраивать по-особому.

16. Финансовая безопасность — это

а) самый простой уровень экономической безопасности домохозяйства, характеризующийся возможностью поддерживать привычный образ жизни; б) уровень экономической безопасности, позволяющий поддерживать привычный уровень расходов при потере постоянного источника доходов на протяжении 6 (иногда 12) месяцев; в) уровень экономической безопасности, при котором уровень пассивных доходов позволяет наращивать личный капитал.

17. Непосредственно к критериям экономической безопасности домохозяйства не относится:

а) удовлетворенность качеством жизни и уверенность в будущем; б) устойчивость к информационным, экономическим и политическим влияниям; в) сформированность экономической инфраструктуры экономической безопасности домохозяйства.

Вариант 6

1. Информация рассматривается как:

а) товар; б) субъект управления; в) сведения независимо от формы их представления; г) знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди в рамках конкретного контекста.

2. К экономическим отношениям субъектов экономики в полной модели рыночных отношений относятся отношения по поводу таких факторов как:

а) Издержки; б) Денежный доход; в) Товары и услуги; г) Потребительские расходы; д) Налоги.

3. Угроза — это:

а) атака с целью нарушить информационную безопасность; б) Потенциальные злоумышленники; в) потенциальная возможность определенным образом нарушить информационную безопасность.

4. Оценка информационного риска — это:

а) Общий процесс анализа информационного риска и его оценивания; б) Систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации; в) Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

5. Сетевая безопасность – это:

а) декларированные административные цели, ради которых создавалась ИС, общие правила закупок, внедрения новых компонентов, эксплуатации и т.п.; б) требования к физической безопасности информационных систем (ИС) и пути их выполнения, правила противопожарной безопасности и т.п.; в) набор требований, предъявляемых к инфраструктуре компьютерной сети предприятия и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа.

6. Аутентификация (*Authentication*) – это:

а) процедура проверки идентификационных данных пользователя (чаще всего, логина и пароля) при доступе к информационной системе; б) предоставление определенному пользователю прав на выполнение некоторых действий; в) целостность информации, подлинность того, что данные были созданы законными участниками информационного процесса, и невозможность отказа от авторства.

7. О наличии вредоносного программного обеспечения (ПО) в системе пользователь может судить по следующим признакам:

а) рассылка писем, которые пользователем не отправлялись, по электронной почте; б) явные проявления присутствия вируса, такие как: сообщения, выдаваемые на монитор или принтер, звуковые эффекты, неожиданный запуск программ, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в системе; в) появление сообщений антивирусных средств о заражении или о предполагаемом заражении, "самопроизвольное" отключение антивирусных программных средств.

8. Вредоносный код, который выглядит как функционально полезная программа, называется

а) троянским; б) вирусом; в) червем; г) вредоносное программное обеспечение.

9. Управление доступом как метод обеспечения защиты информации на предприятии – это:

а) метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.); б) метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия; в) метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

10. К типичным недостаткам, присущим системе безопасности экономических объектов относятся:

а) узкое, несистемное понимание проблемы безопасности объекта; б) пренебрежение профилактикой угроз, работа по принципу "Появилась угроза – начинаем ее устранять"; в) некомпетентность в экономике безопасности, неумение сопоставлять затраты и результаты; г) "технократизм" руководства и специалистов службы безопасности, интерпретация всех задач на языке знакомой им области.

11. Ошибки программного обеспечения с точки зрения информационной безопасности являются:

а) уязвимым местом; б) окном опасности; в) окном безопасности; г) источником угрозы.

12. К организационным методам обеспечения информационной безопасности в зависимости от способа их реализации относятся:

а) реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т. д.; б) которые подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей; в) включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации; г) по защите информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры,

криптопротоколы и т. д.). Без использования программной составляющей практически невыполнимы никакие, в том числе и первые три группы методов (то есть в чистом виде организационные, технологические и аппаратные методы защиты, как правило, реализованы быть не могут — все они содержат программный компонент).

13. Криптографическое средство защиты информации — это:

а) Средство защиты информации, реализующее алгоритмы криптографического преобразования информации; б) Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации; в) Средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

14. Фактор, воздействующий на защищаемую информацию — это:

а) Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.; б) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации; в) Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

15. Основные этапы построения системы защиты заключаются в следующем (расставить по порядку: а) Разработка системы защиты (планирование); б) Анализ; в) Сопровождение системы защиты; г) Реализация системы защиты.

16. Причины массовых ошибок в принятии финансовых решений домохозяйствами (указать правильные ответы):

а) неумение адекватно оценивать риски; б) отсутствие долгосрочных стратегий семейного бюджета — чаще всего решения принимаются спонтанно, под действием примера, слухов или рекламы; краткосрочный горизонт планирования; в) недоступность профессионального финансового консультирования для подавляющего большинства граждан; г) "непрозрачность" для населения финансовой политики ключевых институтов и государственных решений, отсутствие разъяснительной работы; д) недобросовестная реклама потребительского кредита, ипотеки, финансовых услуг.

17. В документе "Национальная стратегия повышения финансовой грамотности 2017-2023 гг." уровень финансовой грамотности домашних хозяйств оценивается как:

а) высокий; б) средний; в) низкий.

СПИСОК ИСТОЧНИКОВ

Основная

1. Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем: учеб. 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 : 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

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ СУБЪЕКТА ЭКОНОМИКИ

Редактор Э. С. Круглова

Уч.-изд. л. 3,3 Печ. л. 3,0

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