Высшая Школа Управления

Негосударственное образовательное частное учреждение высшего образования «Высшая школа управления» (ЦКО)
(НОЧУ ВО «Высшая школа управления» (ЦКО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.14 Основы информационной безопасности

Направление подготовки
38.03.05
«Бизнес-информатика»

Направленность (профиль) подготовки
Информационные системы в бизнесе

Квалификация выпускника
«Бакалавр»
Форма обучения
заочная

Рабочая программа рассмотрена
на заседании кафедры
цифровой экономики и управления и
государственного администрирования
«28» августа 2024, протокол №1

Заведующий кафедрой д.э.н., доцент
Н.Р. Куркина

г. Москва, 2024

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации № 838 от 20 июля 2020 года (зарегистрирован в Минюсте России 19 августа 2020 г. № 59325).

Организация-разработчик: НОЧУ ВО «Высшая школа управления» (ЦКО)

Разработчик: _____

Содержание

1. Цели и задачи освоения дисциплины

Цель дисциплины: формирование у обучающихся системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи дисциплины:

- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;
- формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия;
- формирование навыков настройки и обслуживания аппаратно-программных средств.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к дисциплинам обязательной части блока Б1 «Дисциплины (модули)» учебного плана, согласно ФГОС ВО для направления подготовки 38.03.05 Бизнес-информатика.

3. Планируемые результаты обучения

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Планируемые результаты обучения
ПК-2 Способен осуществлять автоматизацию основных и вспомогательных процессов управления предприятием	ИПК-2.1 Знать методику проведения анализа, моделирования и формирования интегрального представления стратегий и целей, бизнес-процессов и информационно-технологической инфраструктуры предприятий различной отраслевой принадлежности и различных форм собственности, а также учреждений государственного и муниципального управления. ИПК-2.2 Уметь проводить анализ, моделирование и формирование интегрального представления стратегий и целей, бизнес- процессов и информационно- технологической инфраструктуры предприятий различной отраслевой принадлежности и различных форм собственности, а также учреждений государственного и муниципального управления. ИПК-2.3 Владеть навыками формирования информационной базы в процессе сбора и обработки данных для проведения расчета экономических показателей организации	**Знать:** ● Методики проведения анализа, моделирования и формирования комплексного представления стратегий и целей, бизнес-процессов и информационно-технологической инфраструктуры предприятий различной отраслевой принадлежности и форм собственности, а также учреждений государственного и муниципального управления. ● Основы бизнес-ориентированных языков программирования с учётом их преимуществ, недостатков и сфер применения. ● Основы архитектуры предприятия. **Уметь:** ● Проводить анализ, моделирование и формирование комплексного представления о стратегиях и целях, бизнес-процессах и информационно-технологической
ПК-4 Способен разрабатывать приложения на бизнес-ориентированных языках программирования	ИПК-4.1 Знать: основы бизнес-ориентированных языков программирования с учетом их преимуществ, недостатков, сфер применения ИПК-4.2 Уметь: разрабатывать прикладные приложения для профессиональной деятельности ИПК-4.3 Владеть: навыками выбора оптимальных технологий и инструментальных средств разработки оригинального приложения	

ПК-5 Способен осуществлять моделирование архитектуры предприятия	ИПК-5.1 Знать: основы архитектуры предприятия ИПК-5.2 Уметь: моделировать архитектуру предприятия ИПК-5.3 Владеть: навыками моделирования архитектуры предприятия	инфраструктуре предприятий различной отраслевой принадлежности и форм собственности, а также учреждений государственного и муниципального управления. ● Разрабатывать прикладные приложения для профессиональной деятельности. ● Моделировать архитектуру предприятия. **Владеть:** ● Навыками формирования информационной базы в процессе сбора и обработки данных для расчёта экономических показателей организации. ● Навыками выбора оптимальных технологий и инструментальных средств разработки оригинальных приложений. ● Навыками моделирования архитектуры предприятия.

4. Структура и содержание дисциплины (модуля)

4.1 Объем дисциплины и виды учебной работы

Виды учебной работы	Объем в часах
Общая трудоемкость дисциплины	**108 (3 зачетных единицы)**
Контактная работа обучающихся с преподавателем (всего)	10
Аудиторная работа (всего), в том числе:	10
Лекции	4
Семинары, практические занятия	6
Лабораторные работы	
Внеаудиторная работа (всего):	98
в том числе: консультация по дисциплине	
Самостоятельная работа обучающихся (всего)	98
Вид промежуточной аттестации обучающегося	**Зачет с оценкой**

4.2 Тематический план дисциплины

Наименование разделов и тем	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)							Компетенции
		Всего	Из них аудиторные занятия			Самостоятельная работа	Курсовая работа	Контрольная работа	
			Лекции	Лабораторные работы	Практические /семинарские занятия				
Тема 1. Понятие и сущность информационной безопасности и защиты информации	3	12	2		2	8			ПК-2, ПК-4, ПК-5
Тема 2. Становление и развитие понятия «информационная безопасность»	3	12	2		2	8			ПК-2, ПК-4, ПК-5
Тема 3. Правовой уровень обеспечения информационной безопасности	3	12			2	10			ПК-2, ПК-4, ПК-5
Тема 4. Информационная безопасность в системе национальной безопасности РФ	3	12				12			ПК-2, ПК-4, ПК-5
Тема 5. Основы государственной политики РФ в области информационной безопасности	3	10				10			ПК-2, ПК-4, ПК-5

Тема 6. Информационная война, методы и средства её ведения	3	10				10			ПК-2, ПК-4, ПК-5
Тема 7. Методы и средства обеспечения ИБ объектов информационной сферы	3	10				10			ПК-2, ПК-4, ПК-5
Тема 8. Основные угрозы информационной безопасности	3	10				10			ПК-2, ПК-4, ПК-5
Тема 9. Административный уровень обеспечения информационной безопасности	3	10				10			ПК-2, ПК-4, ПК-5
Тема 10. Программно-технический уровень обеспечения защиты информации	3	10				10			ПК-2, ПК-4, ПК-5
Итого		**108**	**4**		**6**	**98**			

4.3 Содержание дисциплины

Тема 1. Понятие и сущность информационной безопасности и защиты информации

Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ.

Тема 2. Становление и развитие понятия «информационная безопасность»

Связь информационной ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.

Тема 3. Правовой уровень обеспечения информационной безопасности

Основные федеральные органы, генерирующие в Российской Федерации, нормативно-правовые акты в сфере ИБ и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.

Тема 4. Информационная безопасность в системе национальной безопасности РФ

Понятие национальной безопасности. Виды безопасности: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечение национальной безопасности государства.

Тема 5. Основы государственной политики РФ в области информационной безопасности

Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Возможные сценарии подрыва национальных интересов РФ.

Тема 6. Информационная война, методы и средства её ведения

Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации.

Тема 7. Методы и средства обеспечения ИБ объектов информационной сферы

Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств

вычислительной техники и автоматизированных информационных систем.

Тема 8. Основные угрозы информационной безопасности

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.

Тема 9. Административный уровень обеспечения информационной

Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки ПИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.

Тема 10. Программно-технический уровень обеспечения защиты информации

Программные сервисы защиты информации в ИС. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потоковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в информационно- телекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.

4.4. Практическая подготовка

Практическая подготовка реализуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Объем занятий в форме практической подготовки составляет 10 часов.

5. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины

5.1 Основная литература

1. Баранов, А. И., Васильев, А. А. Информационная безопасность. Защита информации

/ А. И. Баранов, А. А. Васильев. — 3-е изд., перераб. и доп. — М.: ФОРУМ, 2021. — 384 с.
2. Блинов, А. О., Терехов, А. Н. Информационная безопасность: учебник для вузов / А. О. Блинов, А. Н. Терехов. — М.: Юрайт, 2022. — 496 с.
3. Глинкин, А. А., Капустин, Д. В. Основы информационной безопасности / А. А. Глинкин, Д. В. Капустин. — М.: Академия, 2021. — 432 с.
4. Конотопов, М. Ю. Информационная безопасность: учебное пособие / М. Ю. Конотопов. — СПб.: Питер, 2020. — 416 с.

5.2 Дополнительная литература

1. Гостев, В. Г. Угрозы и защита информационных систем / В. Г. Гостев. — М.: Бином, 2019. — 368 с.
2. Луговской, И. А., Зубков, С. В. Информационная безопасность и защита информации: учебное пособие / И. А. Луговской, С. В. Зубков. — СПб.: Лань, 2021. — 280 с.
3. Полковников, А. А. Политика информационной безопасности Российской Федерации / А. А. Полковников. — СПб.: Питер, 2021. — 296 с.
4. Романец, Ю. В. Основы информационной безопасности: правовые и организационные аспекты / Ю. В. Романец. — М.: Юрайт, 2020. — 352 с.
5. Щербаков, А. П. Информационная война: методы и средства / А. П. Щербаков. — М.: Горячая линия-Телеком, 2020. — 320 с.

5.3 Профессиональные базы данных и информационные справочные системы

1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа)
2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа)
3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)
4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)

5.4 Материально-техническое и программное обеспечение (лицензионное и свободно распространяемое)

Наименование дисциплины (модуля), практик в соответствии с	Наименование специальных помещений и помещений для	Оснащенность специальных помещений и помещений для	Перечень лицензионного программного обеспечения.

учебным планом	самостоятельной работы	самостоятельной работы	
Б1.О.14 Основы информационной безопасности	Кабинет информатики	Учебные места, оборудованные блочной мебелью, компьютерами с выходом в сеть интернет, рабочее место преподавателя в составе стол, стул, тумба, компьютер преподавателя с выходом в сеть интернет, экран, мультимедийный проектор, телевизор, тематические стенды, презентационный материал	Microsoft Windows XP Professional Microsoft Office 2010 Kaspersky Endpoint для бизнеса КонсультантПлюс AdobeReader Cisco WebEx Информационно-коммуникационная платформа «Сферум»
	Аудитория для самостоятельной работы	Учебные места, оборудованные блочной мебелью, компьютерами с выходом в сеть интернет, многофункциональное устройство	

6. Методические указания для обучающихся по освоению дисциплины

6.1 Занятия лекционного и семинарского (практического) типов

Методические указания для занятий лекционного типа. В ходе лекционных занятий обучающемуся необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из основной и дополнительной литературы, рекомендованной преподавателем и предусмотренной учебной программой дисциплины.

Методические указания для занятий семинарского (практического) типа. Практические занятия позволяют развивать у обучающегося творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат

четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Подготовка к практическому занятию включает два этапа. На первом этапе обучающийся планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор основной и дополнительной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку к занятию, которая начинается с изучения основной и дополнительной литературы. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. Далее следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие или по теме, вынесенной на дискуссию (круглый стол), продумать примеры с целью обеспечения тесной связи изучаемой темы с реальной жизнью. Готовясь к докладу или выступлению в рамках интерактивной формы (дискуссия, круглый стол), при необходимости следует обратиться за помощью к преподавателю.

6.2. Самостоятельная работа студентов

Самостоятельная работа студентов предусмотрена учебным планом по дисциплине в объеме 98 часов. Самостоятельная работа реализуется в рамках программы освоения дисциплины в следующих формах:

- работа с конспектом занятия (обработка текста);
- проработка тематики самостоятельной работы;
- написание контрольной работы;
- поиск информации в сети «Интернет» и литературе;
- выполнение индивидуальных заданий;
- подготовка к сдаче зачета с оценкой.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний студентов;
- формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу;
- развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и

самоорганизации;

- развитию исследовательских умений студентов.

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов: библиотека с читальным залом, компьютерные классы с возможностью работы в Интернет, аудитории для самостоятельной работы.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки.

Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.

Контроль самостоятельной работы студентов предусматривает:

-соотнесение содержания контроля с целями обучения;

-объективность контроля;

-валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);

-дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы:

-просмотр и проверка выполнения самостоятельной работы преподавателем;

-организация самопроверки, взаимопроверки выполненного задания в группе;

-обсуждение результатов выполненной работы на занятии;

-проведение письменного опроса;

-проведение устного опроса; организация и проведение индивидуального собеседования;

-организация и проведение собеседования с группой.

7. Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Обучение по дисциплине обучающихся с ограниченными возможностями здоровья (далее – ОВЗ) осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Содержание образования и условия организации обучения, обучающихся с ОВЗ определяются адаптированной образовательной программой, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Освоение дисциплины обучающимися с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ОВЗ.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ОВЗ, индивидуальными программами реабилитации инвалидов (при наличии).

В курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий как оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

– устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

– при необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

Фонд оценочных средств
для текущего контроля и промежуточной аттестации
при изучении дисциплины
Б1.О.14 Основы информационной безопасности

Москва 2024

1. Паспорт фонда оценочных средств

Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
ПК-2 Способен осуществлять автоматизацию основных и вспомогательных процессов управления предприятием	ИПК-2.1 Знать методику проведения анализа, моделирования и формирования интегрального представления стратегий и целей, бизнес-процессов и информационно-технологической инфраструктуры предприятий различной отраслевой принадлежности и различных форм собственности, а также учреждений государственного и муниципального управления. ИПК-2.2 Уметь проводить анализ, моделирование и формирование интегрального представления стратегий и целей, бизнес-процессов и информационно-технологической инфраструктуры предприятий различной отраслевой принадлежности и различных форм собственности, а также учреждений государственного и муниципального управления. ИПК-2.3 Владеть навыками формирования информационной базы в процессе сбора и обработки данных для проведения расчета экономических показателей организации	Текущий контроль: контрольная работа, доклад (реферат) Промежуточный контроль: зачет с оценкой
ПК-4 Способен разрабатывать приложения на бизнес-ориентированных языках программирования	ИПК-4.1 Знать: основы бизнес-ориентированных языков программирования с учетом их преимуществ, недостатков, сфер применения ИПК-4.2 Уметь: разрабатывать прикладные приложения для профессиональной деятельности ИПК-4.3 Владеть: навыками выбора оптимальных технологий и инструментальных средств разработки оригинального приложения	
ПК-5 Способен осуществлять моделирование архитектуры предприятия	ИПК-5.1 Знать: основы архитектуры предприятия ИПК-5.2 Уметь: моделировать	

	архитектуру предприятия ИПК-5.3 Владеть: навыками моделирования архитектуры предприятия	

Этапы формирования компетенций в процессе освоения ОПОП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенций, характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе итоговой аттестации. Дисциплина «Основы информационной безопасности» является промежуточным этапом формирования компетенций ПК-2, ПК-4, ПК-5 в процессе освоения ОПОП.

Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет с оценкой.

2. Оценочные средства

2.1 Текущий контроль

Примерные задания для контрольных работ

Задание 1.

Определите, соответствуют ли ситуация принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации: после проведения аудиторской проверки в государственной организации было выявлено нецелевое использование бюджетных средств. Местные средства массовой информации подготовили публикацию об использовании бюджетных средств, однако руководитель организации запретил публиковать данную информацию.

Задание 2

Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в ситуации: юридическое лицо заключило с таможенным представителем договор представлять свои интересы при оформлении таможенной декларации и помещении товаров под определённую таможенную процедуру при перемещении товаров через таможенную границу Таможенного союза, и предоставил ему информацию о себе, товаре и его назначении.

Задание 3

Гражданин В. подозревался в совершении преступления. В отношении него были

осуществлены оперативно-розыскные действия и собрана информация, в том числе о его личной жизни. Однако виновность В. в совершении преступления не доказана и в отношении него в возбуждении уголовного дела отказано. Так как В. располагает фактами проведения в отношении него оперативно-розыскных мероприятий и полагает, что при этом были нарушены его права, вправе ли он истребовать сведения о полученной информации о нем.

Задание 4

Проведите анализ информационно-правовой нормы и определите вид формы предписания: организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям системы менеджмента информационной безопасности, с целью предотвратить их повторное появление.

Задание 5

Центральный банк РФ для анализа экономической ситуации запросил у АО «Тюмень Нефть» информацию о количестве полученной прибыли за прошедший год и о прогнозах объёма добычи нефти на текущий год. Однако АО не предоставило истребуемой информации, мотивировав тем, что информация отнесена к коммерческой тайне. Имеет ли право Банк России получать данную информацию, и несёт ли ответственность Банк России, а также его должностные лица и работники за разглашение коммерческой тайны.

Шкала и критерии оценивания контрольных работ

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся глубоко и содержательно раскрывает тему контрольной работы, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«хорошо»	Обучающийся в целом раскрывает тему контрольной работы, однако ответ не носит развернутого и исчерпывающего характера.
«удовлетворительно»	Обучающийся в целом раскрывает тему контрольной работы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«*неудовлетворительно*»	Обучающийся не владеет выбранной темой контрольной работы. Тема контрольной работы не раскрыта

Примерный перечень тем для докладов (рефератов)

1. Основные термины по дисциплине организационной и правовой защите информации, их значение и назначение в обеспечении безопасности информации.

2. Нормативные правовые акты и методические документы в области обеспечения безопасности информации, российские и международные стандарты.
3. Концепция и роль организационно-правовых методов в обеспечении информационной безопасности.
4. Организационно-режимные и правовые методы по защите конфиденциальной информации на предприятие.
5. Организационно-режимные и правовые методы по защите коммерческой тайны на предприятие.
6. Компьютерные преступления с использованием высоких технологий, меры дисциплинарной, административной и уголовной ответственности.
7. Нормативные правовые акты и методические документы в области обеспечения безопасности информации, российские и международные стандарты.
8. Методика и организационно-правовые методы построения СЗИ.
9. Концепция и роль организационно-правовых методов в обеспечении информационной безопасности.
10. Место и значение дисциплины ОиОИБ в общем перечне курсов специальности «Организация и технология защиты информации».

Шкала и критерии оценивания докладов (рефератов)

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся глубоко и содержательно раскрывает тему доклада, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер
«хорошо»	Обучающийся в целом раскрывает тему доклада, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«удовлетворительно»	Обучающийся в целом раскрывает тему доклада и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности
«неудовлетворительно»	Обучающийся не владеет выбранной темой

2.2 Промежуточная аттестация

Примерные вопросы к зачету с оценкой

Тема 1. Понятие и сущность информационной безопасности и защиты информации

1. Дайте определение нормативно-правового обеспечения информационной безопасности, цели и решаемые задачи.
2. Дайте определение информационной безопасности (ИБ) и защите информации.
3. Перечислите основные компоненты информационной безопасности государства.

Тема 2. Становление и развитие понятия «информационная безопасность»

4. Определите связь информационной безопасности с информатизацией общества.
5. Перечислите базовые уровни обеспечения информационной безопасности и защиты информации.

Тема 3. Правовой уровень обеспечения информационной безопасности

6. Назовите основные федеральные органы, генеририрующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации.
7. Перечислите цели и задачи Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну.
8. Дайте определение коммерческой тайны и ее роль в системе предпринимательской деятельности.
9. Перечислите основания для отнесения сведений к коммерческой тайне.
10. Перечислите сведения, которые могут быть отнесены и которые нельзя относить к коммерческой тайне.
11. Перечислите содержание методики порядка формирования ведомственного перечня сведений конфиденциального характера.

Тема 4. Информационная безопасность в системе национальной безопасности РФ

12. Дайте определение национальная безопасность государства.
13. Перечислите виды защищаемой информации.
14. Соотношение безопасности личности, общества и государства.
15. Назовите роль и значение информационной безопасности в национальной безопасности Российской Федерации.

Тема 5. Основы государственной политики РФ в области информационной безопасности

16. Перечислите национальные интересы Российской Федерации в информационной сфере.
17. Назовите угрозы национальной безопасности Российской Федерации.
18. Перечислите возможные сценарии подрыва национальных интересов Российской Федерации.

Тема 6. Информационная война, методы и средства её ведения

19. Перечислите виды информационного оружия, его классификация и возможности.
20. Дайте определение целостности и доступности информации.
21. Перечислите искусственные и естественные каналы утечки информации.

Тема 7. Методы и средства обеспечения ИБ объектов информационной сферы

22. Дайте определение обеспечение информационной безопасности.
23. Перечислите правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
24. Перечислите модели, стратегии и системы обеспечения информационной безопасности.

Тема 8. Основные угрозы информационной безопасности

25. Перечислите виды угроз безопасности информации по цели реализации угрозы, принципу, характеру и способу её воздействия.
26. Назовите особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки.

27. Перечислите основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС).
28. Назовите базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России.
29. Перечислите основные задачи по защите информационных ресурсов от реализации угроз.

Тема 9. Административный уровень обеспечения информационной безопасности

30. Назовите концептуальные основы обеспечения информационной безопасности, её цели и этапы построения.
31. Назовите основные положения политики информационной безопасности, как основа административных мер по защите информации на предприятии.
32. Назовите структуру и содержание документа, характеризующего политику безопасности, и основные этапы разработки.
33. Перечислите задачи, решаемые при анализе рисков для информационных ресурсов.
34. Перечислите базовые методики, используемые для оценки рисков.
35. Перечислите Основные стандарты в области разработки информационной безопасности и анализа рисков.
36. Перечислите основные принципы реализации ПИБ.

Тема 10. Программно-технический уровень обеспечения защиты информации

37. перечислите программные сервисы защиты информации в информационных системах.
38. Дайте определение идентификация и аутентификация пользователей как передовой рубеж защиты информации.
39. Перечислите базовые методы парольной аутентификации. Модели разграничения доступа к информации.
40. Дайте определение протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности.
41. Перечислите базовые методы криптографического преобразования данных.
42. Дайте определение потоковое и блочное шифрование.
43. Дайте определение экранирование информации в информационно-телекоммуникационных сетях
(ИТС).
44. Дайте определение компьютерный вирус и вредоносная программа: классификация, методы и средства борьбы с ними.

Шкала и критерии оценивания зачета с оценкой

Шкала оценивания	Критерии оценивания
«отлично»	оценка соответствует повышенному уровню и выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно

	обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«хорошо»	оценка соответствует повышенному уровню и выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос или выполнении заданий, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
«неудовлетворительно»	оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.