МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.15
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы комплексной системы защиты информации
(наименование дисциплины)

по направлению подготовки

38.03.01 Экономика

направленность (профиль)

Финансовый контроль и экономическая безопасность организаций

Форма обучения: заочная

Год набора: 2019

Общая трудоемкость: 4 ЗЕ

Распределение часов дисциплины

Курс	**5**	**Итого**
Форма контроля / **Вид занятий**	**зачёт**	
Лекции	4	4
Лабораторные	2	2
Практические	6	6
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,25	0,25
Контактная работа	12,25	12,25
Самостоятельная работа	128	128
Контроль	3,75	3,75
Итого	144	144

Рабочую программу составил:
Доцент департамента бакалавриата (экономических и управленческих программ),
к.э.н., доцент Филиппова О.А.

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

[*] Отсутствует

[ ] Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана специальности 38.03.01 Экономика, направленность (профиль): Финансовый контроль и экономическая безопасность организаций.

Срок действия рабочей программы дисциплины до «31» августа 2024 г.

УТВЕРЖДЕНО

На заседании департамента бакалавриата (экономических и управленческих программ)

(протокол заседания №1 от «01» сентября 2020 г.).

1. Цель освоения дисциплины

Цель освоения дисциплины – формирование целостной системы знаний о подходах к управлению комплексными системами защиты информации (КСЗИ), навыков профессиональной эксплуатации современного электронного оборудования и программного обеспечения комплексных систем защиты информации с учетом применения различных подходов к автоматизации и информатизации предприятий и организаций; опыта работы с нормативной документацией, регламентирующей процессы функционирования комплексных систем защиты информации. в том числе в условиях неопределенности и риска.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: «Цифровая культура», «Правоведение», «Экономико-правовое сопровождение бизнеса», «Экономическая и информационная безопасность» и «Экономические информационные системы».

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: «Расследование экономических преступлений».

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-2 - Способен организовать проведение анализа информации по результатам проведения контрольных мероприятий для выявления значимых отклонений от требований правовой и нормативной базы и внутренних регламентов	ПК-2.4 Проводит контрольные мероприятия для выявления значимых отклонений от требований правовой и нормативной базы и внутренних регламентов в различных сферах профессиональной деятельности ПК-2.5 Организует проведение анализа информации по результатам проведения контрольных мероприятий в сфере защиты информации	Знать: требования правовой и нормативной базы и внутренних регламентов в различных сферах профессиональной деятельности
		Уметь: проводить контрольные мероприятия для выявления значимых отклонений от требований правовой, нормативной базы, внутренних регламентов и проводить анализ их результатов
		Владеть: навыками применения нормативно-правовых знаний в профессиональной деятельности для организации анализа информации по результатам проведения контрольных мероприятий и принятия соответствующих управленческих решений в сфере защиты информации

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
1. Базовые понятия сущности комплексных систем защиты информации. Историческое развитие экономической безопасности.	Лек	Сущность и задачи комплексной системы защиты информации (КСЗИ). Этапы исторического развития экономической и информационной безопасности.	5	0,4	10	-	Тестирование Отчёт по практической работе №1
	Пр			-			
	Ср			12			
	Лек	Принципы организации и этапы разработки КСЗИ. Факторы, влияющие на организацию КСЗИ.	5	0,4		-	
	Пр			-			
	Ср			12			
	Лек	Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты.	5	0,4		-	
	Пр			1			
	Ср	Практическая работа № 1. Определение объектов защиты и выделение угроз информационной безопасности предприятия (10 баллов)		16			
2 Сущностная характеристика компонентов КСЗИ и определение условий их функционирования	Лек	Идентификация информационных активов предприятия или организации.	5	0,4	30	-	Отчёт по практическим работам №2,3
	Пр			-			
	Ср			12			
	Лек	Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.	5	0,4		-	
	Пр			2			
	Ср	Практическая работа № 2. Анализ рисков информационной безопасности. Разработка формализованной и неформализованной политики информационной безопасности на предприятии. (15 баллов) Практическая работа № 3. Разработка структуры КСЗИ на предприятии. (15 баллов)		16			
	Лек	Определение потенциальных каналов и методов несанкционированного доступа к информации.	5	0,4	15	-	Отчёт по практической работе №4

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
	Пр			-			
	Ср			12			
	Лек	Определение возможностей несанкционированного доступа к защищаемой информации.	5	0,4		-	
	Пр			1			
	Ср	Практическая работа № 4. Разработка нормативно-правовой и организационно-методической подсистем КСЗИ предприятия (15 баллов)		12			
3. Разработка и экономическая оценка модели КСЗИ	Лек	Технологическое и организационное построение КСЗИ.	5	0,4	-	-	Тестирование
	Пр			-			
	Ср			12			
	Лек	Назначение, структура и содержание управления КСЗИ. Принципы и методы планирования функционирования КСЗИ.	5	0,4	45	-	Тестирование Отчёт по практическим работам №5,6 Отчёт по лабораторной работе
	Пр			2			
	Ср	Практическая работа № 5. Разработка модели инженерно-технической подсистемы КСЗИ на предприятии (15 баллов) Практическая работа № 6. Разработка модели программно-аппаратной подсистемы КСЗИ на предприятии (15 баллов)		12			
	Лек	Сущность и содержание контроля функционирования КСЗИ. Состав методов и моделей оценки эффективности КСЗИ. Лабораторная работа. Построение модели оценки эффективности КСЗИ с помощью инструментов MS Excel. (15 баллов)	5	0,4		-	
	Лаб.раб			2			
	Ср			12			

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Промежуточная аттестация			5	0,25		-	
Контроль			5	3,75	100	-	Итоговое тестирование (Вопросы к зачёту)
			Итого:	144	100		

Схема расчета итогового балла:
(Текущий рейтинг + Результат итогового тестирования)/2

5. Образовательные технологии

С целью формирования компетенций у студентов в учебном процессе используется: технология традиционного обучения.

6. Методические указания по освоению дисциплины

Изучение дисциплины предусматривает чтение лекций, проведение практических занятий, самостоятельное изучение специальной литературы по вопросам программы, заданий из соответствующего практикума.

Виды самостоятельной работы студентов:

1. повторение пройденного учебного материала, чтение рекомендованной литературы;
2. подготовка к практическим и лабораторным занятиям;
3. работа с электронными источниками;
4. подготовка к сдаче зачета.

Изучение теоретического материала определяется рабочей учебной программой дисциплины, включенными в нее календарным планом изучения дисциплины и перечнем литературы; рекомендуется при подготовке к занятиям повторить материал предшествующих тем рабочего учебного плана, а также материал предшествующих учебных дисциплин, который служит базой изучаемого раздела данной дисциплины.

При подготовке к практическому или лабораторному занятию необходимо изучить материалы лекции, рекомендованную литературу. Изученный материал следует проанализировать в соответствии с планом занятия, затем проверить степень усвоения содержания вопросов.

При подготовке к зачету следует руководствоваться перечнем вопросов для подготовки к итоговому контролю по курсу. При этом необходимо уяснить суть основных понятий дисциплины.

Самостоятельная работа студентов, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

Предполагается, что, прослушав лекцию, студент должен ознакомиться с рекомендованной литературой из основного списка, затем обратиться к источникам, указанным в библиографических списках изученных книг, осуществить поиск и критическую оценку материала на сайтах Интернет, собрать необходимую информацию.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
5	ПК-2	Тестирование Отчёты по практическим работам Отчёт по лабораторной работе Вопросы к зачету

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Типовые практические задания

Практическая работа 1
Задания:
Для выполнения лабораторной работы необходимо выбрать конкретное предприятие и провести анализ его деятельности.
1. Описание и анализ деятельности должны включать следующие сведения: основные направления деятельности; описание существующего документооборота предприятия; программное и аппаратное обеспечение предприятия.
2. Подготовить функциональную модель разработки КСЗИ для вашего предприятия с помощью BPWin (2-3 уровня детализации).
3. Выделить информационные активы предприятия, подлежащие защите.
4. На основе примеров, построить деревья угроз для выбранного предприятия.

Критерии оценки:
1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;
5 баллов – студент выполнил методические указания не в полном объеме, есть замечания по отчёту;
8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;
10 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

Практическая работа 2
Задания:
Исследовать существующие методы и ПО анализа информационных рисков с проведением сравнительного анализа
1. Изучить методику GRAMM.
2. Изучить методику FRAP
3. Изучить методику OCTAVE.
4. Изучить методику и ПО MSAT
5. Провести анализ рисков для предприятия с использованием одной из методик.
6. Провести анализ рисков предприятия с помощью программы Microsoft Security Assesment Tool 4.0
7. Разработать политику информационной безопасности для предприятия в виде документа

Критерии оценки:

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

8 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

10 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

15 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

Практическая работа 3

Задания:

По результатам выполнения предыдущих работ выполнить:

1. Перечислить существующие подходы к проектированию КСЗИ. Выделить их достоинства и недостатки.

2. Построить математическую модель КСЗИ предприятия.

3. Разработать структуру КСЗИ для предприятия.

Критерии оценки:

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

8 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

10 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

15 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

Практическая работа 4

Задания:

На основании разработанного ранее документа "Политика информационной безопасности для предприятия" в виде документа, выполнить:

1. Построить список нормативно-правовых актов, регулирующих информационную безопасность.

2. Разработать нормативно-правовую подсистему КСЗИ предприятия на основе анализа правовых документов и стандартов в области защиты информации.

3. Разработать организационно-методическую подсистему КСЗИ предприятия, включающую (ОСУ ИБ, документы, инструкции и др).

4. Разработать план внедрения методов и средств разработанных подсистем с указанием мероприятий, сроков и ответственных (в таблице).

Критерии оценки:

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

8 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

10 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

15 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

Практическая работа 5

Задания:

На основании разработанного ранее документа "Политика информационной безопасности для предприятия" в виде документа, выполнить:

1. Разработать 2-3 модели инженерно-технической подсистемы КСЗИ предприятия на основе анализа инженерно-технических методов и средств (выбор инженерно-технических средств проводить на основе аналитических таблиц сравнений по основным параметрам).

2. Выбрать оптимальную модель инженерно-технической подсистемы КСЗИ предприятия (при выборе необходимо учитывать стоимость и качество методов и средств защиты).

Критерии оценки:

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

8 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

10 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

15 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

Практическая работа 6

Задания:

На основании разработанного ранее документа " Политика информационной безопасности для предприятия" в виде документа, выполнить:

1. Сформулировать требования, которые необходимо учесть при разработке программно-аппаратной подсистемы КСЗИ.

2. Разработать 2-3 модели программно-аппаратной подсистемы КСЗИ предприятия на основе анализа программно-аппаратных методов и средств (выбор программно-аппаратных средств проводить на основе аналитических таблиц сравнений по основным параметрам).

3. Выбрать оптимальную модель программно-аппаратной подсистемы КСЗИ предприятия (при выборе необходимо учитывать стоимость и качество методов и средств защиты).

Критерии оценки:

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

8 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

10 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

15 баллов - студент выполнил методические указания в полном объеме, отчёт без

замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

7.2.2. Типовое задание для лабораторной работы

Лабораторная работа 1.

Задание:

Построить модель оценки эффективности КСЗИ с помощью инструментов MS Excel. С помощью аналитических и графических возможностей MS Excel провести анализ эффективности предложенного проекта КСЗИ, результаты представить в виде динамического дашборда.

Критерии оценки:

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

8 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

10 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

15 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

7.2.3. Типовые вопросы из банка тестовых заданий для тестирования

1. Под «информацией» в ФЗ «Об информации, информационных технологиях и защите информации» понимается…

1) информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
2) зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
3) сведения (сообщения, данные) независимо от формы их представления.

2. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) соблюдение конфиденциальности информации ограниченного доступа;
3) реализацию права на доступ к информации.
4) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;
5) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

3. Информационная система – это…
1) компьютерные сети;
2) системы управления работой компьютера;
3) системы хранения, обработки и передачи информации в специально организованной форме.

4.Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц – …
1) распространение информации;
2) хранение информации;
3) предоставление информации.

5 Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
1) распространение информации;
2) хранение информации;
3) предоставление информации.

6. Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду - …
1) служебная тайна;
2) коммерческая тайна;
3) государственная тайна.

7. Действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору - …
1) передача информации;
2) предоставление информации;
3) разглашение информации.

8. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:
1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2) установление ограничений доступа к информации только федеральными законами;
3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

9. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:
1) обеспечение безопасности Российской Федерации при создании информационных

систем, их эксплуатации и защите содержащейся в них информации;
2) достоверность информации и своевременность ее предоставления;
3) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
4) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.
5) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

10. Что относится к правовым мерам защиты информации
1) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения
2) Действия правоохранительных органов для защиты информационных ресурсов
3) Организационно-административные меры для защиты информационных ресурсов
4) Действия администраторов сети защиты информационных ресурсов

11. Информационные технологии – это:
1) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
2) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
3) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

12. Информационная система – это:
1) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
2) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
3) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

13. Информационно-телекоммуникационная сеть – это:
1) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
2) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
3) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

14. Доступ к информации – это:
1) возможность получения информации и ее использования;
2) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
3) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
4) действия, направленные на получение информации неопределенным кругом лиц или

передачу информации неопределенному кругу лиц;

15. Конфиденциальность информации – это:
1) возможность получения информации и ее использования;
2) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
3) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
4) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

16. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
1) электронное сообщение
2) документированная информация
3) конфиденциальная информация

17. Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
1) электронное сообщение
2) документированная информация
3) конфиденциальная информация

18. Информация в зависимости от категории доступа к ней подразделяется на
1) общедоступную информацию
2) информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).
3) секретную информацию
4) конфиденциальную информацию

19.Информация в зависимости от порядка ее предоставления или распространения подразделяется на:
1) информацию, свободно распространяемую;
2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.
5) секретную информацию
6) конфиденциальную информацию

20. Назовите виды информационных систем:
1) государственные информационные системы;
2) муниципальные информационные системы;
3) личные информационные системы.

21. Что представляет собой защита информации:
1) принятие правовых, организационных и технических мер;
2) принятие правовых и технических мер;

3) принятие правовых и организационных мер.

22. На что направлено принятие правовых, организационных, технических и экономических мер защиты информации:
1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) на соблюдение конфиденциальности информации ограниченного доступа;
3) на реализацию права на доступ к информации.

23. Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности
1) Гражданско-правовая
2) Дисциплинарная
3) Материальная
4) Условная

24. Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности
1) Уголовная
2) Административно-правовая
3) Материальная
4) Договорная

25. Что такое государственная тайна
1) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
2) Сведения о состоянии окружающей среды
3) Все сведения, которые хранятся в государственных базах данных
4) Сведения о состоянии здоровья президента РФ
5) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне

26.Что такое коммерческая тайна
1) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам
2) Информация, к которой нет доступа на законном основании
3) Информации, обладатель которой принимает меры к охране ее конфиденциальности
4) Информация, содержащая в учредительных документах
5) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов

27. Кем устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение
1) уполномоченными органами на основании Закона о государственной тайне;
2) собственником информационных ресурсов или уполномоченным лицом на основании Закона об информации;
3) федеральным законом.

28. Кем устанавливается порядок доступа к персональным данным граждан (физических

лиц)
1) уполномоченными органами на основании Закона о государственной тайне;
2) собственником информационных ресурсов или уполномоченным лицом на основании Закона об информации;
3) федеральным законом.

29. Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него - …
1) гриф секретности;
2) резолюция секретности;
3) виза секретности.

30. Грифы секретности для носителей сведений, составляющих государственную тайну:
1) “особой важности”, “совершенной важности” и “секретно”;
2) “совершенно важно”, “совершенно секретно” и “секретно”;
3) “особой важности”, “совершенно секретно” и “секретно”.

31. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
1) оператор информационной системы
2) обладатель информации
3) владелец информации

32. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
1) оператор информационной системы
2) обладатель информации
3) владелец информации

33.Как Федеральный закон Российской Федерации от 27 июля 2006 г. №149 подразделяет информацию в зависимости от категории доступа к ней:
1) на общедоступную информацию;
2) на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа);
3) на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

34. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии:
1) с федеральными законами и (или) по решению суда;
2) с федеральными законами;
3) по решению суда.

35. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Секретно»:
1) первая;
2) вторая;
3) третья.

36. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Сов. Секретно»:
1) первая;
2) вторая;
3) третья.

37. Какова должна быть категория объектов информатизации, на
которых обрабатывается информация с грифом «Особой важности»:
1) первая;
2) вторая;
3) третья.

38. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации
1) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных»;
3) Доктрина информационной безопасности Российской Федерации

39. Назовите Федеральный закон, который регулирует отношения, возникающие при обеспечении защиты информации:
1) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
3) Доктрина информационной безопасности Российской Федерации.

40. Какие правовые документы решают вопросы информационной безопасности
1) Уголовный кодекс РФ
2) Конституция РФ
3) Закон "Об информации, информационных технологиях и защите информации"
4) Закон РФ "Об образовании"
5) Закон РФ " Об электронной подписи "

Критерии оценки:

Баллы выставляются пропорционально правильным ответам на тестовые вопросы автоматически. Максимум – 100 баллов.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр **5**

№ п/п	Вопросы к зачету
1	Понятие комплексной системы защиты информации на предприятии.
2	Сущность и задачи комплексной системы защиты информации (КСЗИ) на предприятии.
3	Принципы организации комплексной защиты информации на предприятии.
4	Требования к комплексной системе защиты информации на предприятии.

№ п/п	Вопросы к зачету
5	Этапы разработки комплексной системы защиты информации на предприятии.
6	Факторы, влияющие на организацию КСЗИ.
7	Определение и нормативное закрепление состава защищаемой информации.
8	Информационные активы предприятия, подлежащие защите.
9	Общие подходы к анализу и оценке угроз безопасности информации.
10	Внутренние и внешние угрозы информации.
11	Риски в сфере информационной безопасности.
12	Управление рисками. Модель перекрытия.
13	Анализ рисков информационной безопасности.
14	Использование современных методик анализа информационных рисков на предприятии.
15	Методика анализа рисков CRAMM.
16	Методика анализа рисков FRAP.
17	Методика анализа рисков OCTAVE.
18	Методика анализа рисков RiskWatch.
19	Методика оценки рисков Microsoft.
20	Программные инструменты анализа информационных рисков.
21	Использование программного инструмента MSAT для анализа информационных рисков предприятия.
22	Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
23	Определение потенциальных каналов и методов несанкционированного доступа к информации.
24	Определение возможностей несанкционированного доступа к защищаемой информации.
25	Методы и средства защиты информации, используемые в КСЗИ.
26	Подходы к построению КСЗИ на предприятии.
27	Математический подход к проектированию КСЗИ.
28	Системный подход к построению КСЗИ.
29	Определение компонентов КСЗИ.
30	Организационно-методическая подсистема КСЗИ на предприятии.
31	Программно-аппаратная подсистема КСЗИ на предприятии.
32	Инженерно-техническая подсистема КСЗИ на предприятии.
33	Разработка политики безопасности и регламента безопасности предприятия.
34	Система управления информационной безопасностью предприятия.
35	Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.
36	Классификация информации по видам тайны и степеням конфиденциальности.
37	Использование международных и российских стандартов безопасности при разработке КСЗИ предприятия.
38	Характеристика основных международных стандартов информационной безопасности.
39	Характеристика основных российских стандартов информационной безопасности.
40	Классификация средств защиты информации от НСД.
41	Кадровое обеспечение функционирования КСЗИ.
42	Принципы и методы планирования функционирования КСЗИ.
43	Принципы управления КСЗИ.
44	Сущность и содержание контроля функционирования КСЗИ.

№ п/п	Вопросы к зачету
45	Оценка эффективности КСЗИ.

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
5	Зачет (по накопительному рейтингу)	«зачтено»	Студент набрал 40 и более баллов по накопительному рейтингу
		«не зачтено»	Студент набрал менее 40 баллов по накопительному рейтингу

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1.	Васильков А.В., Васильков И.А.	Безопасность и управление доступом в информационных системах	Учебное пособие	2019	ЭБС "ZNANIUM.COM"
2.	Под общ. ред. С.А. Коноваленко	Экономическая безопасность	учебник	2021	ЭБС "ZNANIUM.COM"
3.	Партыка Т.Л., Попов И.И.	Информационная безопасность	учебное пособие	2019	ЭБС "ZNANIUM.COM"

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Коллектив авторов: Бобошко Н.М. и др	Актуальные проблемы обеспечения экономической безопасности	Сборник научных трудов	2016	ЭБС "ZNANIUM.COM"
2	Губин Б.В., Иванов Е.А. и др.	Бюджет России: развитие и обеспечение экономической безопасности	Монография	2019	ЭБС "ZNANIUM.COM"
3	Беловицкий К.Б., Николаев В.Г.	Методы, модели, средства хранения и обработки данных	учебник	2017	ЭБС "ZNANIUM.COM"

8.3. Перечень профессиональных баз данных и информационных справочных систем

– КонсультантПлюс — Режим доступа к журн.: http://www.consultant.ru/

– Гарант.РУ [Электронный ресурс] : информационно-правовой портал — Режим доступа к журн.: http://www.garant.ru/

– Scopus [Электронный ресурс] : реферативная база данных. – Netherlands: Elsevier, 2021. – Режим доступа : scopus.com. – Загл. с экрана. – Яз. рус., англ.

– Elibrary [Электронный ресурс] : научная электронная библиотека. – Москва : НЭБ, 2021. – Режим доступа : elibrary.ru. – Загл. с экрана. – Яз. рус., англ.

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Договор № 690 от 19.05.2015г., срок действия - бессрочно
2	Office Standart	Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (С-709)	Столы ученические двухместные (моноблок), стол ученический двухместный, стол преподавательский, стул преподавательский , доска аудиторная (маркерная), доска аудиторная (меловая), трибуна , проектор, экран; компьютер .
3	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий	Столы ученические двухместные, Столы преподавательские, стулья, доска аудиторная (маркерная), доска аудиторная (меловая), экран, кресло., шкафы, стенды, электрощит, огнетушитель, ПК, принтер, компьютер, монитор, проектор, беспроводной маршрутизатор , принтер.

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	текущего контроля и промежуточной аттестации (С-802)	
4	Помещение для самостоятельной работы студентов (Г-401)	Столы ученические, стулья ученические, ПК с выходом в сеть Интернет