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 дисциплины)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

основной профессиональной образовательной программы специалитета
по специальности
38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Профиль (специализация) программы
«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/индикаторами достижения компетенции
ПК-4: Способен формировать, анализировать и оценивать информацию, необходимую для принятия решений по обеспечению экономической безопасности.	ПК-4.1: Формирует, анализирует и оценивает информационную базу, необходимую для обеспечения экономической безопасности.	Информационная безопасность	*Знать:* - предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ; - основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия; - иметь полное представление о значение информационной безопасности для современного бизнеса, о перспективах развития технологий обеспечения информационной безопасности. *Уметь:* - анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; - использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной Инфраструктуры; -применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ; -ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ. *Владеть:* - способностью применять на

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
			практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации ИБ; -способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия; - организовывать и проводить аудит ИБ; - использовать современные инструментальные средства анализа рисков и разработки политики ИБ; - навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности

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;

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

- задания по контрольным работам;

- вопросы для промежуточной аттестации (экзамен) по дисциплине;

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 (16 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.

В приложении № 6 приведены ключи правильных ответов к тестовым заданиям.

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 для проведения лабораторных занятий, предусмотренных рабочей программой модуля.

Для самостоятельной подготовки к лабораторному 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 лабораторные занятия. Неудовлетворительная оценка выставляется,

если студент не выполнил предусмотренные рабочей программой модуля лабораторные задания.

3.4 В приложении № 4 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 экзамена. К экзамену допускаются студенты:

- положительно аттестованные по результатам проведенного тестирования;

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

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

4.2 В приложении № 5 приведены вопросы для проведения промежуточной аттестации (экзамена).

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

Критерии оценивания экзамена по дисциплине

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

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
				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

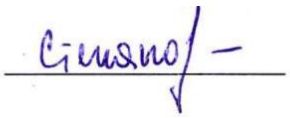
5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Информационная безопасность» 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

ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ «ПРИНЯТИЕ РЕШЕНИЙ В УСЛОВИЯХ РИСКА И НЕОПРЕДЕЛЕННОСТИ»

Вариант 1

1. Информация – это:

а) сведения, поступающие от СМИ;

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

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

2. Наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности является категория:

а) Сотрудники;

б) хакеры;

в) атакующие.

3. Защите подлежит информация:

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

б) только информация, составляющая государственные информационные ресурсы;

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

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

а) достоверной;

б) конфиденциальной;

в) документированной.

5. Угроза – это:

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

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

в) потенциальная возможность определенным образом нарушить информационную безопасность.

6. Конфиденциальность – это:

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

б) защита от несанкционированного доступа к информации;

в) описание процедур.

7. Ошибка – это:

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

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

в) негативное воздействие на программу.

8. Присвоение чужого права относится к:

а) нарушению права собственности;

б) нарушению содержания;

в) внешней среде.

9. Окно опасности – это:

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

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

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

10. Вредоносная программа – это:

а) упорядочение абстракций, расположение их по уровням;

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

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

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

а) ограниченной компетенцией злоумышленника;

б) за определенное время;

в) фиксированными затратами.

12. При классификации данных руководство первым делом должно продумать:

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

б) необходимый уровень доступности, целостности и конфиденциальности;

в) уровень риска и контрмеры.

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

а) аутентификация;

б) идентификация;

в) авторизация.

14. Черви – это:

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

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

в) программа действий над объектом или его свойствами.

15. Административные действия в системе управления базами данных позволяют выполнять привилегии:

а) безопасности;

б) чтения;

в) тиражирования.

16. Соответствие средств безопасности решаемым задачам характеризует:

а) эффективность;

б) корректность;

в) адекватность.

Вариант 2

1. По принадлежности информационные ресурсы подразделяются на:

а) государственные, коммерческие и личные;

б) государственные, не государственные и информацию о гражданах;

в) информацию юридических и физических лиц.

2. По доступности информация классифицируется на:

а) открытую информацию и государственную тайну;

б) конфиденциальную информацию и информацию свободного доступа;

в) информацию с ограниченным доступом и общедоступную информацию.

3. Сбой – это:

а) объект-метод;

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

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

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

а) идентификация;

б) авторизация;

в) аутентификация.

5. Отказ – это:

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

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

в) структура, определяющая последовательность выполнения и взаимосвязи процессов

6. Минимальная длина безопасного пароля, состоящего из одних только строчных английских букв составляет:

а) 15;

б) 12;

в) 10.

7. Инсайдер — это:

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

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

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

8. Вирус – это:

а) небольшая программа для выполнения определенной задачи;

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

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

9. Троянские программы — это:

а) программы-вирусы, которые распространяются самостоятельно;

б) все программы, содержащие ошибки;

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

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

а) надёжность информации;

б) защищённость информации;

в) безопасность информации

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

а) криптология;

б) криптоанализ;

в) криптография

12. Защита информации – это:

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

б) комплекс мероприятий, направленных на обеспечение информационной безопасности.

в) небольшая программа для выполнения определенной задачи.

13. Требования к техническому обеспечению системы защиты:

а) аппаратурные и физические;

б) управленческие и документарные;

в) процедурные и раздельные.

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

а) высокая степень надежности;

б) числовая вероятностная оценка надежности;

в) динамичность.

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

а) системный администратор;

б) генеральный директор предприятия;

в) пользователь.

16. В отношении выявленных рисков целесообразно не предпринимать никаких действий когда:

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

б) Когда необходимые защитные меры слишком сложны;

в) Когда стоимость контрмер превышает ценность актива и потенциальные потери.

Вариант 3

1. Шаблон проекта экономической информационной системы – это:

а) форма ввода данных;

б) интерфейс экономической информационной системы;

в) типовой проект экономической информационной системы.

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

а) системный;

б) внешний;

в) приложений.

3. По доступности информация классифицируется на:

а) открытую информацию и государственную тайну;

б) конфиденциальную информацию и информацию свободного доступа;

в) информацию с ограниченным доступом и общедоступную информацию.

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

а) восстанавливаемость;

б) целостность;

в) доступность.

5. Отказ, ошибки, сбой – это:

а) природные угрозы;

б) преднамеренные угрозы;

в) случайные угрозы.

6. Программные средства – это:

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

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

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

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

а) комплексный;

б) целостный;

в) административный.

8. Безусловной атакой является атака, когда:

а) пользователь принес вирус на дискете;

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

в) на ПК обнаружен вирус, передающий информацию в интернет.

9. Первым этапом разработки системы защиты ИС является:

а) анализ потенциально возможных угроз информации;

б) изучение информационных потоков;

в) стандартизация программного обеспечения.

10. Удачная криптоатака называется:

а) раскрытием шифра;

б) проникновением;

в) взломом.

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

а) актуальностью информации;

б) доступностью;

в) качеством информации.

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

а) директор фирмы;

б) системный администратор;

в) начальник службы безопасности

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

а) администратора сервера баз данных;

б) системного администратора;

в) сетевого администратора.

14. Надежность системы защиты информации определяется:

а) усредненным показателем;

б) самым слабым звеном;

в) количеством отраженных атак.

15. Недостатком многоуровневых моделей безопасности является:

а) сложность представления широкого спектра правил обеспечения безопасности;

б) отсутствие полного аудита;

в) невозможность учета индивидуальных особенностей субъекта.

16. Цель процесса внедрения и тестирования средств защиты —

а) определить уровень расходов на систему защиты;

б) выявить нарушителя;

в) гарантировать правильность реализации средств защиты.

Приложение № 2

к п. 3.2

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

Практическое занятие 1

Тема: Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия

Форма занятия: семинар.

План занятия:

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

Вопросы:

1. Информационное пространство (инфосфера);
2. Информационная война;
3. Информационное противоборство;
4. Информационная преступность;
5. Информационное воздействие;
6. Информационное оружие;
7. Угроза безопасности информации;
8. Информационная безопасность;
9. Объект информационной безопасности;
10. Компьютерная безопасность;
11. Безопасность данных;
12. Безопасность коммуникаций;
13. Политика безопасности;
14. Угроза безопасности информации;
15. Защита информации (ЗИ);
16. Система защиты информации (СЗИ);
17. Виды обеспечения СЗИ;
18. Классы угроз информационной безопасности;
19. Концепция Информационной Безопасности;

20. Правовая основа Концепции;
21. Что подлежит правовой защите;
22. Организационные меры по предотвращению нарушений безопасности информации;
23. Подходы по выработке стратегии управления рисками;
24. Основные цели обеспечения информационной безопасности экономических систем;
25. Основные задачи обеспечения информационной безопасности экономических систем;
26. Нормативно-правовые акты в области информационной безопасности в РФ.

Практическое занятие 2

Тема: Защищенная информационная система. Уровни и структура ИБ

Форма занятия: семинар.

План занятия:

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

Вопросы:

1. Защищаемая информация;
2. Отличительные признаки защищаемой информации;
3. Государственная тайна;
4. Персональные данные;
5. Что такое GDPR;
6. Принципы GDPR;
7. Коммерческая тайна;
8. Автоматизированная система управления технологическим процессом;
9. Документы с грифом «Для служебного пользования»;
10. Открытые информационные ресурсы;
11. Характеристики безопасной ИС;
12. Классификация защищаемой информации;
13. Классификация информации по категориям доступа;
14. Ценность информации;
15. Шаги процедуры построения модели угроз информационной безопасности;

16. Моделирование сценариев угроз;
17. Защищенная информационная система;
18. Модель ЗИС;
19. Состав нормативной базы ФСТЭК России в области обеспечения информационной безопасности КИИ;
20. Политика информационной безопасности (ПИБ);
21. Этапы создания ПИБ.

Практическое занятие 3

Тема: Модели и стандарты в сфере ИБ и управления рисками ИБ

Форма занятия: семинар.

План занятия:

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

Вопросы:

1. Информационный риск;
2. Проблемные аспекты оценки информационных рисков;
3. Виды информационных рисков;
4. Проблемы страхования информационных рисков;
5. Категории IT-рисков;
6. Процесс минимизации ИТ-рисков;
7. Выявление IT-рисков;
8. Методы количественной оценки рисков;
9. Статистические методы;
10. Логико-вероятностные методы;
11. Метод аналогий;
12. Аналитическая группа методов;
13. Виды количественных показателей риска;
14. Формула функции для оценки динамики исследуемого параметра;
15. График плотности вероятности;
16. Основные черты функции нормального распределения;
17. Применение метода VaR в оценке риска;
18. Статистические способы оценки риска;

19. Применение элементов теории игр;
20. Качественные методики управления рисками
21. COBRA
22. RA Software Tool
23. Количественные методики управления рисками
24. CRAMM
25. Методика MethodWare
26. Необходимость стандартизации обеспечения безопасности данных;
27. Международные стандарты в области ИБ;
28. системы менеджмента информационной безопасности;
29. Создание СМИБ с учетом стандартов;
30. Российские СМИБ;
31. Преимущества СМИБ;
32. Исходные положения при синтезе оптимальных систем защиты;
33. Итогом решения задачи синтеза оптимальной системы защиты и его конечная цель;
34. Математическая модель процессов в СЗИ;
35. Пример модели процесса защиты;
36. Выбор модели реализации СЗИ;
37. Архитектурная безопасность;
38. Инсайдеры;
39. Стандартный набор сервисов безопасности.

Практическое занятие 4

Тема: Технологии и методы реализации ИБ, комплексная защита информационной инфраструктуры

Форма занятия: семинар.

План занятия:

1. Опрос по материалам лекций.

2. Дискуссия по пройденному материалу;

Вопросы:

1. Криптографическое преобразование;
2. Криптография с симметричными ключами;

3. Криптография с открытыми ключами;
4. Свойства криптографии с открытыми ключами;
5. Реализация схемы электронной цифровой подписи (ЭЦП);
6. Схема формирования подписи электронного документа (ЭД);
7. Комбинированный метод;
8. Сертификация открытых ключей;
9. ФЗ «О безопасности критической информационной инфраструктуры»;
10. Таргетированная (или целевая) атака;
11. Их цели;
12. Классификация таргетированных атак;
13. Этапы таргетированных атак;
14. Объект воздействия таргетированных атак;
15. Источники таргетированных атак;
16. Анализ риска таргетированных атак;
17. Система защиты должна обеспечивать;
18. Состав эшелонированной системы защиты информации от таргетированных атак;
19. Альтернативные возможности защиты информации;
20. Результаты внедрения;
21. Используемы технологии;
22. Компьютерный вирус;
23. Классификация вирусов;
24. Виды антивирусных программ;
25. Комплексная система защиты информации;
26. Цели и задачи комплексной системы защиты информации;
27. Принципы создания комплексной системы защиты информации;
28. Основные функции КСЗИ по обеспечению ИБ;
29. Основные модули КСЗИ;
30. Внешние угрозы информационной безопасности;
31. Внутренние угрозы информационной безопасности;
32. Выгоды при внедрении комплексной системы защиты информации;
33. К организационным методикам относятся;
34. Основными методами защиты информации являются.

Приложение № 3

к п. 3.3

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

Лабораторное занятие 1

Тема: Парольная защита

Форма занятия: лабораторное.

План занятия:

1. Выполнение лабораторных заданий.

Задания:

1. Определить время перебора всех паролей с параметрами:

Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

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

Таблица 3 – Варианты для задания 1

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

2. Определить минимальную длину пароля с параметрами:

Алфавит состоит из n символов.

Время перебора не меньше t лет.

Скорость перебора s паролей в секунду.

Таблица 4 – Варианты для задания 2

вариант	n	t	s
1	33	100	100
2	26	120	13

3	52	60	30
вариант	n	t	s
4	66	70	20
5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

3. Определить количество символов алфавита с параметрами:

Пароль состоит из k символов

Время перебора не меньше t лет.

Скорость перебора s паролей в секунду.

Таблица 5 – Варианты для задания 3

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

Лабораторное занятие 2

Тема: Шифр простой замены. Таблица Вижинера

Форма занятия: лабораторное.

План занятия:

1. Выполнение лабораторных заданий.

Задания:

1. Используя возможности Microsoft Office Excel составить алгоритм шифрования и расшифрования текста с использованием шифра Цезаря.

Таблица 6 – Варианты для задания 1

Вариант	Ключ
1	5
2	6
3	7

4	8
5	9
Вариант	Ключ
6	10
7	11
8	12
9	13
10	14
11	15
12	16
13	17
14	18

2. Используя возможности Microsoft Office Excel составить алгоритм шифрования и расшифрования текста с использованием шифра Вижинера.

Таблица 7 – Варианты для задания 2

Вариант	Ключ		
	К	О	Д
1	16	15	21
2	15	16	20
3	14	17	19
4	13	18	12
5	12	5	11
6	11	6	10
7	10	7	18
8	6	8	17
9	5	9	16
10	4	10	15
11	9	11	14
12	8	12	9
13	7	13	8
14	3	14	7

Лабораторное занятие 3

Тема: Шифр RSA

Форма занятия: лабораторное.

План занятия:

1. Выполнение лабораторных заданий.

Задания:

Используя возможности Microsoft Office Excel и языка программирования Python составить алгоритм шифрования и расшифрования текста с использованием шифра RSA.

Лабораторное занятие 4

Тема: QR-коды

Форма занятия: лабораторное.

План занятия:

1. Выполнение лабораторных заданий.

Задания:

Используя различные информационные средства сгенерировать QR-код для своей страницы в ЭИОС.

Приложение № 4

к п. 3.4

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

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

Таблица 8 – Выбор варианта для теоретических вопросов

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

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

Теоретические вопросы

1. Объективная необходимость управления информационной безопасностью.
2. Современная концепция информационной безопасности.
3. Цели и концептуальные основы защиты информации.
4. Понятие и сущность информационной безопасности для субъектов экономики.
5. Классификации защищаемой информации.
6. Ключевые положения корпоративной концепции информационной безопасности.

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

8. Международные стандарты ISO по защите информации.

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

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

11. Трехуровневая модель параметров оценки защищенности ИС.

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

13. Понятие и виды информационных рисков.

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

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

16. Законопроект «О безопасности критической информационной инфраструктуры».

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

18. Необходимость стандартизации обеспечения безопасности данных.

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

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

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

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

23. Порядок разработки и структурные элементы программы информационной безопасности.

24. Порядок разработки Политики ИБ.

25. Математические методы оценки информационных рисков.

26. Технологии (методики) управления информационными рисками.

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

28. Методы криптографического преобразования информации.

29. Обобщённая схема криптографической системы.

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

31. Средства и виды антивирусных средств защиты.

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

33. Реализация методики оценки информационных рисков.

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

35. Особенности и задачи корпоративных систем защиты информации.

Задания

1. Определить время перебора всех паролей с параметрами:

Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

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

Таблица 9 – Варианты для задания 1

вариант	n	k	s	m	v
0	35	8	10	3	0
1	28	10	20	0	5
2	54	9	30	5	0
3	68	5	40	4	3
4	61	7	50	0	6
5	120	11	60	4	2
6	130	6	70	3	0
7	152	4	80	0	0
8	252	12	90	5	7
9	495	3	100	0	3

2. Определить минимальную длину пароля с параметрами:

Алфавит состоит из n символов.

Время перебора не меньше t лет.

Скорость перебора s паролей в секунду.

Таблица 10 – Варианты для задания 2

вариант	n	t	s
0	35	5	10
1	28	10	20
2	54	15	30
3	68	20	40
4	61	25	50
5	120	30	60
6	130	35	70
7	152	40	80
8	252	45	90
9	495	50	100

3. Определить количество символов алфавита с параметрами:

Пароль состоит из k символов

Время перебора не меньше t лет.

Скорость перебора s паролей в секунду.

Таблица 11 – Варианты для задания 3

вариант	k	t	s
0	12	5	10
1	13	10	20
2	14	15	30
3	5	20	40
4	6	25	50
5	7	30	60
6	8	35	70
7	9	40	80
8	10	45	90
9	11	50	100

4. Используя возможности Microsoft Office Excel составить алгоритм шифрования и расшифрования ФИО с использованием шифра Цезаря.

Таблица 12 – Варианты для задания 4

Вариант	Ключ
1	5
2	6
3	7
4	8
5	9
6	10
7	11
8	12
9	13
10	14

11	15
Вариант	Ключ
12	16
13	17
14	18

5. Используя возможности Microsoft Office Excel составить алгоритм шифрования и расшифрования ФИО с использованием шифра Вижинера.

Таблица 13 – Варианты для задания 5

Вариант	Ключ		
	К	О	Д
1	16	15	21
2	15	16	20
3	14	17	19
4	13	18	12
5	12	5	11
6	11	6	10
7	10	7	18
8	6	8	17
9	5	9	16
10	4	10	15
11	9	11	14
12	8	12	9
13	7	13	8
14	3	14	7

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

Приложение №5

к п. 4.2

ВОПРОСЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЭКЗАМЕН) ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Перечень вопросов

1. Трехуровневая модель параметров оценки защищенности ИС.
2. Политика ИБ как комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов.
3. Понятие и виды информационных рисков.
4. Общая характеристика математических методов оценки и обоснования требований к СЗИ.
5. Криптография как наука о методах обеспечения конфиденциальности и аутентичности информации.
6. Законопроект «О безопасности критической информационной инфраструктуры».
7. Внешние и внутренние угрозы информационной безопасности информационной безопасности предприятия.
8. Необходимость стандартизации обеспечения безопасности данных.
9. Практические примеры нарушения информационной безопасности и их последствия для государства, бизнеса, личности.
10. Международный опыт правового обеспечения информационной безопасности.
11. Сравнительная характеристика международного и российского законодательства в сфере ИБ.
12. Обязательный учёт в модели всех актуальных угроз на всех стадиях их жизненного цикла.
13. Процедура построения модели угроз информационной безопасности, состоящая из нескольких последовательных шагов.
14. Пересмотр и обновление модели информационной безопасности на основе постоянно меняющихся данных.
15. Порядок разработки и структурные элементы программы информационной безопасности.
16. Порядок разработки Политики ИБ.

17. Математические методы оценки информационных рисков.

18. Технологии (методики) управления информационными рисками.

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

20. Методы криптографического преобразования информации.

21. Обобщённая схема криптографической системы.

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

23. Средства и виды антивирусных средств защиты.

24. Модель защищенных информационных систем.

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

26. Реализация методики оценки информационных рисков.

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

28. Особенности и задачи корпоративных систем защиты информации.

29. Объективная необходимость управления информационной безопасностью.

30. Современная концепция информационной безопасности.

31. Цели и концептуальные основы защиты информации.

32. Понятие и сущность информационной безопасности для субъектов экономики.

33. Классификации защищаемой информации.

34. Ключевые положения корпоративной концепции информационной безопасности.

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

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

37. Международные стандарты ISO по защите информации.

38. Содержание, объём и ценность защищаемой информации.

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

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