Автономная некоммерческая организация высшего образования
«Институт социальных наук»

УТВЕРЖДАЮ

Ректор Бианкина А.О.

« 01 » июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

для студентов направления подготовки

38.03.05 Бизнес-информатика

Профиль

«Бизнес-аналитика»

Квалификация (степень) выпускника – бакалавр

Форма обучения: очная

Москва

Рабочая программа дисциплины «Информационная безопасность»

Направление подготовки 38.03.05 Бизнес –информатика

Составитель

Программа рассмотрена и согласована на заседании кафедры экономики и управления (протокол № от « » _____20 г.)

Заведующий кафедрой _____

(подпись)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

2. Объем и место дисциплины в структуре образовательной программы

3. Содержание и структура дисциплины

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации

4.2. Материалы текущего контроля успеваемости обучающихся

4.3. Оценочные средства для промежуточной аттестации

4.4. Методические материалы

5. Методические указания для обучающихся по освоению дисциплины

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

6.2. Дополнительная литература

6.3. Учебно-методическое обеспечение самостоятельной работы

6.4. Нормативные правовые документы

6.5. Интернет-ресурсы

6.6. Иные источники

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Таблица 1.1

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1.2	Способность использовать системный подход при анализе предметной области
УК ОС-1	Способность применять критический анализ информации и системный подход для решения задач обоснования собственной гражданской и мировоззренческой позиции	УК ОС-1.2	Способность рассматривать систему как элемент системы более высокого уровня (видеть систему как совокупность подсистем).

В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 1.2

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код этапа освоения компетенции	Результаты обучения
Выполнение трудовой функции «Управление информационной безопасностью ресурсов ИТ» в соответствии с обобщенной трудовой функцией профессионального стандарта «Менеджер информационных технологий» - управление ресурсами ИТ.	ОПК-1.2	на уровне знаний: – способов представления и преобразования различных видов информации в компьютере; форм представления данных, методы обеспечения надёжности при передаче и хранении, оценки объемов информации различных видов; – возможностей базовых ИКТ и ИС на уровне умений: – представлять числовую информацию в различных системах счисления и выполнять все виды арифметических и логических действий в этих системах; – работать с различными видами информации в текстовом и табличном процессорах, использовать текстовый и табличный процессор при решении классических задач профессиональной деятельности; – подготавливать презентации, вести деловые беседы, доклады на их основе; – вести делопроизводство в том числе на основе использования систем электронного документооборота; – решать простейших задачи профессиональной деятельности с использованием методов системного анализа и принципов системного подхода.
	УК ОС-1,2	на уровне знаний: - система, свойства систем, классификация систем, - системный подход, принципы системного подхода - гражданская позиция, мировоззренческая позиция на уровне умений:

		- критериально оценивать информацию; - выявлять обратные связи в системах, - выявлять эмерджентные свойства систем; - учитывать фактор времени при анализе явлений

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц /180 академ. часов.

Дисциплина реализуется с применением дистанционных образовательных технологий (*далее - ДОТ*).

Таблица 2

Вид работы	Трудоемкость (акад/астр.часы)
Общая трудоемкость	180/135
Контактная работа с преподавателем	62/46,5
Лекции	24/18
Практические занятия	38/28,5
Лабораторные занятия	
Самостоятельная работа	91/68,25
Контроль	27/20,25
Форма текущего контроля	Курсовая работа
Форма промежуточной аттестации	Экзамен

Место дисциплины в структуре ОП ВО

Дисциплина Б1.Б.16 «Информационная безопасность» относится к базовой части учебного плана по направлению «Бизнес-информатика» 38.03.05. Преподавание дисциплины «Информационная безопасность» основано на дисциплинах – Б1.Б.07.03 «Теория вероятностей и математическая статистика», Б1.Б.08 «Теория систем и системный анализ», Б1.В.11 «Анализ данных», В свою очередь она создаёт необходимые предпосылки для освоения программ таких дисциплин, как Б1.Б.19. «Моделирование бизнес-процессов», Б1.В.10 «Архитектура предприятия», Б1.В.08 «Управление жизненным циклом ИС» и ряда дисциплин по выбору студента.

Дисциплина изучается в 6-м семестре 3-го курса.

Формой промежуточной аттестации в соответствии с учебным планом является экзамен.

3. Содержание и структура дисциплины

Таблица 3

№ п/п	Наименование тем	Объем дисциплины час.						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Нормативная база и стандарты в области информационной безопасности и защиты информации	52	6				46	Т
Тема 2	Угрозы безопасности информации	30	8		6		16	З/Т
Тема 3	Методы и средства	50	6		32		12	КС/Т

	защиты информации от несанкционированного доступа							
Тема 4.	Компьютерная преступность	21	4				17	Д,Т
Контроль		27						
Текущий контроль								КР
Промежуточная аттестация						2*		Экзамен
Всего:		180/135	24/18		38/28,4		91/68,25	

2* - консультация, не входящая в общий объем дисциплины

Т- тестирование

З – задание

КС – круглый стол

КР – курсовая работа

Содержание дисциплины

Тема 1. Нормативная база и стандарты в области информационной безопасности и защиты информации

Нормативная база информационной безопасности и защиты информации. Государственная политика в сфере информационной безопасности и защиты информации. Правовое обеспечение информационной безопасности. Конституция РФ об «информационных правах и обязанностях». Основные нормативные документы, регулирующие отношения в сфере информационной безопасности.

Виды «тайн» по Российскому законодательству. Классификация тайн.

Обобщенная модель информационной безопасности. Национальные стандарты в области информационной безопасности и защиты информации. Международные стандарты в области информационной безопасности и защиты информации. Проблемы гармонизации стандартов информационной безопасности.

Тема 2. Угрозы безопасности информации

Каналы силового деструктивного воздействия на информацию. Электромагнитный спектр как источник воздействия на информацию. Каналы силового деструктивного воздействия (СДВ) на информацию. Классификация средств СДВ. Рекомендации по защите компьютерных систем от СДВ.

Технические каналы утечки информации. Классификация технических каналов утечки информации. Модели и способы утечки информации по техническим каналам.

Угрозы несанкционированного доступа к информации. Классификация угроз несанкционированного доступа (НСД) к информации. Категории нарушителей безопасности информации и их возможности. Общая характеристика уязвимостей. Способы реализации угрозы НСД к информации.

Нетрадиционные информационные каналы. Понятие и обобщенная модель нетрадиционного информационного канала. Методы сокрытия информации в текстовых файлах. Методы сокрытия информации в графических файлах. Методы сокрытия информации в звуковых файлах. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.

Тема 3. Методы и средства защиты информации от несанкционированного доступа

Криптографическая защита информации. Модель криптосистемы. Историография и классификация шифров. Примеры криптографических алгоритмов. Криптосистема с симметричными и несимметричными ключами. Электронная цифровая подпись.

Методы и средства разграничения и контроля доступа к информации. Мандатная и дискреционная модели доступа. Процедура идентификации, аутентификации и авторизации. Система паролирования. Системы контроля и управления доступом. Система охраны периметра.

Системы предотвращения утечки информации из корпоративной сети. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети. Понятие и функционал DLP-систем. Объем и структура данных защищаемых DLP-системами. Каналы коммуникаций, контролируемые DLP-системами. Критерии оценки программных продуктов, реализующих функциональность DLP.

Тема 4. Компьютерная преступность

Понятие компьютерной преступности. Масштабы и общественная опасность компьютерной преступности. Виды и субъекты компьютерных преступлений. Специфика расследования компьютерных преступлений. Предупреждение компьютерных преступлений. Кодификатор Интерпола.

Ответственность за нарушения и преступления в сфере информационной безопасности. Дисциплинарная ответственность за разглашение охраняемой законом тайны. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации. Уголовная ответственность за преступления в сфере компьютерной информации. Уголовная ответственность за нарушение закона о государственной тайне.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

Промежуточная аттестация может проводиться с использованием ДОТ.

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 4.1

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Нормативная база и стандарты в области информационной безопасности и защиты информации	Устный опрос, деловая игра «Проблемы и приоритеты в сфере информационной безопасности»
Тема 2. Угрозы безопасности информации	Защита задания
Тема 3. Методы и средства защиты информации от несанкционированного доступа	Круглый стол/Тестирование
Тема 4. Компьютерная преступность	Диспут, тестирование

4.1.2. Экзамен проводится с применением следующих методов (средств) :

Экзамен проводится в компьютерном классе. Во время экзамена проверяются этапы освоения компетенций ОПК - 1.2, УК ОС - 1.2.

Во время проверки сформированности этапа компетенции ОПК - 1.2 оцениваются:

- выполнение и защита курсовой работы;
- выполнение работ с информационной системой обеспечения информационной безопасности.
- тестирование.

Во время проверки сформированности этапа УК ОС 1.2 оцениваются:

- презентация модели и полученных результатов в виде отчета или в офисных приложениях.

4. 2. Материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по темам дисциплины

Типовые тесты

1. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему (последовательность номеров через запятую):

1) морально-этический;

2) организационно-технический;
3) нормативно-правовой;
4) программно-аппаратный;
5) духовно-нравственный.

2. Что НЕ является элементом системы обеспечения информационной безопасности РФ (номер по порядку):
1) Палаты Федерального собрания;
2) Президент;
3) Органы местного самоуправления;
4) Общественная Палата;
5) Органы исполнительной власти;
6) Совет безопасности?

3. Кто НЕ наделен полномочиями по отнесению сведений к государственной тайне:
1) Министр сельского хозяйства;
2) Председатель Банка РФ;
3) Руководитель Росгидромета;
4) Руководитель Федеральной таможенной службы?

4. Служба безопасности на предприятии призвана:
1) постепенно заменить государственные правоохранительные органы и специальные службы;
2) помочь олигархическим группам в борьбе за власть;
3) обеспечить безопасность в тех областях, которые находятся вне компетенции правоохранительных органов;
4) осуществлять все, что указано в предыдущих пунктах?

5. Коммерческая тайна – это:
1) общее понятие для тайн профессиональной, личной, семейной;
2) то же самое, что и интеллектуальная собственность;
3) то же самое, что и профессиональная тайна;
4) то же самое, что и банковская тайна;
5) частный случай государственной тайны;
6) частный случай конфиденциальной информации.

6. Основанием для видов коммерческой тайны является:
1) сфера деятельности предприятия;
2) способ организации защиты тайны;
3) отраслевая принадлежность предприятия;
4) все указанное в 1)–3);
5) все указанное в 1)–2).

7. Режим коммерческой тайны не может быть установлен в отношении сведений:
1) о задолженности по выплате зарплаты;
2) о размерах доходов некоммерческих организаций;
3) о составе имущества предприятия любой формы собственности;
4) о системе оплаты труда (неверное зачеркнуть).

8. При отсутствии трудовых договоров охрана КТ должна включать в себя:
1) определение перечня сведений;
2) ограничение доступа;
3) учет лиц, получивших доступ;
4) регулирование отношений с контрагентами;
5) нанесение грифа «Коммерческая тайна» (неверное зачеркнуть).

9. Не подлежит засекречиванию информация о:
1) состоянии окружающей среды;
2) состоянии здоровья премьер-министра;
3) размерах золотовалютного резерва;

4) состоянии борьбы с преступностью;
5) привилегиях.

10. Какой степени секретности НЕ существует:
1) государственной важности;
2) совершенно секретно;
3) особой важности;
4) секретно?

11. Основанием для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:
1) признание его рецидивистом;
2) постоянное проживание близких родственников за границей;
3) сообщение заведомо ложных анкетных данных;
4) наличие медицинских противопоказаний;
5) наличие загранпаспорта (неверное зачеркнуть).

12. К органам защиты государственной тайны относятся:
1) Федеральная служба безопасности;
2) Служба внешней разведки;
3) Министерство внутренних дел;
4) Федеральная служба по техническому и экспортному контролю;
5) Министерство обороны (неверное зачеркнуть).

13. Включение кейса с электролитическими конденсаторами в сетевую розетку офисной ЛВС является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

14. Включение кейса с электролитическими конденсаторами в офисную розетку сети электропитания является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

15. Включение электрошокера в сетевой разъем маршрутизатора является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

16. Мощный разряд молнии в непосредственной близости является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

17. Внедрение программной закладки в источник бесперебойного питания. является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

18. Перехват побочных электромагнитных излучений от работы ПЭВМ и ВТСС является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;

4) радиоканал;
5) параметрический.

19. Съём наводок информационных сигналов с посторонних проводников является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

20. Беспроводной прием информации, передаваемой аппаратными закладками является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

21. Приём переизлученных высокочастотных колебаний, модулированных информационным сигналом является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

22. Перехват речевых сигналов направленными микрофонами является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

23. По виду защищаемой информации различаются угрозы НСД к:
1) речевой информации;
2) видовой информации;
3) сигнальной информации;
4) логической информации;
5) тестовой информации (лишнее зачеркнуть).

24. По видам возможных источников различаются угрозы НСД к информации, создаваемые:
1) нарушителем;
2) аппаратной закладкой;
3) вредоносными программами;
4) сетевыми атаками (лишнее зачеркнуть).

25. По виду нарушаемого свойства информации различаются угрозы:
1) конфиденциальности;
2) целостности;
3) доступности;
4) идентифицируемости (лишнее зачеркнуть).

26. По способам реализации различаются угрозы с применением:

1) программных средств операционной системы;
2) специально разработанного программного обеспечения;
3) вредоносных программ;
4) пользовательских программ (лишнее зачеркнуть).

27. По используемой уязвимости различаются угрозы:
1) системного программного обеспечения;
2) прикладного программного обеспечения;
3) вызванные аппаратной закладкой; 4) протоколов сетевого взаимодействия;
5) недостатков организации технической защиты информации от НСД;
6) вызванные наличием технических каналов утечки информации;
7) недостатков системы защиты информации:
8) специальных воздействий (лишнее зачеркнуть)

28. По объекту воздействия различаются угрозы:
1) информации, обрабатываемой на АРМ;
2) информации, обрабатываемой в выделенных технических средствах обработки информации;
3) информации, передаваемой по сетям;
4) прикладным программам обработки информации;
5) системному программному обеспечению;
6) пользовательским программам (лишнее зачеркнуть)

29. Сколько текстовой информации может быть скрыто методами стеганографии в цветной фотографии, сделанной 3-х мегапиксельной камерой мобильного телефона:
1) 108 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);
2) 71 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);
3) 23 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5)?

30. Сколько текстовой информации может быть скрыто методами стеганографии в цветной фотографии формата *bmp*, сделанной мегапиксельной камерой мобильного телефона?
1) 108 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);
2) 71 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);
3) 23 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5)?

Типовые вопросы для круглого стола

1. По каким схемам можно включить контур информационной безопасности в сеть предприятия?
2. Зачем нужна фильтрация по прокси-серверам?
3. Зачем нужна фильтрация по почтовым серверам?
4. Какие виды поиска рекомендуются для структурированных документов?
5. Что такое фильтр ограничений по перехвату?
6. Что такое «белый список»?
7. Какой должен быть интервал обновления индексов?
8. Для чего применяется каталог образцов?
9. Можно ли снять цифровой отпечаток из pdf-файла?
10. Что такое шаблон регулярного выражения?

Ключи к тестам

Тест	1	2	3	4	5	6	7	8	9	10
Ключ	3).2).4),1),5)	4)	3)	3)	6)	5)	3)	1), 2)	4)	1)
Тест	11	12	13	14	15	16	17	18	19	20
Ключ	5)	3)	1)	2)	1)	3)	2)	1)	3)	4)

Тест	21	22	23	24	25	26	27	28	29	30
Ключ	5)	2)	5)	4)	4)	4)	8)	6)	2)	3)

4.3. Оценочные средства для промежуточной аттестации.

Таблица 4.2

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1.2	Способность использовать системный подход при анализе предметной области
УК ОС-1	Способность применять критический анализ информации и системный подход для решения задач обоснования собственной гражданской и мировоззренческой позиции	УК ОС-1.2	Способность рассматривать систему как элемент системы более высокого уровня (видеть систему как совокупность подсистем).

Таблица 4.3

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ОПК - 1.2	Демонстрирует знания основных положений теории информационной безопасности, методов и моделей обеспечения информационной безопасности, в том числе при взаимодействии с партнерами и клиентами. Демонстрирует умение проектировать средства обеспечения информационной безопасности, методы и модели оценки угроз и рисков. Демонстрирует умение решать частные задачи организации взаимодействия с клиентами и партнерами, управлять информационной безопасностью.	Правильность и полнота решения задач по кодированию и декодированию, оценке информационной безопасности. Полнота реализации темы курсовой работы. Умение использовать частные инструменты по управлению информационной безопасностью.
УК ОС - 1.2	Показывает знания возможностей ИКТ-технологий, компьютерных	Продемонстрированы знания возможностей ИТ-систем и технологий.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
	систем, систем математического моделирования, которые могут быть использованы для описания и моделирования процессов Демонстрирует умение использовать возможности современных языков описания и моделирования процессов. Показывает результаты решения частных задач моделирования с использованием ИТ	Показаны результаты решения частных задач моделирования с использованием ИТ в соответствии с полученным заданием Корректно использованы правила построения моделей. Сделаны правильные ответы на поставленные вопросы или тесты

Для оценки сформированности компетенций, знаний и умений, соответствующих данным компетенциям, используются вопросы, темы курсовых работ, при выполнении которых необходимо построить модели угроз, модели нарушителя, модели обеспечения и управления информационной безопасностью организации.

Примерная тематика курсовых работ:

1. Защита персональных данных в облачных хранилищах данных.
2. Угрозы безопасности персональным данным при их обработке в информационных системах персональных данных.
3. Риски и вызовы криптовалют для монетарной политики.
4. Правовые аспекты организации обработки персональных данных.
5. Алгоритм шифрования ГОСТ 28147-89.
6. ГОСТ Р 34.10-2012. Процессы формирования и проверки электронной подписи.
7. Защита конфиденциальной информации при работе с лингвистическим анализом DLP- систем.
8. Контроль записи конфиденциальных данных на внешние носители в DLP-системе.
9. Комплексное программное решение для защиты от утечки конфиденциальных данных.
10. Использование цифровых меток для защиты конфиденциальных данных.
11. Использование функции DLP-систем «поиск по атрибутам» при работе с информацией, содержащей конфиденциальные данные.
12. Контроль персональных данных в исходящей электронной почте.
13. Выявление утечки персональных данных с использованием функции DLP-системы «поиск похожих».
14. Использование функции DLP-систем «поиск по словарю» для защиты персональных данных.
15. Контроль информации, содержащей конфиденциальные данные и выводимой на печать.
16. Сложности внедрения DLP-систем для защиты персональных данных.
17. Предотвращение утечки конфиденциальных данных в почтовом трафике на примере программного комплекса SearchInform.

18. Исследование функции фразового поиска DLP-систем при работе с персональными данными.

19. Предотвращение утечек персональных данных путем перехвата содержимого мониторов рабочих станций пользователей.

20. Построение модели комплексной защиты информации на предприятии.

21. Применение запросов с цифровыми отпечатками в DLP-системах при работе с конфиденциальными данными.

22. Оценка необходимости использования «Белых списков» в DLP системах при защите персональных данных.

23. Исследование средств статического анализа уязвимостей.

24. Исследование средств анализа защищенности: сетевые сканеры безопасности.

25. Исследование средств для сбора информации об атакуемой сети.

26. Система защиты государственной тайны в РФ.

27. Порядок допуска сотрудников к государственной тайне.

28. Правовые основы защиты профессиональной тайны в РФ.

29. Каналы утечки электронной конфиденциальной информации.

30. Основные методы защиты электронной конфиденциальной информации.

Типовые вопросы, выносимые на экзамен для оценки знаний, умений и навыков и опыта деятельности, характеризующие этапы формирования компетенций в процессе формирования освоения образовательной программы

1) Государственная политика в сфере информационной безопасности и защиты информации.

2) Правовое обеспечение информационной безопасности.

3) Конституция РФ об «информационных правах и обязанностях».

4) Основные нормативные документы, регулирующие отношения в сфере информационной безопасности.

5) Акты регуляторов в сфере защиты информации.

6) Институт «тайны» в Российском законодательстве.

7) Классификация тайн.

8) Правовые основания отнесения сведений к категории ограниченного доступа.

9) Краткая история защиты информации в России.

10) Обобщенная модель информационной безопасности.

11) Институт стандартизации сферы информационной безопасности.

12) Национальные стандарты в области информационной безопасности и защиты информации.

13) Международные стандарты в области информационной безопасности и защиты информации.

14) Проблемы гармонизации стандартов информационной безопасности.

15) «Ландшафт» стандартов информационной безопасности.

16) Электромагнитный спектр как источник воздействия на информацию.

17) Каналы силового деструктивного воздействия (СДВ) на информацию.

18) Классификация средств СДВ.

19) Рекомендации по защите компьютерных систем от СДВ.

20) Классификация технических каналов утечки информации.

21) Модель и способы утечки по радиоканалу.

22) Модель и способы утечки по электрическому каналу.

23) Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу.

24) Модель и способы утечки по параметрическому (смешанному) каналу.

25) Модель и способы утечки по оптическому (оптико-электронному) каналу.

26) Модель и способы утечки по каналу ПЭМИН.

27) Классификация угроз несанкционированного доступа (НСД) к информации.

28) Категории нарушителей безопасности информации и их возможности.
29) Общая характеристика уязвимостей.
30) Способы реализации угрозы НСД к информации.
31) Понятие и обобщенная модель нетрадиционного информационного канала.
32) Методы сокрытия информации в текстовых файлах.
33) Методы сокрытия информации в графических файлах.
34) Методы сокрытия информации в звуковых файлах.
35) Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
36) Модель криптосистемы.
37) Историография и классификация шифров.
38) Примеры криптографических алгоритмов.
39) Криптосистема с симметричными и несимметричными ключами.
40) Электронная цифровая подпись.
41) Мандатная и дискреционная модели доступа.
42) Процедура идентификации, аутентификации и авторизации.
43) Система паролирования.
44) Системы контроля и управления доступом.
45) Система охраны периметра.
46) Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
47) Понятие и функционал DLP-систем.
48) Объем и структура данных защищаемых DLP-системами.
49) Каналы коммуникаций, контролируемые DLP-системами.
50) Критерии оценки программных продуктов, реализующих функциональность DLP.
51) Понятие компьютерной преступности.
52) Масштабы и общественная опасность компьютерной преступности.
53) Виды и субъекты компьютерных преступлений.
54) Специфика расследования компьютерных преступлений.
55) Предупреждение компьютерных преступлений.
56) Кодификатор Интерпола.
57) Дисциплинарная ответственность за разглашение охраняемой законом тайны.
58) Административная ответственность за нарушения в сфере информационной безопасности и защиты информации.
59) Уголовная ответственность за преступления в сфере компьютерной информации.
60) Уголовная ответственность за нарушение закона о государственной тайне.

Шкала оценивания.

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Использование БРС осуществляется в соответствии с приказом от 28 августа 2014 г. №168 «О применении балльно-рейтинговой системы оценки знаний студентов». БРС по дисциплине отражена в схеме расчетов рейтинговых баллов (далее – схема расчетов). Схема расчетов сформирована в соответствии с учебным планом направления, согласована с руководителем научно-образовательного направления, утверждена деканом факультета. Схема расчетов доводится до сведения студентов на первом занятии по данной дисциплине и является составной частью рабочей программы дисциплины и содержит информацию по изучению дисциплины, указанную в Положении о балльно-рейтинговой системе оценки знаний обучающихся в АНОВО «Институт социальных наук»

На основании п. 14 Положения о балльно-рейтинговой системе оценки знаний обучающихся в АНОВО «Институт социальных наук» принята следующая шкала перевода оценки из многобалльной системы в пятибалльную:

Таблица 4.3

Количество баллов	Оценка	
	прописью	буквой
96-100	отлично	A
86-95	отлично	B
71-85	хорошо	C
61-70	хорошо	D
51-60	удовлетворительно	E

Шкала перевода оценки из многобалльной в систему «зачтено»/ «не зачтено»:

Таблица 4.4

от 0 до 50 баллов	«не зачтено»
от 51 до 100 баллов	«зачтено»

Примечание: если дисциплина изучается в течение нескольких семестров, схема расчета приводится для каждого из них.

Баллы выставляются за посещаемость (максимум 12 баллов), результативность практических занятий (максимум 20), результат устного опроса (максимум 3 балла), результаты выполнения тестовых заданий (максимум 10 баллов), выполнение курсовой работы (максимум 25 баллов), ответ на экзамене (максимум 30 баллов). Дисциплина считается освоенной, если экзаменуемый набрал не менее 51 балла в результате выполнения всех типов заданий, включая ответ на экзамене. Минимальное количество баллов для допуска к экзамену – 45.

4.4. Методические материалы

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, включают в себя:

- комплект тестовых заданий по темам дисциплины,
- рекомендации и требования к выполнению и оформлению курсовых работ,
- критерии оценивания курсовых работ,
- требования к защите курсовых работ и критерии их оценивания,
- основания для получения максимального количества баллов по защите курсовой работы,
- основания для снижения количества баллов в диапазоне от max до min по защите курсовой работы,
- указания причин для доработки курсовой работы и допуска к экзамену по дисциплине. Методические материалы в виде презентаций размещены в Ресурсах сети СЗИУ в STUDBOX в папке кафедры ЭиФ.

5. Методические указания для обучающихся по освоению дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия, курсовые работы. Преподавание дисциплины ведется с применением следующих видов образовательных технологий, обусловливающих самоорганизацию процесса освоения дисциплины.

Организация работы с информацией.

Информационные технологии: обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки и объективного

контроля и мониторинга знаний студентов.

Использование электронных образовательных ресурсов (презентационный материал, размещенный в Ресурсах сети АНОВО «ИСН») при подготовке к лекциям, практическим занятиям. Организация работы студентов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

Проблемное обучение (проблемные лекции, лекции с элементами дискуссии) с целью развитие критического мышления, стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы. Для этого студенту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет.

Развитие профессиональной компетентности:

Case-study на практических занятиях с целью формирования способности к анализу реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.

Контекстное обучение (лекции с элементами дискуссии, практические занятия) с целью развития мотивации бакалавров к усвоению знаний путем выявления связей между конкретным знанием и его применением.

Организация группового взаимодействия в образовательном процессе.

Деловая игра: на практических занятиях ролевая имитация студентами реальной профессиональной деятельности с выполнением функций специалистов на различных рабочих местах, организация дискуссии, обучения на основе социального взаимодействия.

Работа в команде с целью развития способности к взаимодействию студентов в группе при выполнении домашних заданий по разделам дисциплины.

Осуществление учения с учетом возрастающей роли субъектности и самостоятельности:

Обучение на основе опыта: активизация познавательной деятельности студентов за счет ассоциации и собственного опыта с предметом изучения, самоуправляемого обучения, самообразовательной деятельности

С целью контроля сформированности компетенций разработан фонд контрольных заданий. Его использование позволяет реализовать балльно-рейтинговую оценку, определенную приказом от 28 августа 2014 г. №168 «О применении балльно-рейтинговой системы оценки знаний студентов».

Контрольные вопросы для подготовки к занятиям

Таблица 5

№ п/п	Наименование темы или раздела дисциплины	Контрольные вопросы для самопроверки
1	Тема 1. Нормативная база и стандарты в области информационной безопасности и защиты информации	Раскройте содержание основных принципов Доктрины ИБ РФ. Перечислите основные направления обеспечения ИБ в мировой практике. Сформулируйте основные задачи обеспечения ИБ РФ. Приведите основные функции государственной системы обеспечения ИБ РФ. Сформулируйте задачи обеспечения безопасности функционирования информации в КС? Каковы основные отечественные и зарубежные стандарты в области ИБ? Какова структура и основные положения нормативной

		базы РФ?
2	Тема 2. Угрозы безопасности информации	Проведите сравнительный анализ понятий «угрозы информационной безопасности» и «угрозы безопасности информации». Составьте классификацию угроз информационной безопасности. Назовите каналы утечки информации. Каковы основные каналы несанкционированного доступа к информации? На основании чего строится модель нарушителя информационной безопасности?
3	Тема 3. Методы и средства защиты информации от несанкционированного доступа	Сформулируйте основные проблемы ИБ. Приведите классификацию методов предотвращения угроз несанкционированного доступа в КС. Какие базовые методы защиты информации от несанкционированного доступа актуальны сегодня? Назовите средства защиты информации от несанкционированного доступа.
4	Тема 4. Компьютерная преступность	1. Постройте дерево понятия «компьютерная преступность». 2. Какими могут быть масштабы и общественная опасность компьютерной преступности? 3. Охарактеризуйте ответственность за нарушения и преступления в сфере информационной безопасности.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

Артемов, А.В. Информационная безопасность / А.В. Артемов – Орел: МАБИВ, 2014. – 256 с. [Электронный ресурс]. – Режим доступа: http://idp.nwipa.ru:2945/33430.html

Басалова, Г.В. Основы криптографии / Г.В. Басалова – М.: ИНТУИТ, 2016. – 282 с. [Электронный ресурс]. – Режим доступа: http://idp.nwipa.ru:2945/52158.html?replacement=1

Петров, С.В. Информационная безопасность / С.В. Петров, П.А. Кисляков – Саратов: Ай Пи Ар Букс, 2015. – 326 с. [Электронный ресурс]. – Режим доступа: http://idp.nwipa.ru:2945/33857.html

Скляров, Д.В. Искусство защиты и взлома информации / Д.В. Скляров – М.:БХВ-Петербург, 2014. – 276 с. [Электронный ресурс]. – Режим доступа: http://idp.nwipa.ru:2228/reading.php?productid=335110

Электронно-библиотечная система. Издательство «Лань» [Электронный ресурс] Курило А.П., Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Издательство "Горячая линия-Телеком", 2012 г. - 244 с., Режим доступа: http://nwapa.spb.ru

Все источники основной литературы взаимозаменяемы.

6.2 Дополнительная литература

Галатенко, В.А. Основы информационной безопасности / В.А. Галатенко – М.: ИНТУИТ, 2016. – 266 с. [Электронный ресурс]. Режим доступа: http://idp.nwipa.ru:2945/52209.html?replacement=1

Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А Скрипник – М.: ИНТУИТ, 2016. – 429 с. [Электронный ресурс]. – Режим доступа: http://idp.nwipa.ru:2945/52161.html?replacement=1

Фаронов, А.Е. Основы информационной безопасности при работе на компьютере / А.Е Фаронов – М.: ИНТУИТ, 2016. – 154 с. [Электронный ресурс]. – Режим доступа: http://idp.nwipa.ru:2945/52160.html?replacement=1

Электронно-библиотечная система. Издательство «Лань» [Электронный ресурс] Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М. : Горячая линия-Телеком,2012.- 130 с. Режим доступа: http://nwapa.spb.ru

Электронно-библиотечная система. Издательство «Лань» [Электронный ресурс] Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3 / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М. : Горячая линия-Телеком,2012.- 170 с. Режим доступа: http://nwapa.spb.ru

6.3. Учебно-методическое обеспечение самостоятельной работы.

Положение об организации самостоятельной работы студентов АНОВО «Институт социальных наук».

Положение о курсовой работе (проекте) выполняемой студентами АНОВО «Институт социальных наук»

Нормативные правовые документы.

Не используются

6.4. Интернет-ресурсы.

Русскоязычные ресурсы

Электронные учебники электронно - библиотечной системы (ЭБС) «Айбукс»

Электронные учебники электронно – библиотечной системы (ЭБС) «Лань»

Иные источники.

– Не используются.

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Курс включает использование программного обеспечения операционной системы Windows XP или Windows 7, пакет программ MS Office 2013, 2016, виртуальной машины MSWare, программной системы «Контур информационной безопасности» компании SearchInform, справочная электронной системы «Гарант» для подготовки текстового и табличного материала.

Методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов).

Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы)

Для организации дистанционного обучения используется система Moodle.