Автономная некоммерческая организация высшего образования
“ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА”
ФАКУЛЬТЕТ УПРАВЛЕНИЯ БИЗНЕСОМ

УТВЕРЖДАЮ
Ректор _____С.С. Юров
«29» июня 2023 г.

Б1.О.04 МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.05 ЗАЩИТА ИНФОРМАЦИИ

Для направления подготовки:
38.03.05 Бизнес-информатика
(уровень бакалавриата)

Типы задач профессиональной деятельности:
организационно-управленческий; проектный

Направленность (профиль):
Управление цифровыми продуктами

Форма обучения:
очная

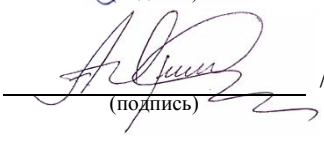
Москва – 2023

Разработчик: Мелехов Игорь Сергеевич, преподаватель кафедры гуманитарных и естественно-научных дисциплин АНО ВО «Институт бизнеса и дизайна».

«21» июня 2023 г.  /И.С.Мелехов/

СОГЛАСОВАНО:

Декан факультета  /Н.Е. Козырева /
(подпись)

Заведующий кафедрой
разработчика РПД  /А.Б. Оришев /
(подпись)

Протокол заседания кафедры № 10 от «22» июня 2023 г.

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

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

Задачи:

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Место дисциплины в учебном плане:
Блок: Блок 1. Дисциплины (модули).
Часть: Обязательная часть.
Модуль: Модуль общепрофессиональной подготовки.
Осваивается: 4 семестр.

3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК - 2 - способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

ОПК - 3 - способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

		Владеет: способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов
ОПК-3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	**ОПК-3.2.** Знает современные стандарты информационного взаимодействия систем	**Знает:** методологию подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности **Умеет:** самостоятельно подготавливать обзоры, аннотации, рефераты, научные доклады, публикации при решении задач профессиональной деятельности **Владеет:** навыками самостоятельной подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности с учетом требований информационной безопасности

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Защита информации» для студентов очной формы обучения, реализуемой в АНО ВО «Институт бизнеса и дизайна» по направлению подготовки 38.03.05 Бизнес-информатика составляет: 3 з.е. / 108 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц
Аудиторные занятия	72
в том числе:	
Лекции	36
Практические занятия	36
Лабораторные работы	-
Самостоятельная работа	36
в том числе:	
часы на выполнение КР / КП	-
Промежуточная аттестация:	
Вид	Зачет с оценкой
Трудоемкость (час.)	
Общая трудоемкость з.е. / часов	3 з.е. / 108 час.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Темы дисциплины		Количество часов			
№	Наименование	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
1	Понятие и сущность информационной безопасности и защиты информации	2	2	-	4
2	Становление и развитие информационной безопасности и защиты информации	2	2	-	4
3	Правовой уровень обеспечения информационной безопасности	4	4	-	4
4	Информационная безопасность в системе национальной безопасности РФ	4	4	-	4
5	Основы государственной политики РФ в области информационной безопасности	4	4	-	4
6	Основные угрозы информационной безопасности	4	4	-	4
7	Методы и средства обеспечения информационной безопасности и защиты информации	4	4	-	4
8	Административный уровень обеспечения информационной безопасности и защиты информации	4	4	-	4
9	Процедурный уровень обеспечения информационной безопасности и защиты информации	4	4	-	2
10	Аппаратно- программный уровень обеспечения информационной безопасности и защиты информации	4	4	-	2
	Итого (часов)	36	36	-	36
	Форма контроля:	Зачет с оценкой			
	Всего по дисциплине:	108 / 3 з.е.			

СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

Тема 1. Понятие и сущность информационной

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

Тема 2. Становление и развитие информационной безопасности и защиты информации

Цели и задачи информационной безопасности в Российской Федерации. Связь информационной безопасности с информатизацией общества. Базовые уровни обеспечения информационной безопасности и защиты информации.

Тема 3. Правовой уровень обеспечения информационной безопасности.

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации. Роль в России Межведомственной комиссии по защите государственной

тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне.

Тема 4. Информационная безопасность в системе национальной безопасности РФ

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности.

Основания и методика отнесения сведений к коммерческой тайне.

Тема 5. Основы государственной политики РФ в области информационной безопасности

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности.

Основания и методика отнесения сведений к коммерческой тайне.

Тема 6. Основные угрозы информационной безопасности

Классификация источников угроз безопасности информации по принципу и характеру его воздействия на объект защиты. Методы и способы воздействия источников угроз на объект защиты в зависимости от используемых средств нападения. Классификация угроз безопасности информации по степени нарушения состояния информационной безопасности (доступности, целостности, конфиденциальности). Каналы несанкционированного доступа к информационным ресурсам в информационной системе. Цели и задачи по защите информационных ресурсов от несанкционированного доступа в соответствии с нормативно-правовыми документами России.

Тема 7. Методы и средства обеспечения информационной безопасности и защиты

Правовые, организационно-технические и экономические методы обеспечения информационной безопасности. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Тема 8. Административный уровень обеспечения информационной безопасности и защиты информации.

Правовые, организационно-технические и экономические методы обеспечения информационной безопасности. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Тема 9. Процедурный уровень обеспечения информационной безопасности и защиты информации.

Основные классы мер процедурного уровня Управление персоналом Физическая защита Поддержание работоспособности Реагирование на нарушения режима безопасности Планирование восстановительных работ

Тема 10. Аппаратно- программный уровень обеспечения информационной безопасности и защиты информации

Программно-аппаратные сервисы обеспечения безопасности информационных ресурсов в информационных системах. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Процедура формирования электронной подписи. Экранирование информации в информационно-телекоммуникационных сетях. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с вредоносными программами. Управление высокой доступности.

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

Курсовая работа не предусмотрена

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

9.1. Рекомендуемая литература:

1. Мансуров, Г. З. Право цифровой безопасности : учебник : [16+] / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=687364
2. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485
3. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие : [16+] / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; под науч. ред. А. Г. Волеводза ; Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации. – Москва : Прометей, 2023. – 1086 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=701090
4. Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие : [16+] / О. В. Литвиненко. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. – 63 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694774
5. Цветкова, Е. М. Технический контроль и информационная защита : учебное пособие : [16+] / Е. М. Цветкова, И. О. Танрывердиев ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 64 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612595
6. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611084

9.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.

При осуществлении образовательного процесса по данной учебной дисциплине предполагается использование:

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:

1. Windows 10 Pro Professional (Договор: Tr000391618, Лицензия: V8732726);
2. Microsoft Office Professional Plus 2019 (Договор: Tr000391618, Лицензия: V8732726).
3. Браузер Google Chrome;
4. Браузер Yandex;
5. Adobe Reader - программа для просмотра, печати и комментирования документов в формате PDF

9.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://biblioclub.ru/ - университетская библиотечная система online Библиоклуб.ру
2. http://window.edu.ru/ - единое окно доступа к образовательным ресурса
3. https://uisrussia.msu.ru/ - база данных и аналитических публикаций университетской информационной системы Россия
4. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
5. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
6. https://gufo.me/ - справочная база энциклопедий и словарей
7. Единый федеральный реестр сведений о банкротстве https://bankrot.fedresurs.ru/
8. https://slovaronline.com - поисковая система по всем доступным словарям и энциклопедиям
9. https://www.tandfonline.com/ - коллекция журналов Taylor&Francis Group включает в себя около двух тысяч журналов и более 4,5 млн. статей по различным областям знаний
10. http://pravo.gov.ru/ - официальный интернет-портал правовой информации
11. https://minjust.gov.ru/ru/ - Министерство юстиции Российской Федерации
12. https://digital.gov.ru/ru/ - официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации
13. http://www.securitylab.ru - информационный портал о защите информации

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.
2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

4. Аудио и видеоаппаратура.

№ 403

Учебная аудитория для проведения учебных занятий. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети «Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

№ 402

Помещение для самостоятельной работы. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети «Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Продуктивность усвоения учебного материала во многом определяется интенсивностью и качеством самостоятельной работы студента. Самостоятельная работа предполагает формирование культуры умственного труда, самостоятельности и инициативы в поиске и приобретении знаний; закрепление знаний и навыков, полученных на всех видах учебных занятий; подготовку к предстоящим занятиям, экзаменам; выполнение контрольных работ.

Самостоятельный труд развивает такие качества, как организованность, дисциплинированность, волю, упорство в достижении поставленной цели, вырабатывает умение анализировать факты и явления, учит самостоятельному мышлению, что приводит к развитию и созданию собственного мнения, своих взглядов. Умение работать самостоятельно необходимо не только для успешного усвоения содержания учебной программы, но и для дальнейшей творческой деятельности.

Основу самостоятельной работы студента составляет работа с учебной и научной литературой. Из опыта работы с книгой (текстом) следует определенная последовательность действий, которой целесообразно придерживаться. Сначала прочитать весь текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом (не запоминать, а понять общий смысл прочитанного). Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом.

Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую

информацию, целесообразно его законспектировать.

Результаты конспектирования могут быть представлены в различных формах:

- **План** – это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект.

- **Конспект** – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов.

- **План-конспект** – это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.

- **Текстуальный конспект** – это воспроизведение наиболее важных положений и фактов источника.

- **Свободный конспект** – это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.

- **Тематический конспект** – составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

В процессе изучения материала источника, составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым, удобным для работы.

Подготовка к практическому занятию включает 2 этапа:

Первый этап – организационный;

Второй этап - закрепление и углубление теоретических знаний.

На первом этапе студент планирует свою самостоятельную работу, которая включает:

- уяснение задания на самостоятельную работу;
- подбор рекомендованной литературы;
- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.

Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам.

В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь.

При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

Методические рекомендации для обучающихся с ОВЗ и инвалидов по освоению дисциплины

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья имеют возможность изучать дисциплину по индивидуальному плану, согласованному с преподавателем и деканатом.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения.

При освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья по индивидуальному плану предполагаются: изучение дисциплины с использованием информационных средств; индивидуальные консультации с преподавателем (разъяснение учебного материала и углубленное изучение материала), индивидуальная самостоятельная работа.

В процессе обучения студентам из числа инвалидов и лиц с ограниченными возможностями здоровья информация предоставляется в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа (с возможностью увеличения шрифта).

В случае необходимости информация может быть представлена в форме аудиофайла.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Индивидуальные консультации с преподавателем проводятся по отдельному расписанию, утвержденному заведующим кафедрой (в соответствии с индивидуальным графиком занятий обучающегося).

Индивидуальная самостоятельная работа обучающихся проводится в соответствии с рабочей программой дисциплины и индивидуальным графиком занятий.

Текущий контроль по дисциплине осуществляется в соответствии с фондом оценочных средств, в формах адаптированных к ограничениям здоровья и восприятия информации обучающихся.

Приложение 1

Автономная некоммерческая организация высшего образования
«ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА»

Факультет управления бизнесом

Фонд оценочных средств

Текущего контроля и промежуточной аттестации
по дисциплине (модулю)

Б1.О.04.05 ЗАЩИТА ИНФОРМАЦИИ

Для направления подготовки:
38.03.05 Бизнес-информатика
(уровень бакалавриата)

Типы задач профессиональной деятельности:
организационно-управленческий; проектный.

Направленность (профиль):
Управление цифровыми продуктами

Форма обучения:
очная

Москва – 2023

РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов
ОПК-3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	**ОПК-3.2.** Знает современные стандарты информационного взаимодействия систем	**Знает:** методологию подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности **Умеет:** самостоятельно подготавливать обзоры, аннотации, рефераты, научные доклады, публикации при решении задач профессиональной деятельности **Владеет:** навыками самостоятельной подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности с учетом требований информационной безопасности

Показатели оценивания результатов обучения

Шкала оценивания			
Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
УК-2.2 Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения			
Не знает: методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Не умеет:** определять круг задач, планировать и выбирать пути их	**Поверхностно знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **В целом умеет:** определять круг задач,	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения, но допускает несущественные ошибки **Умеет:** определять круг	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их

решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Не владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов	планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но испытывает затруднения **В целом владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но испытывает сильные затруднения	задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но иногда затрудняется с объективной оценкой **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но иногда допускает ошибки	решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов
ОПК-3.2. Знает современные стандарты информационного взаимодействия систем			
Не знает: методологию подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности **Не умеет:** самостоятельно подготавливать обзоры, аннотации, рефераты, научные доклады, публикации при решении задач профессиональной деятельности **Не владеет:** навыком навыками самостоятельной подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности с учетом требований информационной безопасности	**Поверхностно знает:** методологию подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности **В целом умеет:** правильно трактовать и самостоятельно подготавливать обзоры, аннотации, рефераты, научные доклады, публикации при решении задач профессиональной деятельности, но испытывает затруднения **В целом владеет:** навыками самостоятельной подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности с учетом требований информационной безопасности, но испытывает сильные затруднения	**Знает:** методологию подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности, но допускает несущественные ошибки **Умеет:** самостоятельно подготавливать обзоры, аннотации, рефераты, научные доклады, публикации при решении задач профессиональной деятельности, но иногда затрудняется с объективной оценкой **Владеет:** навыками самостоятельной подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности с учетом требований информационной безопасности, но иногда допускает ошибки	**Знает:** методологию подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности **Умеет:** самостоятельно подготавливать обзоры, аннотации, рефераты, научные доклады, публикации при решении задач профессиональной деятельности **Владеет:** навыками самостоятельной подготовки обзоров, аннотаций, рефератов, научных докладов, публикаций при решении задач профессиональной деятельности с учетом требований информационной безопасности

Оценочные средства

Задания для текущего контроля

Пример теста:

1. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:
а) со стороны злоумышленника;
б) со стороны законного отправителя сообщения;
в) со стороны законного получателя сообщения.

2. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?
а) асимметричный;
б) симметричный;
в) правильного ответа нет.

3. Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:
а) шифрование;
б) дешифровка;
в) расшифровка.

4. В каких основных форматах существует симметричный алгоритм?
а) блока и строки;
б) потока и блока;
в) потока и данных

5. Открытым текстом в криптографии называют:
а) расшифрованный текст;
б) любое послание;
в) исходное послание.

6. Какой ключ известен только приемнику?
а) открытый;
б) закрытый.

7. Наука, занимающаяся защитой информации, путем преобразования этой информации это:
а) криптография;
б) криптология;
в) криптоанализ.

8. В каких шифрах результат шифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных?
а) в потоковых;
б) в блочных.

9. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:
а) шифр функциональных преобразований;
б) шифр замен;
в) шифр перестановок.

10. Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:
а) функция шифрования шага преобразования;
б) инвариант стандартного шага шифрования.

11. Шифрование-это:
а) процесс создания алгоритмов шифрования;
б) процесс сжатия информации;
в) процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется.

12. В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?
а) при шифровании с помощью асимметричного алгоритма;
б) при шифровании с помощью симметричного алгоритма;
в) арбитр необходим всегда.

13. Можно ли отнести слабую аутентификацию к проблемам безопасности?
а) нет;
б) да;
в) в редких случаях.

14. Возможно ли расшифровывать информацию без знания ключа?
а) нет;
б) да;
в) в редких случаях.

15. Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?
а) нет;
б) да;
в) в редких случаях.

16. Характерная черта алгоритма Эль-Гамаля состоит в:
а) протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя;
б) в точной своевременной передаче сообщения;
в) алгоритм не имеет особенностей и идентичен RSA.

17. Аутентификацией называют:
а) процесс регистрации в системе;

б) способ защиты системы;
в) процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов.

18. Аутентификация бывает:
а) Статическая;
б) устойчивая;
в) постоянная;
г) все варианты правильные;
д) правильного варианта нет.

19. Стойкость ключа характеризуется
а) длинной;
б) непредсказуемостью;
в) все варианты правильные;
г) правильного варианта нет.

20. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:
а) на основе произвольно выбранного шифротекста;
б) на основе произвольно выбранного открытого текста;
в) на основе только шифротекста.

21. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:
а) на основе произвольно выбранного шифротекста;
б) на основе произвольно выбранного открытого текста;
в) правильного ответа нет.

Оценка формируется следующим образом:

- оценка «отлично» - 85-100% правильных ответов;
- оценка «хорошо» - 70-84% правильных ответов;
- оценка «удовлетворительно» - 40-69% правильных ответов;
- оценка «неудовлетворительно» - менее 39% правильных ответов.

Примерные темы рефератов

1. Цели и задачи защиты информации.
2. Проблемы защиты информации.
3. Этапы развития концепции обеспечения безопасности информации. Общие теоретические принципы теории безопасности.
4. Общие методические принципы теории безопасности. Проблемы информационного противоборства.

5. Государственная политика в информационной сфере. Региональные проблемы информационной безопасности.
6. Современная доктрина информационной безопасности Российской Федерации.
7. Современная концепция информационной безопасности.
8. Основное содержание теории защиты информации.
9. Общеметодологические принципы формирования теории защиты информации. Модели систем и процессов защиты информации.
10. Особенности и состав научно-методологического базиса решения задач защиты информации. Нечеткие множества.
11. Нестрогая математика. Методы оценки.
12. Неформальный поиск оптимальных решений. Требования системного подхода к защите информации.
13. Условия обеспечения требований безопасности. Виды обеспечения системы информационной безопасности.
14. Концептуальная модель информационной безопасности.
15. Критерии, условия и принципы отнесения информации к защищаемой.
16. Количественная и качественная оценки ценности информации. Категории важности информации.
17. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности: государственная тайна, коммерческая тайна, коммерческая информация, персональная информация, информация для внутреннего пользования и др.
18. Виды и типы угроз безопасности. Классификация угроз.
19. Классификация угроз конфиденциальности, целостности и доступности информации. Изменение активности угроз в зависимости от стадии жизненного цикла.
20. Формирование и коррекция кортесов потенциальных угроз.
21. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
22. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
23. Виды уязвимости информации и формы ее проявления. Каналы несанкционированного получения информации. Радиоканалы утечки информации.
24. Акустические каналы утечки информации. Электрические каналы утечки информации. Визуально-оптические каналы утечки информации.
25. Материально-вещественные каналы утечки информации. Линии связи.
26. Каналы утечки информации при эксплуатации ЭВМ.
27. Методы и средства несанкционированного получения информации по техническим каналам. Методы и средства разрушения информации.
28. Направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации.
29. Система мер, направленных на обеспечение информационной безопасности. Подходы к созданию комплексной системы защиты информации.
30. Виды защиты информации. Характеристики защитных действий. Кадровое и ресурсное обеспечение защиты информации.
31. Современные методы и средства оценивания состояния безопасности информационных систем: препятствие, управление доступом, маскировка,

регламентация, принуждение, побуждение.

32. Классификация средств защиты информации. Технические средства защиты информации. Программные средства защиты.
33. Программно-технические средства защиты. Криптографическая защита.
34. Скремблирование. Стеганография.
35. Законодательные средства. Организационные средства защиты. Морально-этические средства.
36. Кадровое и ресурсное обеспечение защиты информации. Построение систем защиты информации.
37. Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты.
38. Функциональное, организационное и структурное построение систем защиты информации. Типизация систем защиты.
39. Стандартизация систем защиты. Современные факторы, влияющие на защиту информации

Оценка рефератов производится по шкале «зачтено» / «не зачтено».

Примерные вопросы к зачету с оценкой

1. Опишите необходимость и значимость нормативно-правовых документов в области информационной безопасности.
2. Дайте определение информационной безопасности и защите информации.
3. Назовите основные компоненты (параметры) информационной безопасности.
4. Перечислите цели и основные задачи в области обеспечения информационной безопасности.
5. Назовите цели и задачи информационной безопасности в Российской Федерации.
6. Опишите связь информационной безопасности с информатизацией общества.
7. Назовите базовые уровни обеспечения информационной безопасности и защиты информации.
8. Перечислите основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации.
9. перечислите основные задачи Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну.
10. Значение обеспечения безопасности коммерческой тайны в системе предпринимательской деятельности.
11. Опешите порядок отнесения сведений к коммерческой тайне.
12. Порядок формирования на фирме перечня сведений, относящихся к коммерческой тайне.
13. Дайте определение национальная безопасность.
14. Назовите виды безопасности и дайте им определение: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая.
15. Перечислите виды защищаемой информации.

16. Назначение и роль информационной безопасности в обеспечение национальной безопасности государства.
17. Перечислите национальные интересы РФ в информационной сфере и методы их обеспечения.
18. Перечислите виды угроз национальной безопасности РФ.
19. Назовите возможные сценарии подрыва национальных интересов РФ.
20. Проведите классификацию источников угроз безопасности информации по принципу и характеру его воздействия на объект защиты.
21. Перечислите методы и способы воздействия источников угроз на объект защиты в зависимости от используемых средств нападения.
22. Проведите классификацию угроз безопасности информации по степени нарушения состояния информационной безопасности (доступности, целостности, конфиденциальности).
23. Назовите возможные каналы несанкционированного доступа к информационным ресурсам в информационной системе.
24. Перечислите цели и задачи по защите информационных ресурсов от несанкционированного доступа в соответствии с нормативно-правовыми документами России.
25. Перечислите правовые, и организационные методы обеспечения информационной безопасности
26. Перечислите технические методы обеспечения информационной безопасности
27. Перечислите экономические методы обеспечения информационной безопасности.
28. Назовите модели и системы обеспечения информационной безопасности.
29. Перечислите классы защищенности от несанкционированного доступа к средствам вычислительной техники и автоматизированным системам.
30. Перечислите концептуальные основы обеспечения информационной безопасности.
31. Назовите состав, структуру и содержимое документа политика информационной безопасности
32. Перечислите задачи, решаемые при анализе рисков для информационных систем.
33. Назовите базовые методики, используемые для оценки рисков.
34. Перечислите основные стандарты в области разработки политики информационной безопасности и анализа рисков.
35. Перечислите базовые инструментальные средства для анализа рисков и управления рисками.
36. Основные классы мер процедурного уровня
37. Физическая защита
38. Поддержание работоспособности
39. Реагирование на нарушения режима безопасности
40. Планирование восстановительных работ
41. Программно-аппаратные сервисы обеспечения безопасности информационных ресурсов в информационных системах.
42. Идентификация и аутентификация пользователей как передовой рубеж защиты информации.
43. Базовые методы парольной аутентификации. Модели разграничения доступа к информации.

44. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности.
45. Базовые методы криптографического преобразования данных.
46. Потоковое и блочное шифрование.
47. Процедура формирования электронной подписи.
48. Экранирование информации в информационно-телекоммуникационных сетях (ИТС).
49. Основные сервисы защиты в ИТС.
50. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.

Критерии оценки при проведении промежуточной аттестации

<table>
<tr><th>4-балльная шкала (экзамен, зачет с оценкой)</th><th>Двух-балльная шкала (зачет)</th><th>Показатели</th><th>Критерии</th></tr>
<tr><td>Отлично</td><td rowspan="3">зачтено</td><td rowspan="4">1. Полнота ответов на вопросы и выполнения задания.
2. Аргументированность выводов.
3. Умение перевести теоретические знания в практическую плоскость.</td><td>глубокое знание теоретической части темы, умение проиллюстрировать изложенное примерами, полный ответ на вопросы</td></tr>
<tr><td>Хорошо</td><td>глубокое знание теоретических вопросов, ответы на вопросы преподавателя, но допущены незначительные ошибки</td></tr>
<tr><td>Удовлетворительно</td><td>знание структуры основного учебно-программного материала, основных положений теории при наличии существенных пробелов в деталях, затруднения при практическом применении теории, существенные ошибки при ответах на вопросы преподавателя</td></tr>
<tr><td>Неудовлетворительно</td><td>Не зачтено</td><td>существенные пробелы в знаниях основных положений теории, не владение терминологией, основными методиками, не способность формулировать свои мысли, применять на практике теоретические положения, отвечать на вопросы преподавателя</td></tr>
</table>