Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Начальник УРОПСП

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
0174a99400e2af6fb74dca3b394e65efc4
Владелец: Мельникова Виктория Александровна
Действителен: с 12.04.2023 по 12.04.2024

Фонд оценочных средств
(приложение к рабочей программе модуля)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ СУБЪЕКТА ЭКОНОМИКИ

основной профессиональной образовательной программы специалитета
по специальности
38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Специализация
«ЭКОНОМИКО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ»

ИНСТИТУТ отраслевой экономики и управления

РАЗРАБОТЧИК кафедра экономической теории и инструментальных методов

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторам и достижения компетенции
ОПК-6 Способен использовать современные информационные технологии и программные средства при решении профессиональных задач; ОПК-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-6.2 Применяет современные информационные технологии и программные средства для решения профессиональных задач; ОПК-7.2 Применяет сетевые информационные технологии для представления информации, разработки и оформления документации.	Обеспечение информационной и технической безопасности субъекта экономики	*Знать:* - 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;

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторам и достижения компетенции
			- 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. .

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПОЭТАПНОГО ФОРМИРОВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ (ТЕКУЩИЙ КОНТРОЛЬ) И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2.1 Для оценки результатов освоения дисциплины используются:

- оценочные средства текущего контроля успеваемости;

- оценочные средства для промежуточной аттестации по дисциплине.

2.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания;

- задания по темам практических занятий;

- задания по контрольным работам (для заочной формы обучения).

2.3 К оценочным средствам для промежуточной аттестации по дисциплине, проводимой в форме зачета, относятся:

- промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

3.1 Тестовые задания используются для оценки освоения тем дисциплины студентами всех форм обучения (приложение №1). Тестирование проводится как форма самостоятельной работы студентов всех форм обучения.

Тестовое задание предусматривает выбор правильного ответа на поставленный вопрос из предлагаемых вариантов ответа.

Тестирование производится методом случайной выборки (15 вопросов в итоговом тестовом задании) в системе тестирования «INDIGO», в любое время суток с использованием ЕИП ИНОТЭКУ КГТУ. 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 выставляется студенту при получении от 56 до 100% верных ответов.

3.2 В приложении № 2 приведены типовые задания для проведения практических занятий, предусмотренных рабочей программой модуля.

Для самостоятельной подготовки к практическому занятию необходимо внимательно изучить материал лекций. Следует помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. Положительная оценка ставится при выполнении студентом задания и защиты его у преподавателя ведущего практические занятия. Неудовлетворительная оценка выставляется, если студент не выполнил предусмотренные рабочей программой модуля практические задания.

3.3 В приложении № 3 приведены типовые задания по контрольным работам для студентов заочной формы обучения. Контрольная работа предполагает раскрытие теоретических вопросов по дисциплине, а также решение задач по вариантам.

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.

По результатам проверки контрольной работы выставляется оценка. Работа положительно оценивается при условии соблюдения требований задания на ее выполнение. В том случае, если работа не отвечает предъявляемым требованиям (не раскрыты теоретические вопросы, использовано менее пяти литературных источников по каждому вопросу, изложение материала поверхностно, отсутствуют выводы, не решены задачи), то она возвращается автору на доработку. Студент должен переделать работу с учетом замечаний и предоставить для проверки новый вариант.

Критерии оценивания контрольной работы строятся на основе универсальной системы оценивания результатов обучения, представленной в таблице 2 раздела 4.

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1 Промежуточная 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.

4.2 В приложении № 4 приведены вопросы для проведения промежуточной аттестации (зачета).

4.3 Зачетная оценка («зачтено», «не зачтено») является экспертной и зависит от уровня освоения специалистом тем дисциплины.

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 (табл. 2)

Таблица 2 – 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 %**
	«неудовлетвори-тельно»	**«удовлетвори-тельно»**	**«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

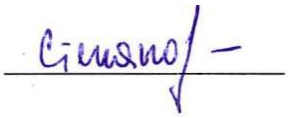
5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Обеспечение информационной и технической безопасности субъекта экономики» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 38.05.01 Экономическая безопасность (специализация «Экономико-правовое обеспечение экономической безопасности»).

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры экономической теории и инструментальных методов (протокол № 8 от 01.04.2022 г.).

Заведующий кафедрой Л.И. Сергеев

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры экономической безопасности (протокол № 9 от 26.04.2022 г.).



Заведующая кафедрой Т.Е. Степанова

Приложение № 1

к п. 3.1

ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ СУБЪЕКТА ЭКОНОМИКИ»

Вариант 1

1. Субъектами экономики являются:

а) Государство;

б) Предприятия;

в) Домашние хозяйства;

2. Информация – это:

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.

3. Собственниками информации могут быть (укажите правильные ответы):

а) государство;

б) юридическое лицо;

в) группа физических лиц;

г) отдельное физическое лицо;

д) домохозяйство.

4. Доступность информации – это:

а) неизменность информационных объектов;

б) гарантия получения требуемой информации;

в) обеспечение конфиденциальности информации;

г) информация сейчас существует в ее исходном виде.

5. 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.

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

а) Обеспечением доступности информации;

б) Обеспечением целостности информации;

в) Обеспечением конфиденциальности информации.

7. 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.

8. 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.

9. 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.

10. Меры каких уровней входят в организацию системы обеспечения информационной безопасности:

а) законодательного уровня;

б) административного уровня;

в) процедурного уровня;

г) программно-технического уровня;

д) программно-аппаратного уровня.

11. Рынок ресурсов – это:

а) место, где ресурсы и услуги поставщиков ресурсов продаются и покупаются;

б) место, где товары и услуги фирм покупаются и продаются;

в) система учреждений и организаций, обеспечивающих движение ресурсов на рынке.

12. К экономическим отношениям субъектов экономики в полной модели рыночных отношений относятся отношения по поводу таких факторов как (перечислить пункты):

а) Издержки;

б) Денежный доход;

в) Товары и услуги;

г) Потребительские расходы;

д) Налоги.

13. 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.

14. 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.

15. К средствам обеспечения безопасности экономического объекта относится:

а) Физические;

б) Аппаратные;

в) Программные;

г) Законодательные;

д) Управление доступом.

Вариант 2

1. Экономические субъекты – это:

а) Субъекты экономических отношений, принимающие участие в производстве экономических благ;

б) Субъекты экономических отношений, принимающие участие в распределении экономических благ;

в) Субъекты экономических отношений, принимающие участие в обмене и потреблении экономических благ.

2. 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.

3. Информация — это:

а) Факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации;

б) Зафиксированная на материальном носителе путем документирования информация с реквизитами;

в) Сведения (сообщения, данные) независимо от формы их представления.

4. 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.

5. 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).

6. К методам обеспечения безопасности экономического объекта не относится метод:

а) Препятствия;

б) Управление доступом;

в) Программный.

7. 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.

8. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов, принято считать:

а) политикой безопасности;

б) методом защиты информации;

в) ограничением доступа к информации учётными записями пользователей.

9. 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.

10. Защита информации — это:

а) практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации;

б) совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее;

в) системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определёнными критериями и показателями безопасности;

г) совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

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

а) физический;

б) технический (аппаратный);

в) программный.

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

а) доступностью информации;

б) целостностью информации;

в) предоставлением информации;

г) конфиденциальностью информации.

13. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:

а) утечкой;

б) разглашением;

в) взломом.

14. К уровням формирования режима информационной безопасности относятся:

а) законодательно-правовой;

б) административный (организационный);

в) программно-технический.

15. 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.

Приложение № 2

к п. 3.2

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Практическое занятие 1

Тема: Проблема информационной и технической безопасности для субъектов экономики

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;
2. Дискуссия по пройденному материалу;
3. 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.

Практическое занятие 2

Тема: Составляющие информационной и технической безопасности

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;
2. Дискуссия по пройденному материалу;
3. 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.

Практическое занятие 3

Тема: Классификация угроз информационной и технической безопасности

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;
2. Дискуссия по пройденному материалу;
3. 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.

Практическое занятие 4

Тема: Технологии, методы, технические средства, механизмы обеспечения информационной безопасности

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;
2. Дискуссия по пройденному материалу;
3. 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.

Практическое занятие 5

Тема: Экономическая эффективность обеспечения информационной и технической безопасности субъекта экономики

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций;
2. Дискуссия по пройденному материалу;
3. 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.

Приложение № 3

к п. 3.3

ТИПОВЫЕ ЗАДАНИЯ ПО КОНТРОЛЬНОЙ РАБОТЕ ПО ДИСЦИПЛИНЕ «ПРИНЯТИЕ РЕШЕНИЙ В УСЛОВИЯХ РИСКА И НЕОПРЕДЕЛЕННОСТИ»

Выбор варианта осуществляется в соответствии со списком студентов.

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?

Приложение №4

к п. 4.2

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ДИСЦИПЛИНЕ, КОТОРЫЕ ПРИ НЕОБХОДИМОСТИ МОГУТ БЫТЬ ИСПОЛЬЗОВАНЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Перечень 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. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 6 апреля 2011 г. N 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.