Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 10 » июля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Информационная безопасность
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: бакалавриат
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 38.03.01 Экономика
(код и наименование направления)

Направленность: Экономика (общий профиль, СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - изучение принципов обеспечения информационной безопасности и защиты информации, подходов к анализу угроз безопасности и освоение компетенций для решения основных задач обеспечения информационной безопасности деятельности предприятий и организаций
Задачи дисциплины:
- изучение основных понятий в области информационной безопасности и защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности для бизнес-процессов предприятий и организаций;
- изучение способов и средств обеспечения информационной безопасности, основных сервисов защиты информации, критериев оценки защищенности информационных систем;
- приобретение умений в организации деятельности по обеспечении личной и корпоративной информационной безопасности, применения отдельных способов и средств защиты информации.

1.2. Изучаемые объекты дисциплины

- основные понятия, общеметодологические принципы теории информационной безопасности;
- виды информации ограниченного доступа;
- угрозы безопасности информации и уязвимости информационных систем;
- основные методы нарушения конфиденциальности, целостности и доступности информации;
- причины, виды каналы утечки информации и несанкционированного доступа;
- уровни и сервисы защиты информации;
- способы и средства защиты информации;
- критерии оценки защищенности информационных систем;
- основы организации защиты информации на предприятии.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-5.6	ИД-1ПК-5.6	Знает основы обеспечения информационной безопасности и защиты информации в деятельности предприятий и организаций	Знает основы экономики, финансового менеджмента, информатики, защиты информации , Законодательство РФ и методические документы по финансовому анализу, бюджетированию и управлению денежными потоками	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-5.6	ИД-2ПК-5.6	Умеет учитывать требования по обеспечению информационной безопасности, при определении объема и планировании работ по финансовому анализу бюджетированию и управлению денежными потоками, принятии решения по корректировке стратегии и тактике в области финансовой политики.	Умеет определять объем и планировать работы по финансовому анализу бюджетированию и управлению денежными потоками, вырабатывать сбалансированные решения по корректировке стратегии и тактике в области финансовой политики. Вносить соответствующие изменения в финансовые планы (сметы, бюджеты, бизнес-планы).	Отчёт по практическому занятию
ПК-5.6	ИД-3ПК-5.6	Владеет навыками учета основных способов обеспечения информационной безопасности при разработке финансовой политики экономического субъекта и осуществлении мер по обеспечению ее финансовой устойчивости.	Владеет навыками разработки финансовой политики экономического субъекта и осуществления мер по обеспечению ее финансовой устойчивости.	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	18	18
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	32	32
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	90	90
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
8-й семестр				
Основные понятия и задачи обеспечения информационной безопасности	2	0	4	8
Сущность и значение информации в развитии современного общества. Задачи защиты информации на предприятии. Взаимосвязь информационных и экономических процессов. Основные понятия в области информационной безопасности. Конфиденциальность, целостность и доступность информации. Уровни обеспечения информационной безопасности				
Сущность и виды информации ограниченного доступа	2	0	6	10
Понятие, сущность и виды информации ограниченного доступа. Виды конфиденциальной информации в деятельности предприятия. Особенности сведений, составляющих коммерческую тайну. Персональные данные, как вид конфиденциальной информации. Объекты защиты информации				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Угрозы и риски информационной безопасности в деятельности предприятий и организаций	2	0	4	10
Понятие угрозы безопасности информации. Классификация угроз безопасности информации. Актуальные угрозы безопасности информации в деятельности предприятия. Утечка информации и несанкционированный доступ. Обеспечение открытости информационных ресурсов. Модель нарушителя. Оценка рисков информационной безопасности.				
Правовая защита информации	2	0	2	10
Понятие и структура правовой защиты информации. Основные международные нормы и внутригосударственные нормативно-правовые документы в области обеспечения информационной безопасности. Ответственность за нарушение законодательства в информационной сфере.				
Правовое регулирование процессов защиты информации на предприятии	2	0	4	12
Требования к оформлению внутренних документов предприятия. Порядок разработки внутренней организационно-распорядительной документации по защите информации. Нормативное закрепление состава защищаемой информации				
Организация защиты информации на предприятии	2	0	4	10
Сущность организационных мер защиты информации. Организация охраны и режима. Организация работы с персоналом в системе защиты информации. Организация работы с документами. Понятия управления информационной безопасностью.				
Способы и средства защиты информации	2	0	4	10
Понятие способов и средств защиты информации. Техника защиты информации и ее применение. Средства физической, программно-технической, криптографической защиты информации. Порядок применения электронной подписи				
Особенности обеспечения информационной безопасности от	2	0	2	10
Особенности требований по защите сведений, составляющих коммерческую и банковскую тайну. Требования по защите персональных данных. Обеспечение информационной безопасности объектов критической информационной инфраструктуры				
Порядок разработки комплексной системы защиты информации на предприятии	2	0	2	10
Порядок реализации требований по обеспечению				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
безопасности информации. Политика информационной безопасности. Последовательность создания системы защиты информации на предприятии. Аудит информационной безопасности предприятия.				
ИТОГО по 8-му семестру	18	0	32	90
ИТОГО по дисциплине	18	0	32	90

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Сущность и значение информации в развитии современного общества
2	Основные понятия и задачи в области обеспечения информационной безопасности и защиты информации
3	Понятие, сущность и виды информации ограниченного доступа
4	Разработка перечня сведений конфиденциального характера (ПЗ)
5	Актуальные угрозы безопасности информации и их классификация. Разработка модели нарушителя (ПЗ)
6	Оценка рисков информационной безопасности
7	Особенности правовой защиты информации на предприятии
8	Ответственность за нарушение законодательства в информационной сфере.
9	Порядок разработки внутренней организационно-распорядительной доку-ментации по защите информации
10	Организация охраны и режима на предприятии (ПЗ)
11	Организация работы с персоналом в системе защиты информации (ПЗ)
12	Современные способы и средства защиты информации на предприятии
13	Порядок применения электронной подписи и средств защиты информации
14	Особенности обеспечения информационной безопасности отдельных категорий информации ограниченного доступа
15	Общий порядок создания системы защиты информации на предприятии
16	Аудит информационной безопасности

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические и семинарские занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Анисимов А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2010.	2
2	Информационная безопасность : учебное пособие / С. В. Петров [и др.]. - Новосибирск Москва: АРТА, 2012.	1
3	Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. - Санкт-Петербург: БХВ-Петербург, 2003.	3
4	Садердинов А. А. Информационная безопасность предприятия : учебное пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - Москва: Дашков и К, 2004.	13

5	Ч. 1. - Старый Оскол: , ТНТ, 2007. - (Обеспечение информационной безопасности машиностроительных предприятий : учебное пособие для вузов; Ч. 1).	2
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Галатенко В. А. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2010.	1
2	Данилов А. Н. Основы информационной безопасности : учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. - Пермь: Изд-во ПГТУ, 2008.	62
3	Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2011.	2
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Обеспечение информационной безопасности бизнеса	https://pqm-online.com/assets/files/lib/books/andrianov.pdf	сеть Интернет; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных уязвимостей CVE Mitre	https://cve.mitre.org/
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечная система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность»
Приложение к рабочей программе дисциплины

Направление:	**38.03.01«Экономика»**
Профиль программы бакалавриата:	Экономика предприятий и организаций Финансовые технологии в цифровой экономике
Квалификация выпускника:	**Бакалавр**
Выпускающая кафедра:	Экономики и финансов
Форма обучения:	Очная

Курс: 4 **Семестр**: 8

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Диф. зачет: 8 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (8-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим заданиям и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ПЗ**	**Т/КР**		**Зачет**
Усвоенные знания						
З.1 Знать основы обеспечения информационной безопасности и защиты информации в деятельности предприятий и организаций		ТО1 ТО2 ТО3 ТО4	ПЗ1 ПЗ 2 ПЗ 3 ПЗ 5	Т		ТВ
Освоенные умения						
У.1 Уметь учитывать требования по обеспечению информационной безопасности, при определении объема и планировании работ по финансовому анализу бюджетированию и управлению денежными потоками, принятии решения по корректировке стратегии и тактике в области финансовой политики			ПЗ 4 ПЗ 6 ПЗ 7 ПЗ 12 ПЗ 13 ПЗ 14	Т		ПЗ
Приобретенные владения						
В.1 Владеть навыками учета основных способов обеспечения информационной безопасности при разработке финансовой политики экономического субъекта и осуществлении мер по обеспечению ее финансовой устойчивости			ПЗ 8 ПЗ 9 ПЗ 10 ПЗ 11 ПЗ 15 ПЗ 16	Т		КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1. Проблемы региональной информационной безопасности.

Тема 2. Общеметодологические принципы теории информационной безопасности.

Тема 3. Основные понятия информационной безопасности.

Тема 4. Понятие интеллектуальной собственности и особенности ее защиты.

Тема 5. Основные элементы канала реализации угрозы безопасности информации.

Тема 6. Информационная война как способ воздействия на информационные системы различного назначения и объекты критической информационной инфраструктуры.

Тема 7. Туннелирование, как сервис информационной безопасности.

Тема 8. Ролевое управление доступом. Назначение формальных моделей безопасности. Варианты моделей защиты и сущность политики безопасности. Формальные модели целостности.

Тема 9. Комплексные решения в обеспечении защиты информации, SOC-центры.

Тема 10. Стандарты по управлению информационной безопасностью ISO/IEC 27000. Критерии оценки безопасности компьютерных систем «Оранжевая книга».Общие критерии безопасности информационных технологий. Основные руководящие документы ФСТЭК России, определяющие требования по защите информации.

Тема 11. Средства криптографической защиты информации и электронной подписи.

Тема 12. Системы обнаружения/предотвращения вторжений (IDS/IPS).

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 16 практических (семинарских) занятий. Темы практических (семинарских) занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для

проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Стратегия национальной безопасности Российской Федерации. Стратегические национальные приоритеты обеспечения национальной безопасности РФ.
2. Доктрина информационной безопасности Российской Федерации. Национальные интересы РФ в информационной сфере.
3. Основные угрозы информационной безопасности РФ и основные направления по обеспечению информационной безопасности РФ.
4. Роль специалиста по защите информации в обеспечении национальной безопасности государства.
5. Основные понятия информационной безопасности и их источники.
6. Общеметодологические принципы теории информационной безопасности.
7. Понятие и сущность информации ограниченного доступа. Особенности доступа и ограничения доступа к информации.
8. Права и обязанности обладателя информации.
9. Виды информации ограниченного доступа. Перечень сведений конфиденциального характера.
10. Понятие интеллектуальной собственности и особенности ее защиты.
11. Понятие угрозы безопасности информации.
12. Факторы, воздействующие на информацию. Типы дестабилизирующих факторов.
13. Классификация и виды угроз информационной безопасности.
14. Внутренние и внешние источники угроз безопасности информации.
15. Угрозы утечки информации и угрозы несанкционированного доступа.
16. Основные элементы канала реализации угрозы безопасности информации.
17. Субъекты и цели информационного противоборства.
18. Способы, принципы и стадии информационного противоборства.
19. Информационное оружие, его классификация и возможности.
20. Информационная война как способ воздействия на информационные системы.
21. Использования социальных сетей в информационных войнах.
22. Информационная безопасность объектов критической информационной инфраструктуры.
23. Использование кибернетического оружия в информационной войне.

24. Автоматизированная система, как объект информационной безопасности.

25. Уровни информационной безопасности объекта оценки информационных технологий.

26. Характеристика законодательного, административного и процедурного уровней информационной безопасности.

27. Перечень сервисов безопасности программно-технического уровня.

28. Идентификация и аутентификация как сервисы безопасности.

29. Управление доступом и его виды. Авторизация как сервис безопасности.

30. Протоколирование, аудит и управление, как сервисы безопасности.

31. Экранирование, туннелирование и анализ защищенности как сервисы безопасности.

32. Основные способы защиты информации и их характеристика.

33. Понятие и классификация средств защиты информации. Техника защиты информации.

34. Средства физической, криптографической и программно-технической защиты информации.

35. Перечень и характеристика разновидностей современных средств защиты информации.

36. Понятие и структура правовой защиты информации. Основные международные нормы и внутригосударственные нормативно-правовые документы в области обеспечения информационной безопасности.

37. Ответственность за нарушение законодательства в информационной сфере.

38. Основные административные регламенты по обеспечению информационной безопасности объектов информатизации предприятий нефтегазового комплекса.

39. Сущность организационных мер защиты информации. Организация охраны и режима.

40. Организация работы с персоналом в системе защиты информации.

41. Организация работы с документами в системе защиты информации.

42. Понятия управления информационной безопасностью.

43. Организация защиты персональных данных и объектов критической информационной инфраструктуры.

44. Классификация технических каналов утечки информации.

45. Структура канала утечки информации.

46. Способы и основные средства защиты информации от утечки по техническим каналам.

47. Характеристика организационных и технических мер по защите от утечки информации.

48. Криптография и криптографическая защита информации. Основные понятия.

49. Управление криптографическими ключами. Протокол Kerberos.

50. Понятие и классы Хэш-функции. Алгоритм SHA-1

51. Средства шифрования и электронной подписи. Виды и классификация электронных подписей.

Типовые практические задания для контроля освоенных умений:

1. Определить виды информации ограниченного доступа, обрабатываемые на объекте информатизации.
2. Определить состав носителей информации ограниченного доступа.
3. Изучить порядок формирования и структуру Базы данных (список) уязвимостей информационных систем.
4. Проанализировать деятельность организации (предприятия), выявить уязвимости информационной системы.
5. Классифицировать состав угроз информационной безопасности.
6. Определить состав характерных угроз информационной безопасности для автоматизированной системы.
7. Определить содержание административного уровня обеспечения информационной безопасности (перечислить основные нормативные документы, которые разрабатываются на объекте информатизации и обеспечивают его информационную безопасность).
8. Определить содержание процедурного уровня обеспечения информационной безопасности предприятия (перечислить применяемые процедурные меры).
9. Определить состав применяемых сервисов безопасности программно-технического уровня для варианта автоматизированной системы, с учетом особенностей объекта информатизации.
10. Сформировать матрицу (оформить рисунок) полномочий доступа для варианта информационной системы. При условии большого количества пользователей – фрагмент матрицы.
11. Оптимизировать состав матрицы управления доступа за счет введения ролевого управления доступом.
12. Сформировать перечень основных мер по обеспечению безопасности информации для ИСПДн 1,2,3,4 УЗ.
13. Предложить состав мер по противодействию утечке информации на объекте информатизации.
14. Выполнить практическое задание по реализации функции шифрования, с использованием ОС Windows, в соответствии с Приложением.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.

Приложение 1.

Образец теста для текущего тестирования

Тест по дисциплине «Информационная безопасность»

Модуль «Понятие и сущность информационной безопасности»

Тема 1. Основные понятия и задачи обеспечения информационной безопасности

Группа _____ **ФИО _____**

1. **Информация, имеющая интеллектуальную ценность для организации и предприятия, обычно разделяется на _____ вида(ов):**
   a) *пять;*
   b) *четыре;*
   c) *три;*
   d) *два.*
2. **Не являются конфиденциальными документы содержащие:**
   a) *банковскую тайну;*
   b) *профессиональную тайну;*
   c) *государственную тайну;*
   d) *служебную тайну.*
3. **Сложившееся или организованное в пределах информационной системы движение данных в определенном направлении, называется:**
   a) *документооборотом;*
   b) *документопотоком;*
   c) *делопроизводством;*
   d) *документоведением.*
4. **Документы, направляемые вышестоящими органами власти и управления подчиненным организациям, составляют:**
   a) *нисходящий документопоток;*
   b) *восходящий документопоток;*
   c) *горизонтальный документопоток;*
   d) *вертикальный документооборот.*
5. **Основу принципа избирательности в доставке и использовании конфиденциальной информации составляет действующая в фирме:**
   a) *разделительная (запретительная) система доступа персонала к конфиденциальной информации, документам и базам данных;*
   b) *избирательная (ограничительная) система доступа персонала к конфиденциальной информации, документам и базам данных;*
   c) *разрешительная (разграничительная) система доступа персонала к конфиденциальной информации, документам и базам данных;*
   d) *разрешительная (запретительная) система доступа персонала к конфиденциальной информации, документам и базам данных.*

Приложение 2.

Образец теста для рубежного тестирования

Тест по дисциплине Информационная безопасность

Модуль «Организация защиты информации от угроз информационной безопасности»

Группа _____ **ФИО _____**

1. **Упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих перед функциональными элементами (стадиями) документопотока называется:**
   a. *технологическая схема обработки и хранения конфиденциальных документов;*
   b. *техническая система по обработке и хранению конфиденциальных документов;*
   c. *технологическая система обработки и хранения конфиденциальных документов;*
   d. *технологическая система обработки документопотока.*
2. **Ведение конфиденциального делопроизводства централизуется в едином подразделении аппарата управления — службе КД, функционально _____с подразделением, обрабатывающим открытые документы.**
   a. *связанной;*
   b. *не связанной;*
   c. *подчиненной;*
   d. *соподчиненной.*
3. **Автоматизированные системы делопроизводственной ориентации имеют в большинстве случаев _____ характер и функционируют _____ с традиционной технологией обработки и хранения бумажных документов.**
   a. *информационно-справочный…одновременно;*
   b. *распорядительный …независимо;*
   c. *информационно-справочный…независимо;*
   d. *распорядительный…одновременно.*
4. **Рассмотрение и исполнение электронных конфиденциальных документов и электронных аналогов бумажных документов допускается только при наличии _____системы защиты компьютеров и локальной сети.**
   a. *надежной;*
   b. *специально разработанной;*
   c. *технически оснащенной;*
   d. *сертифицированной.*
5. **Учет конфиденциальных документов, прежде всего, преследует цель:**
   a. *конфиденциальности документов и возможности их контроля;*
   b. *защиты документов от копирования и контроля их наличия;*
   c. *защиты их от подделки и раскрытия фактов мошенничества;*
   d. *сохранности документов и фиксирования их местонахождения.*
6. **В предметном и технологическом аспектах учет конфиденциальных документов отличается от регистрации открытых документов, тем, что организуется:**
   a. *учет входящих документов;*
   b. *учет подготовленных исходящих и внутренних документов;*
   c. *учет пакетов (конвертов), содержащих документы;*
   d. *инвентарный учет документов.*
7. **Основой индексирования (присвоения условного обозначения, имени) конфиденциального документа является валовая нумерация всего потока документов в течение _____.**
   a. *месяца;*
   b. *квартала;*
   c. *полугодия;*
   d. *календарного года.*
8. **Сведения, включаемые в учетную форму при регистрации конфиденциальных документов, всегда разделяются на блока(ов):**
   a. *два;*
   b. *три;*
   c. *четыре;*
   d. *пять.*
   e. *заверяется его подписью …одной чертой.*
9. **На инвентарный учет не берутся следующие конфиденциальные документы:**
   a. *не включенные в номенклатуру дел и не подлежащие подшивке в дела;*
   b. *изъятые по какой-либо причине из дела документы;*
   c. *исходящие документы;*

d. *бумажные или технические носители информации.*

10. **Автоматизированный учет конфиденциальных документов не предусматривает следующей процедуры:**
    a. *контроль доступа к конфиденциальной информации;*
    b. *ввод исходных сведений о документах в автоматизированный банк данных;*
    c. *распечатка на бумажном носителе исходных учетных сведений о документах;*
    d. *ежедневная проверка правильности регистрации документов и их наличия;*
11. **Если документ поступил с грифом ограничения доступа, то этот гриф _____, если документ не входит в число конфиденциальных для данной фирмы.**
    a. *должен быть снят;*
    b. *не может быть снят;*
    c. *может быть снят;*
    d. *может быть понижен.*
12. **Информация и документы, отнесенные к коммерческой тайне, имеют несколько уровней грифа ограничения доступа, соответствующих различным степеням конфиденциальности информации:**
    a. *секретно, совершенно секретно;*
    b. *конфиденциально, строго конфиденциально;*
    c. *конфиденциально, особой важности;*
    d. *для служебного пользования, коммерческая тайна.*
13. **На документах, содержащих сведения, отнесенные к служебной тайне, ставится гриф:**
    a. *служебная тайна;*
    b. *конфиденциальная информация;*
    c. *для служебного пользования;*
    d. *секретно.*
14. **Гриф конфиденциальности присваивается документу:**
    a. *председателем экспертной комиссии;*
    b. *исполнителем при подготовке к составлению проекта документа;*
    c. *начальником службы безопасности;*
    d. *начальником отдела конфиденциального делопроизводства.*
15. **Все типы носителей конфиденциальной документированной информации должны быть учтены:**
    a. *до составления проекта будущего документа;*
    b. *после составления проекта будущего документа;*
    c. *во время составления проекта будущего документа;*
    d. *во время проведения годовой проверки делопроизводства.*
16. **Неподписанные или неутвержденные проекты подготовленных конфиденциальных документов со всеми материалами, а также черновики документов:**
    a. *уничтожаются исполнителем;*
    b. *хранятся в сейфе у исполнителя;*
    c. *сдаются непосредственному начальнику;*
    d. *сдаются в службу КД для уничтожения.*
17. **Разрешением на отправку конфиденциального документа является:**
    a. *подписанное первым руководителем фирмы сопроводительное письмо к документу;*
    b. *приказ первого руководителя фирмы;*
    c. *виза руководителя на документе;*
    d. *разрешение начальника отдела КД.*
18. **Конфиденциальные текущие и архивные дела хранятся:**
    a. *на рабочих местах исполнителей в сейфах;*
    b. *централизованно в службе КД;*
    c. *в рабочих папках исполнителей;*
    d. *централизованно в секретных архивах.*
19. **Без составления акта уничтожаются:**
    a. *дела, включенные в номенклатуру дел;*
    b. *картотеки (журналы) учета конфиденциальных документов;*
    c. *внутренние описи документов;*
    d. *подлинники видео-, аудиодокументов.*