МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Специальность и специализация
38.05.01 Экономическая безопасность. Экономико-правовое обеспечение экономической безопасности

Год набора на ОПОП
2023

Форма обучения
очная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Информационная безопасность предприятия» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.05.01 Экономическая безопасность (утв. приказом Минобрнауки России от 14.04.2021г. №293) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Иванова А.В., старший преподаватель, Кафедра информационной безопасности, Ivanova.A@vvsu.ru

Шумик Е.Г., кандидат экономических наук, доцент, Кафедра маркетинга и торговли, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 25.05.2023 , протокол № 3

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000B4E470
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Ознакомить студентов с законодательными, административными, организационными, программно-техническими мерами информационной безопасности, с действующими стандартами в этой области.
Задачи дисциплины состоят в том, что в результате ее изучения студенты должны:
– иметь представление об использовании основных положений теории информационной безопасности в различных областях ИС и иметь представление о направлении развития и перспективах защиты информации;
– знать правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;
– уметь применять методы защиты компьютерной информации в различных предметных областях.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
38.05.01 «Экономическая безопасность» (ЭБ)	ПКВ-2 : Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга	ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации	РД1	Знание	концепции защиты информации и систем безопасности предприятия и их роль в обеспечении экономической безопасности
			РД2	Умение	обосновывать свой выбор при применении методов и приемов защиты от несанкционированного доступа
			РД3	Навык	методами анализ угроз информационной безопасности
		ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации	РД4	Знание	методы предупреждения рисков информационной безопасности, влияющих на экономическую безопасность организации
			РД5	Умение	соблюдать требования, установленные к информационной безопасности организации

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Информационная безопасность предприятия» относится к дисциплинам по выбору. Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Информатика модуль 1 (Основы информационных технологий)», «Информатика модуль 2 (Информационно-коммуникационные технологии)».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
38.05.01 Экономическая безопасность	ОФО	С1.ДВ.А	8	4	55	18	36	0	1	0	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Основные понятия и определения информационной безопасности	РД1, РД5	4	8	0	22	Тестовые задания, практические работы
2	Государственная система информационной безопасности. Законодательный уровень информационной безопасности	РД1, РД3, РД5	4	8	0	15	Тестовые задания, практические работы
3	Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	РД2, РД3, РД4	4	10	0	24	Тестовые задания, практические работы
4	Методы обеспечения информационной безопасности	РД2, РД3, РД4, РД5	6	10	0	28	Тестовые задания, практические работы
Итого по таблице			**18**	**36**	**0**	**89**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Основные понятия и определения информационной безопасности.

Содержание темы: Проблемы информационной безопасности в современном

обществе. Основные понятия в области защиты информации. Уровни информационной безопасности (личности, общества, государства).

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 2 Государственная система информационной безопасности. Законодательный уровень информационной безопасности.

Содержание темы: Содержание и структура законодательства в области информационной безопасности. Правовое регулирование защиты информации в России. Содержание и структура законодательства в области информационной безопасности. Обзор документов в области обеспечения информационной безопасности по отраслям права.Регуляторы в области информационной безопасности. Изучение нормативных документовв сфере обеспечения информационной безопастности. ФЗ "О персональных данных" Обзор документов в области обеспечения информационной безопасности по отраслям права. Регуляторы в области информационной безопасности. Обзор документов в области юридической ответственности за правонарушения в области информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 3 Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия.

Содержание темы: Общий анализ угроз безопасности информации. Пути реализации угроз информационной. Общий анализ угроз безопасности информации. Пути реализации угроз информационной. Классификация угроз безопасности информации. Анализ киберугроз. Методические основы оценки угроз. Влияние угроз информационной безопасности на экономическую безопасность организации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 4 Методы обеспечения информационной безопасности.

Содержание темы: Управление информационными рисками. Соблюдение режима секретности. Комплексная защита информации. Соблюдение режима секретности. Управление информационными рисками. Соблюдение режима секретности. Комплексная защита информации. Критическая информационная инфраструктура. Категорирование объекта КИИ. Организационные меры обеспечения защиты информации. Аудит информационной безопасности организации. Обзор методических материалов. Организационных мер защиты информации. Критическая информационная инфраструктура. Категорирование объекта КИИ. Организационные меры обеспечения защиты информации. Программно-технические средства защиты информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Успешное освоение дисциплины предполагает активную работу студентов на лекциях и практических занятиях, выполнение аттестационных мероприятий, эффективную самостоятельную работу.

В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение рефератов и самостоятельное изучение некоторых вопросов курса. Методические рекомендации по обеспечению самостоятельной работы

Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В рамках подготовки к практическим занятиям студенты сначала прорабатывают лекционный материал, презентации по теме работы, знакомятся с целью, задачами и информационными источниками.

При необходимости подбирают дополнительные информационные материалы, необходимую литературу, нормативные и законодательные документы, знакомятся с ними. В случае, если в заданиях работы необходимо написать размышление или эссе, изучают источники, различные данные и др., чтобы иметь представление о вопросах, затрагиваемых в работе.

Задания представляют собой ситуационные практические задания, выполняемые индивидуально или группой студентов - временным творческим коллективом в составе нескольких студентов (2-3 человека).

Самостоятельная работа специалистов предполагает:

1. Изучение материала по теме занятия и подготовка к практическому занятию.

2. Поиск и сбор первичной и вторичной информации по заявленной проблеме в рамках ситуационных заданий к практическим занятиям и подготовка отчета по результатам самостоятельно проведенных исследовании форме презентации (файл с расширением .ppt).

3. Защита ситуационного практического задания проводится на практическом занятии с демонстрацией отчета или презентации, ответы на вопросы, обсуждение.

По результатам проверки студенту выставляется определенное количество баллов, которое входит в общее количество баллов студента, набранных им в течение семестра. При оценке результатов выполнения заданий учитываются четкость структуры работы, умение сбора вторичной информации, умение ставить проблему и анализировать ее, умение логически мыслить, владение профессиональной терминологией, грамотность оформления.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания,

консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Документальное обеспечение информационной безопасности : учебное пособие / составители Е. Е. Смычков [и др.]. — Севастополь : СевГУ, 2022. — 142 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/261899 (дата обращения: 22.11.2023). — Режим доступа: для авториз. пользователей.

2. Правовые основы информационной безопасности : практикум / сост. Х. В. Белогорцева (Пешкова). - Воронеж : Научная книга, 2021. - 80 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1996330 (дата обращения: 14.12.2023).

7.2 Дополнительная литература

1. Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие / А. В. Ванюшина, С. Ю. Рыбаков. — Москва :МТУСИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333701 (дата обращения: 22.11.2023). — Режим доступа: для авториз. пользователей.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2020. — 267 с. — ISBN 978-5-406-07382-7. — URL: https://book.ru/book/932059 (дата обращения: 11.01.2024). — Текст : электронный.

3. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 14.12.2023).

4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912987 (дата обращения: 01.03.2023). – Режим доступа: по подписке.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "BOOK.ru"
2. Электронно-библиотечная система "ZNANIUM.COM"
3. Электронно-библиотечная система "ZNANIUM.COM" - Режим доступа: https://znanium.com/
4. Электронно-библиотечная система "ЛАНЬ"
5. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
6. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
7. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

· Проектор

Программное обеспечение:

· МойОфис

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Специальность и специализация

38.05.01 Экономическая безопасность. Экономико-правовое обеспечение экономической безопасности

Год набора на ОПОП
2023

Форма обучения
очная

Владивосток 2023

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
38.05.01 «Экономическая безопасность» (ЭБ)	ПКВ-2 : Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга	ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации
		ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-2 «Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации	РД 1	Знание	концепции защиты информации и систем безопасности предприятия и их роль в обеспечении экономической безопасности	ответы на тестовые задания
	РД 2	Умение	обосновывать свой выбор при применении методов и приемов защиты от несанкционированного доступа	корректное выполнение практического задания
	РД 3	Навык	методами анализ угроз информационной безопасности	корректное выполнение практического задания
ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации	РД 4	Знание	методы предупреждения рисков информационной безопасности, влияющих на экономическую безопасность организации	ответы на тестовые задания
	РД 5	Умение	соблюдать требования, установленные к информационной безопасности организации	корректное выполнение практического задания

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и предствление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : концепции защиты информации и системы безопасности предприятия и их роль в обеспечении экономической безопасности	1.1. Основные понятия и определения информационной безопасности	Тест	Список вопросов
		1.2. Государственная система информационной безопасности. Законодательный уровень информационной безопасности	Тест	Список вопросов
РД2	Умение : обосновывать свой выбор при применении методов и приемов защиты от несанкционированного доступа	1.3. Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	Практическая работа	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Практическая работа	Список вопросов
РД3	Навык : методами анализ угроз информационной безопасности	1.2. Государственная система информационной безопасности. Законодательный уровень информационной безопасности	Практическая работа	Список вопросов
		1.3. Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	Практическая работа	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Практическая работа	Список вопросов
РД4	Знание : методы предупреждения рисков информационной безопасности, влияющих на экономическую безопасность организации	1.3. Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	Тест	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Тест	Список вопросов
РД5	Умение : соблюдать требования, установленные к информационной безопасности организации	1.1. Основные понятия и определения информационной безопасности	Практическая работа	Список вопросов

		1.2. Государственная система информационной безопасности. Законодательный уровень информационной безопасности	Практическая работа	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Практическая работа	Список вопросов

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест	Практические задания	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия	20	40		60
Промежуточная аттестация			20	20
Итого	40	40	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, нет очности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры тестовых заданий

Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с

другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. аппелеруемость

В классификацию вирусов по способу заражения входят

1. опасные
2. файловые
3. резидентные
4. загрузочные
5. файлово -загрузочные
6. нерезидентные

Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

1. комплексное обеспечение ИБ
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:

1. компаньон - вирусами
2. черви
3. паразитические
4. студенческие
5. призраки
6. стелс - вирусы
7. макровирусы

К видам системы обнаружения атак относятся :

1. системы, обнаружения атаки на ОС
2. системы, обнаружения атаки на конкретные приложения
3. системы, обнаружения атаки на удаленных БД
4. все варианты верны

Автоматизированная система должна обеспечивать

1. надежность
2. доступность
3. целостность
4. контролируемость

Основными компонентами парольной системы являются

1. интерфейс администратора
2. хранимая копия пароля
3. база данных учетных записей
4. все варианты верны

Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….

1. идентификатор пользователя
2. пароль пользователя
3. учетная запись пользователя
4. парольная система

К принципам информационной безопасности относятся

1. скрытость
2. масштабность
3. системность
4. законность
5. открытости алгоритмов

Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных
5. все варианты верны

Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

1. информационная война
2. информационное оружие
3. информационное превосходство

Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

1. государственная тайна
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

1. конфиденциальность
2. целостность

3. доступность
4. аутентичность
5. аппелеруемость

Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. принцип разумной достаточности
5. принцип гибкости системы

Особенностями информационного оружия являются:

1. системность
2. открытость
3. универсальность
4. скрытность

К функциям информационной безопасности относятся:

1. совершенствование законодательства РФ в сфере обеспечения информационной безопасности
2. выявление источников внутренних и внешних угроз
3. Страхование информационных ресурсов
4. защита государственных информационных ресурсов
5. подготовка специалистов по обеспечению информационной безопасности

Хранение паролей может осуществляться

1. в виде сверток
2. в открытом виде
3. в закрытом виде
4. в зашифрованном виде
5. все варианты ответа верны

Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:

1. ревизором
2. иммунизатором
3. сканером
4. доктора и фаги

К достоинствам технических средств защиты относятся:

1. регулярный контроль
2. создание комплексных систем защиты
3. степень сложности устройства
4. Все варианты верны

К тщательно контролируемым зонам относятся:

1. рабочее место администратора
2. архив
3. рабочее место пользователя

К национальным интересам РФ в информационной сфере относятся:

1. Реализация конституционных прав на доступ к информации
2. Защита информации, обеспечивающей личную безопасность

3. Защита независимости, суверенитета, государственной и территориальной целостности
4. Политическая экономическая и социальная стабильность
5. Сохранение и оздоровлении окружающей среды

Информационная безопасность это:

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
2. Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз
3. Состояние, когда не угрожает опасность информационным системам
4. Политика национальной безопасности России

Наиболее распространенные угрозы информационной безопасности:

1. угрозы целостности
2. угрозы защищенности
3. угрозы безопасности
4. угрозы доступности
5. угрозы конфиденциальности

Что относится к классу информационных ресурсов:

1. Документы
2. Персонал
3. Организационные единицы
4. Промышленные образцы, рецептуры и технологии
5. Научный инструментарий

Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:

1. конфиденциальность
2. доступность
3. аутентичность
4. целостность

Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?

1. Информационный саботаж
2. Физический саботаж
3. Информационные инфекции

Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации
5. Безопасность данных

Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

1. Служебная информация
2. Коммерческая тайна
3. Банковская тайна
4. Конфиденциальная информация

Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. Информационные услуги
5. Информационные продукты

Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. Информационные услуги
5. Информационные продукты

Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

1. Информационная война
2. Информационное оружие
3. Информационное превосходство

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:

1. Защищенность информации
2. Защищаемая информация
3. Защищенность потребителей информации
4. Защита информации

Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

1. Государственная тайна
2. Коммерческая тайна
3. Банковская тайна
4. Конфиденциальная информация

Соотнесите интересы в области информационной безопасности:

1. Национальные интересы
2. Интересы личности
3. Интересы государства
4. Интересы общества

1. состоят в реализации конституционных прав и свобод [2], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина
2. обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями
3. состоят в незыблемости конституционного строя, суверенитета и территориальной

целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправно го и взаимовыгодного международного сотрудничества.

4. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России.

Соотнесите основные методы получения паролей:

1. метод тотального перебора
2. словарная атака
3. получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы
4. проверка паролей, устанавливаемых в системах по умолчанию
5. для перебора используется словарь наиболее вероятных ключей
6. двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей
7. опробываются все ключи последовательно, один за другим
8. пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа.

Шкала оценки

Оценка	Баллы	Описание
5	40	Студент ответил безошибочно
4	39-30	Студент совершил от 1 до 5 ошибок в ответах на тест
3	29-20	Студент совершил от 5 до 15 ошибок в ответах на тест
2	19-0	Студент совершил от 16 и более в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Разбившись на группу 3-5 человек, придумать организацию и разработать для нее концепцию информационной безопасности.

Краткие методические указания

В рамках концепции необходимо отразить следующие пункты:

1. Общие положения Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности

Предприятия.

• Классификации угроз.

• Основные непреднамеренные искусственные угрозы.

• Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности

Предприятия

4.1. Организационное обеспечение информационной безопасности.

• Задачи организационного обеспечения информационной безопасности.

• Подразделения, занятые в обеспечении информационной безопасности.

• Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности

Предприятия.

• Общие положения.

• Защита информационных ресурсов от несанкционированного доступа.

• Средства комплексной защиты от потенциальных угроз.

• Обеспечение качества в системе безопасности.

• Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

• Правовое обеспечение юридических отношений с работниками Предприятия.

• Правовое обеспечение юридических отношений с партнерами Предприятия.

• Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

4.5. Оценить влияние построений системы информационной безопасности на экономическую безопасность предприятия

4.6. Определить необходимые ресурсы для построения системы информационной безопасности.

Шкала оценки

Оценка	Баллы	Описание
5	34-40	Оценка «отлично» выставляется при выполнении работы в установленные сроки, в полном о бъеме и на высоком теоретическом уровне. Студент свободно владеет теоретическим материалом, умеет применить его при решении кейса; на все вопросы дает правильные и обос нованные ответы, убедительно защищает свою точку зрения.
4	26-34	Оценка «хорошо» выставляется при выполнении работы в установленные сроки, в полном об ъеме. Студент достаточно владеет теоретическим материалом, может применять его самостоя тельно или по указанию преподавателя. На большинство вопросов даны правильные ответы, защищает свою точку зрения достаточно обосновано.
3	16-25	Оценка «удовлетворительно» выставляется при выполнении работы в установленные сроки, в основном правильно, но без достаточно глубокой проработки некоторых разделов. Студент усвоил только основные разделы теоретического материала и по указанию преподавателя (бе з инициативы и самостоятельности) применяет его практически; на вопросы отвечает неувере нно или допускает ошибки, неуверенно защищает свою точку зрения.
2	0-15	Оценка «неудовлетворительно» выставляется в случае, если студент не выполняет работу в у становленные сроки. Решения кейса не раскрыто, ответы не полные. Студент не может защит ить свои выводы, допускает грубые фактические ошибки при ответах на поставленные вопро сы или не отвечает на них.

5.3 Экзаменационные вопросы

1 Что такое информационная безопасность?

2 Какие предпосылки и цели обеспечения информационной безопасности?

3 В чем заключаются национальные интересы РФ в информационной сфере?

4 Что включает в себя информационная борьба? Какие пути существуют?

5 Каковы общие принципы обеспечения защиты информации?

6 Какие имеются виды угроз информационной безопасности предприятия (организации)?

7 Какие источники наиболее распространенных угроз информационной безопасности существуют?

8 Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?

9 Что включают в себя требования по обеспечению комплексной системы информационной безопасности?

10 Какие уровни информационной защиты существуют, их основные составляющие?

11 В чем заключается контроль участников взаимодействия?

12 Какие функции выполняет служба регистрации и наблюдения?

13 Какой процесс называется аутентификацией пользователя?

14 Какие схемы аутентификации вы знаете?

15 Какие атаки изнутри вы знаете?

16 Какие атаки системы снаружи вы знаете?

17 Какая программа называется вирусом?

18 Какая атака называется атакой отказа в обслуживании?

19 Какие виды вирусов вы знаете?

20 Какие вирусы называются паразитическими?

21 Как распространяются вирусы?

22 Какие методы обнаружения вирусов вы знаете?

23 Что представляет собой домен?

24 В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?

25 Какие характеристики положены в основу системы классификации информационных систем управления предприятием?

26 Какие задачи решает система компьютерной безопасности?

27 Какие пути защиты информации в локальной сети существуют?

28 Какие задачи решают технические средства противодействия экономическому шпионажу? . Какой порядок организации системы видеонаблюдения?

29 Что включает в себя защита информационных систем с помощью планирования?

30 Какие условия работы оцениваются при планировании?

31 Из каких этапов состоят работы по обеспечению информационной безопасности предприятия? . Что такое мобильные программы?

32 Что представляет собой метод «песочниц»?

33 Что такое интерпретация?

34 Что понимают под политикой информационной безопасности?

35 Что включает в себя политика информационной безопасности РФ?

36 Какие нормативные документы РФ определяют концепцию защиты информации?

Краткие методические указания

Подготовка к опросу проводится в ходе самостоятельной работы студентов и включает в себя повторение пройденного материала по вопросам предстоящего опроса. Помимо основного материала студент должен изучить дополнительную рекомендованную литературу и информацию по теме, в том числе с использованием Интернет-ресурсов.

Шкала оценки

Оценка	Баллы	Описание
5	2	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный ма териал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	1	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по суще ству излагает его, не допуская существенных неточностей в ответе на вопрос, правильно при меняет теоретические положения при решении практических вопросов и задач.
3	0,5	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные форму лировки. Не может связать с практическими примерами.

2	0	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной част и программного материала, допускает существенные ошибки.