

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.06.1 Международная информационная безопасность

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

Автор программы:

Анурьева Мария Сергеевна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	11
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	29
6. Учебно-методическое и информационное обеспечение дисциплины.....	31
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	31

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	На основе международных стандартов информационной безопасности администрирует программно-аппаратные средства защиты информации в компьютерных сетях

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		3	4	5	8
1	"Networksecurity"		+		
2	International information security			+	
3	Анализ защищенности компьютерных сетей		+		
4	Безопасность компьютерных сетей		+		
5	Компьютерные сети	+	+		
6	Стандарты в области информационной безопасности			+	
7	Эксплуатационная практика				+

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Международная информационная безопасность» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Международная информационная безопасность» изучается в 5 семестре.

3.Объем и содержание дисциплины

3.1.Объем дисциплины:

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	144
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Экзамен	36

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
5 семестр					
1	Этапы развития и структура системы защиты информации в зарубежных странах.	4	4	6	Тестирование
2	Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке.	4	4	6	Тестирование
3	Состояние проблемы информационной безопасности в странах Евросоюза.	4	4	6	Тестирование
4	Система защиты информации в США.	4	4	6	Тестирование
5	Система защиты информации в Великобритании.	4	4	6	Тестирование

6	Системы защиты информации во Франции.	6	6	6	Тестирование
7	Системы защиты информации в Китае.	6	6	8	Тестирование

Тема 1. Этапы развития и структура системы защиты информации в зарубежных странах. (ПК-2)

Лекция.

История развития систем защиты информации в зарубежных странах. Этапы развития системы защиты информации в настоящее время. Структура систем защиты информации, применяемых в общемировой практики обеспечения информационной безопасности: организационная защита информации, техническая или инженерно-техническая защита информации, программно-аппаратная защита, криптографические методы, психологические виды защиты, морально-этические виды защиты, страховая защита информации. Основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма.

Лабораторные работы.

Выполнить практическую работу

Задания для самостоятельной работы.

1. Систематизация истории развития методов и средств ЗИ в процессе эволюции человечества.
2. Выделите особенности второго и третьего периода развития методов и средств ЗИ.
3. Каковы основные виды носителей информации были в 60-80 гг. ?
4. На какой период приходится наиболее интенсивное решение проблем информационной безопасности?
5. Охарактеризуйте современное состояние проблемы защиты информации в мире.
6. Назовите основные элементы типовой системы защиты информации в современной системе.

Тема 2. Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке. (ПК-2)

Лекция.

Выработка навыка анализа защиты информации в древности (Древние Германия, Ирландия, Исландия, Дания и другие скандинавские страны, Древние Греция и Рим, Древние Египет и Месопотамия, Страны Ближнего Востока, Древняя Индия, Древняя Япония, Древний Китай). Защита информации в средние века (Средневековая Европа). Защита информации в 17-19 веках. Защита информации в 1-й половине XX в. Защита информации во время второй мировой войны. Защита информации во второй половине XX в.

Лабораторные работы.

Криптографическая защита информации на начальном этапе.

Задания для самостоятельной работы.

- Записать краткий конспект лекции.
- Изучить базовую и дополнительную литературу по теме лекции
- Выполнить лабораторную работу.

Тематика вопросов:

1. Как шифровали информацию при помощи рун?
2. В чем заключается формирования и каковы особенности систем защиты информации в древнем Китае и Индии?
3. Каковы источники, характеризующие особенности и закономерности становления систем защиты информации в Древнем мире?
4. Каковы особенности систем защиты коммерческой тайны в странах Западной Европы в XIX - начале XX вв?
5. Перечислите этапы становление системы защиты информации в США?
6. Чем европейские подходы к защите информации отличается от восточных?
7. Что понимается под «индейской криптографией»?
8. В чем было слабое место в германской машине Энигма?

Тема 3. Состояние проблемы информационной безопасности в странах Евросоюза. (ПК-2)

Лекция.

Европейское агентство по сетевой и информационной безопасности (ENISA) и государственные стратегии кибербезопасности. Центр по борьбе с киберпреступностью. Ближайшие проекты Евросоюза.

Лабораторные работы.

Принципы шифрования. Анализ развития зарубежной практики применения алгоритмов криптографической защиты данных.

Задания для самостоятельной работы.

- Записать краткий конспект лекции.
- Изучить базовую и дополнительную литературу по теме лекции
- Выполнить практическую работу

Тематика вопросов:

1. Когда и с какой целью был создан Европейский союз?

2. Что такое информационное оружие?
3. Какова основная особенность информационного оружия?
4. С какой целью было создано Европейское агентство по сетевой и информационной безопасности?
5. Какие факторы оказывают влияние на функционирование ключевых информационных систем общего пользования?
6. Что такое кибербезопасность?
7. Для чего ENISA разработало специальное руководство GoodPracticeGuide on NCSS?
8. Каковы сферы ответственности Европейского центра по борьбе с киберпреступностью?
9. Каковы основные направления обеспечения Информационной безопасности Евросоюза в краткосрочной перспективе?
10. В чем суть новых правил защиты персональных данных, предложенных на рассмотрение в ЕС?

Тема 4. Система защиты информации в США. (ПК-2)

Лекция.

Концепция национальной безопасности США. Государственные органы обеспечения национальной безопасности США. Разведывательное управление (DI). Оперативное управление (DO). Научно-техническое управление (DS&T). Административное управление (DA). Поиск, анализ и систематизирование научной информации, отечественного и зарубежного опыта по теме исследования.

Лабораторные работы.

Изучение государственных органов обеспечения информационной безопасности США.

Задания для самостоятельной работы.

- Записать краткий конспект лекции.
- Изучить базовую и дополнительную литературу по теме лекции
- Выполнить практическую работу

Тематика вопросов:

1. Перечислите нормативно-правовые акты, регламентирующие государственную политику США в области информатизации.
2. Какую политику должны вести США для успешной реализации положений Концепции национальной безопасности США?

3. Что является результатом реализации положений Концепции национальной безопасности США?
4. Какими директивами Президента США регламентируется решение важные стратегические вопросы национальной политики в сфере информационной безопасности?
5. Что такое «Разведывательное Сообщество» США и какие организации в него входят?
6. Какие органы исполнительной власти США занимаются исключительно только разведывательной деятельностью?
7. Какие структурные подразделения входят в состав ЦРУ?
8. Назовите причины и цели создания Министерства внутренней безопасности США.
9. Какие управления и отделы входят в состав Национального управления военно-космической разведки США?
10. Какие методы использует АНБ в своей профессиональной деятельности?

Тема 5. Система защиты информации в Великобритании. (ПК-2)

Лекция.

Парламентский комитет по разведке и безопасности Великобритании (IntelligenceAndSecurityCommittee /ISC/). Разведывательная служба Великобритании SecretIntelligenceService / MI6. Контрразведывательная служба MI-5. Центр правительственной связи (GovernmentCommunicationsHeadquarters /GCHQ/). Программные средства ИБ.

Лабораторные работы.

Стандарты ИБ. Структура затрат на защиту информации в правительстве Британии.

Задания для самостоятельной работы.

Поиск информации о государственных органах обеспечения информационной безопасности Великобритании.

Тема 6. Системы защиты информации во Франции. (ПК-2)

Лекция.

Спецслужбы Французской республики. Структура спецслужб Французской республики. ДГСЕ. Управление военной разведки (ДРМ). Структура ДРМ.

Лабораторные работы.

Изучение государственных органов обеспечения информационной безопасности Франции.

Задания для самостоятельной работы.

1. Как правительство Франции рассматривает концепцию информационной войны?
2. Чем французское представление экономического конфликта отличается от других европейских стран?

3. Анализ преимуществ виртуальной войны?

4. Для каких целей во Франции создаётся информационно-аналитическая система поддержки принятия решений?

5. Какие методы по мнению французских экспертов обеспечивает надёжную защиту информации и какие меры необходимы для достижения этих методов?

6. Что препятствует защитным действиям по предотвращению и снижению угроз информационной войны?

Тема 7. Системы защиты информации в Китае. (ПК-2)

Лекция.

Представление об информационном противоборстве в Китае. Законодательство в сфере информационной безопасности в Китае. Обеспечение безопасности компьютерных и информационных систем. Организационная структура спецслужб Китая. «Великая стена» информационной безопасности Китая. Министерство государственной безопасности КНР. Поиск, анализ и систематизирование научной информации, отечественного и зарубежного опыта по теме исследования.

Лабораторные работы.

Изучение государственных органов обеспечения информационной безопасности Китая.

Задания для самостоятельной работы.

1. Охарактеризуйте нормативно-правовую базу Китая в сфере ИБ и ответственность за компьютерные преступления в Китае.

2. Перечислите основные спецслужбы Китая, какие функции они выполняют?

3. Что такое «Великая стена» информационной безопасности Китая? Чем она отличается от политики ИБ в России?

4. Каковы особенности поддержки Интернет-ресурсов частными лицами в Китае?

5. Какие задачи решаются в Китае в рамках интеграции в мировые информационные системы?
6. Что подразумевается под собой "Концепция сетевых сил" ?
7. Назовите основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны.
8. Что представляет собой концепция ИВ Китая?
9. Каковы основные элементы правовой системы ИБ Китая?
10. Каковы основные мероприятия по обеспечению ИБ Китая, осуществляемые в процессе интеграции в глобальную сеть Интернет?

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

5 семестр

- посещаемость – 5 баллов
- текущий контроль – 45 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 10 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Макс. кол-во баллов	Методика проведения занятия и оценки
1.	Этапы развития и структура системы защиты информации в зарубежных странах.	Тестирование	9	8-9 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;

2.	Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке.	Тестирование(контрольный срез)	10	10 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;
3.	Состояние проблемы информационной безопасности в странах Евросоюза.	Тестирование	9	8-9 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;
4.	Система защиты информации в США.	Тестирование	9	8-9 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;
5.	Система защиты информации в Великобритании.	Тестирование(контрольный срез)	10	10 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;
6.	Системы защиты информации во Франции.	Тестирование	9	8-9 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;
7.	Системы защиты информации в Китае.	Тестирование	9	8-9 баллов – студент правильно отвечает на 75-100% вопросов в тесте; 6-7 баллов - студент правильно ответил на 50-75% вопросов; 3-4 баллов - студент правильно ответил на 25-50% вопросов; 2 балла - правильных ответов менее 25% теста;
8.	Посещаемость		5	5 баллов – стопроцентное посещение занятий студентом 4 баллов – посещаемость студента составляет не менее 80 % занятий 3 баллов – посещаемость студента составляет не менее 50 % занятий 2 балла – посещаемость студента составляет не менее 25 % занятий
9.	Премияльные баллы		10	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

10.	Ответ на экзамене	30	25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно»
11.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	70	Добор: студент может предоставить все задания текущего контроля и контрольные срезы
12.	Итого за семестр	100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Тестирование

Тема 1. Этапы развития и структура системы защиты информации в зарубежных странах.

1. На сколько периодов делится процесс развития средств и методов ЗИ?

- a. 1
- b. 2
- c. 3
- d. 4

2. Кто автор «дискового шифра»?

- a. А. Дамм
- b. Т. Джефферсон
- c. А. Тьюринг
- d. Л. Эйлер

3. Наиболее распространенной в автоматизированной системе обработки данных (АСОД) в 60-70 гг. была(-и) проверка(-и)

- a. по доступу к базе данных
- b. по разграничению доступа к массиву данных
- c. по отпечатку пальца
- d. по методу шифрования

4. К характеристикам этапа развития системы ЗИ в 70-80 гг. НЕ относится

- a. объединение всех применяемых средств защиты в самостоятельные системы
- b. осознание необходимости комплексирования целей защиты
- c. изменение методологического подхода к ЗИ
- d. осознание необходимости комплексирования целей защиты

5. На каких признаках в 70-80 гг. разрабатывались методы и средства для опознавания лиц, имеющих право пользоваться КИ?

- a. все перечисленное
- b. отпечатки пальцев
- c. голос
- d. сетчатка глаза

6. Основной задачей третьего этапа (80ые г-настоящее время) является:

- a. объединение всех применяемых средств защиты
- b. комплексирование целей защиты
- c. перевод процесса ЗИ на строго научную основу
- d. изобретение нового метода шифрования

7.Соединение в единое целое отдельных элементов, механизмов, процессов, явлений, мероприятий, мер и программ их взаимосвязей, способствующих реализации целей защиты и обеспечению структурного построения системы защиты – это...

- a. Защита Информации
- b. Подсистема Защиты Информации
- c. Информационная Безопасность
- d. Конфиденциальность Информации

8.Защита информации, предусматривающая возмещение убытков от ее уничтожения или модификации путем получения выплат

- a. страховая ЗИ
- b. организационная ЗИ
- c. криптографическая ЗИ
- d. техническая ЗИ

Тема 2. Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке.

1.Как называется классический общегерманский рунический строй?

- a. Энея
- b. Друид
- c. Атта
- d. Футарк

2.Наиболее распространенный шифр в Древней Греции и Риме:

- a. Аристотеля
- b. Светония
- c. Платона

d. Цезаря

3. Кто изобрел «книжный шифр»?

a. Полибий

b. Аристотель

c. Плутарх

d. Эней

4. Кто первыми открыли и описали методы криптоанализа?

a. греки

b. индусы

c. немцы

d. арабы

5. Что НЕ входило в функции агентов в Древней Индии?

a. выявление шпионов

b. наблюдение за партиями

c. контроль за родственниками царя

d. охрана периметров

6. Кто придумал первый транспозиционный шифр?

a. Д. Кардано

b. А. Тьюринг

c. Г. Л. Вильена

d. Ф. Бэкон

7.Как называется первый документ на территории Америки, в котором используется шифр «caracteres ignotos»?

- a. нет верного ответа
- b. письма Э.Кортеса
- c. переписка католических орденов
- d. депеша Христофора Колумба

8.Отцом криптографии США называли:

- a. Б.Чёрча
- b. Д.Ловелля
- c. Т.Джефферсона
- d. Ч.Уитстона

9.Кто изобрел машину с вращательными шифровальными дисками с различным количеством букв?

- a. Ж.-Ф.Шампольон
- b. Д.Вадсворт
- c. А.Тьюринг
- d. Ч.Уитстон

Тема 3. Состояние проблемы информационной безопасности в странах Евросоюза.

1.Какую особенность использования информационного оружия особо выделяют эксперты?

- a. достоверность
- b. скрытность
- c. уязвимость
- d. открытость

2.Какая страна имеет лидерство в сфере разработок в области систем связи и обработки данных?

- a. Германия
- b. Англия
- c. США
- d. Россия

3.Какая страна в рамках ВТО НЕ согласовала отмену внутренних ограничений на допуск иностранного капитала в область национальных телекоммуникаций?

- a. Испания
- b. Франция
- c. Бельгия
- d. Италия

4.Как называется европейское агентство по сетевой и ИБ?

- a. Юнеско
- b. ЕАСИБ
- c. нет верного ответа
- d. ENISA

5.Набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя это:

- a. техническая безопасность
- b. национальная безопасность

c. кибербезопасность

d. организационная безопасность

6. Как называется стратегия защиты от киберугроз, опубликованная Еврокомиссией?

a. «Открытое и безопасное киберпространство»

b. «Безопасное киберпространство»

c. «Открытое, безопасное и надежное киберпространство»

d. «Открытое и надежное киберпространство»

7. Полицейская служба Евросоюза называется:

a. Евроохрана

b. Евромир

c. Европол

d. Еврокомиссия

8. Какую поддержку должен оказывать отдел «Проверка сети» странам ЕС ?

a. быстрая проверка связанных с терроризмом или экстремизмом сообщений

b. повышение различных электронных услуг

c. шифрование входящих сообщений

d. принятие пакета электронных границ

Тема 4. Система защиты информации в США.

1. В каких направлениях осуществляется деятельность системы ЗИ в США?

a. контроль за допуском персонала к секретным документам и порядком выезда секретноносителей за границу

b. засекречивание материалов на ведомственном и правительственном уровне

c. сотрудничество с другими странами

d. реформирование структуры, обеспечивающей национальную безопасность

2. Законы, НЕ создающие правовую основу для формирования и проведения единой государственной политики в области информатизации и ЗИ?

a. «О свободе информации»

b. «О ЗИ»

c. «О безопасности компьютерных сетей»

d. «О секретности»

3. Какой закон США устанавливает приоритет национальных интересов при решении вопросов ИБ?

a. «О доступе к информации о деятельности ЦРУ»

b. «О доступе к информации»

c. «О безопасности КС»

d. «Об обеспечении безопасности ЭВМ»

4. В «Разведывательное сообщество» (помимо органов МО) НЕ входит:

a. ФБР Министерства юстиции

b. ЦРУ

c. Управление разведки Министерства энергетики

d. ВМФ США

5. В каком штате находится штаб-квартира ЦРУ?

a. Висконсин

b. Вашингтон

c. Виргиния

d. Южная Каролина

6. Какое управление НЕ входит в состав ЦРУ?

a. разведывательное

b. оперативное

c. административное

d. розыскное

7. Кто руководит Министерством Внутренней безопасности США?

a. Ф. Кальвелли

b. Д. Бреннан

c. Д. Джонсон

d. С. Р. Кейпс

8. В каком году было создано Агентство национальной безопасности США?

a. 1971

b. 1960

c. 1964

d. 1953

9. Кому подчиняется Разведывательное Управление Министерства Обороны (РУМО)?

a. Министерству обороны

b. Государственному департаменту

c. Президенту

d. ЦРУ

Тема 5. Система защиты информации в Великобритании.

1. За расходованием бюджетных средств, управлением и политикой какой спецслужбы НЕ следит Комитет по разведке и безопасности Великобритании

- a. Объединённый центр разведывательных служб (JIC)
- b. Центр правительственной связи Центр правительственной связи (GCHQ);
- c. Секретная разведывательная служба Великобритании (SIS);
- d. Национальная Служба Безопасности Великобритании (MI5)

2. Основная разведывательная служба Великобритании

- a. Лицензия программного Обеспечения (ISC)
- b. Секретная разведывательная служба Великобритании (SIS)
- c. Национальная Служба Безопасности Великобритании (MI5)
- d. Государственный Орган Внешней Разведки (MI6)

3. С разведкой какой страны у Секретной разведывательной службы Великобритании (SIS) нет тесной связи

- a. Новая Зеландия
- b. Исландия
- c. Австрия
- d. Канада

4. Что входит в обязанности Национальной Службы Безопасности Великобритании (MI5)

- a. постановка заданий и подготовка разведывательной продукции
- b. снабжение разведки оперативно-техническими средствами

- c. охрана государственной границы
- d. обеспечение внутренней безопасности

5. Какого департамента НЕТ в структуре Национальной Службы Безопасности Великобритании (MI5)

- a. международный терроризм
- b. оперативная поддержка
- c. Ирландский террор
- d. расследование вербовки граждан

6. Где располагается штаб-квартира Центра правительственной связи (GCHQ)

- a. Челтенхем
- b. Лондон
- c. Ричмонд
- d. Кембридж

7. Кем определяется политика защищенности правительственной секретной информации в Великобритании

- a. Лицензия программного Обеспечения (ISC);
- b. Основы политики безопасности (SPF)
- c. Секретной разведывательной службой Великобритании (SIS)
- d. MPS

8. Какой цифровой код в настоящее время имеет стандарт «Практические правила УИБ»

- a. BS7989
- b. BS7799

c. ISO17900

d. ISO17799

Тема 6. Системы защиты информации во Франции.

1.Какое объединение занимается разработкой стратегии направления политики по обеспечению национальной безопасности

a. Sagem

b. CLUSIF

c.NIOKR

d. Матра (Matra)

2.Что, по мнению французских экспертов, обеспечивает наилучшую ЗИ в сетях

a. методы шифрации

b. технические средства

c. организационные средства

d. программные средства

3.Кто координирует работу спецслужб Министерства Обороны Франции

a. Премьер-министр Франции

b.Генеральный секретариат Министерства юстиции

c. Президент

d. Генеральный секретариат национальной обороны

4.После какой операции была создана бригада разведки и радиоэлектронной борьбы

a. «Буря в пустыне»

b. «Сюртэ милитрэ»

с. «Волновой перехват»

d. «Внешняя угроза»

5. Какие управления входят в состав Управления Военной Разведки (DRM)

a. исследовательское

b. все перечисленное

с. аналитическое

d. техническое

6. В компетенцию Генерального Управления Внешней Безопасности (DGSE) входит

a. проведение тайных операций

b. все вышеперечисленное

с. выявление и предупреждение антифранцузской деятельности за границей

d. добыча и анализ информации, имеющая отношение к безопасности Франции

7. Какое управление НЕ входит в состав Генерального Управления Внешней Безопасности (DGSE)

a. техническое

b. контрразведывательное

с. административное

d. стратегическое

8. Какие станции имеются в оперативном управлении Генерального Управления Внешней Безопасности (DGSE)

a. Безопасности Территорий (DGT)

b. Центральная служба безопасности информационных систем (SCSSI)

c. CPES

d. Управление Военной Разведки (DRM)

Тема 7. Системы защиты информации в Китае.

1.Какая комиссия формирует положение о регулировании деятельности структур подключенных к зарубежным компьютерным сетям

a. Национальная безопасность

b. по делам ИБ

c. по делам информатизации

d. нет верного ответа

2.Основные задачи, которые должны быть решены Китаем в процессе интегрирования в глобальные системы

a. защита государственных границ

b. блокирование доступа к зарубежной

c.организация разведки спецслужб

d. защита от шпионажа

3.За какие виды компьютерных преступлений введена уголовная ответственность в Китае

a. сетевое мошенничество

b. азартные игры в онлайн среде

c. посягательство на авторские и смежные права, преступления против интеллектуальной собственности

d. все перечисленное

4.Кто несет ответственность за обеспечение информационной защиты

a. милиция

b. спецслужба

c. агентство нац.безопасности

d. армия

5.С какой страной МГБ обменялось официально аккредитованными резидентами

a. Германией

b. Италией

c. Россией

d. Францией

6.Как называется проект, именуемый «Великая стена»

a. S219

b. S222

c. S210

d. S200

7.Как называется информационное агентство в составе Министерства Государственной Безопасности (МГБ)

a. Синьхуа

b. Хуэйган

c. Лиюнь

d. Пиньинь

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ПК-2)

1.За что отвечает агентство национальной безопасности (NSA) в США?

2. Что наносит больший ущерб, внутренние угрозы или внешние угрозы? И почему?
3. Что такое «Великая стена» информационной безопасности Китая? Чем она отличается от политики ИБ в России?
4. Для каких целей во Франции создаётся информационно-аналитическая система поддержки принятия решений?
5. Какие факторы оказывают влияние на функционирование ключевых информационных систем общего пользования?
6. Что подразумевается под собой "Концепция сетевых сил" ?
7. Назовите основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны.

Типовые задания для экзамена (ПК-2)

1. Кто впервые в истории реализовал на практике схему дистанционного съема акустической информации...
 - a. Япония+
 - b. Китай
 - c. Англия
 - d. Россия
2. В какой стране до первой мировой войны существовали военные дешифровальные органы...
 - a. Германия
 - b. Австрия
 - c. Россия
 - d. Франция+
3. В каком году в США было создано Центральное Разведывательное Управление (ЦРУ)?
 - a. 1941
 - b. 1947+
 - c. 1945г
 - d. 1955
4. Наиболее распространенный шифр в Древней Греции и Риме:
 - a. Аристотеля
 - b. Светония
 - c. Платона
 - d. Цезаря+
5. Кто первыми открыли и описали методы криптоанализа?
 - a. греки
 - b. индусы
 - c. немцы
 - d. арабы+
6. Какая страна имеет лидерство в сфере разработок в области систем связи и обработки данных?
 - a. Германия
 - b. Англия
 - c. США+
 - d. Россия

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«отлично» (85 - 100 баллов)	ПК-2	Владеет высоким уровнем знаний о принципах теоретического обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия. Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях.
«хорошо» (70 - 84 баллов)	ПК-2	Владеет хорошим уровнем знаний о принципах теоретического обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия. Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях.
«удовлетворительно» (50 - 69 баллов)	ПК-2	Владеет достаточным уровнем знаний о принципах теоретического обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия. Не до конца может администрировать программно-аппаратные средства защиты информации в компьютерных сетях.
«неудовлетворительно» (менее 50 баллов)	ПК-2	Не владеет знаниями о принципах теоретического обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия. Не способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
2. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>
3. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
4. Крутских А.В. Международная информационная безопасность. Теория и практика. В трех томах. Том 2. Сборник документов (на русском языке) : учебное пособие. - Москва: Аспект-Пресс, 2021. - 784 с. - Текст : электронный // ЭБС «Консультант студента вуза и медвуза [сайт]. - URL: <https://www.studentlibrary.ru/book/ISBN9785756710991.html>
5. Международная информационная безопасность, 2021

6.2 Дополнительная литература:

1. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 242 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458012>

6.3 Методические разработки:

1. Петренко В. И. Теоретические основы защиты информации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015. - 222 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

6.4 Иные источники:

1. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>
2. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
3. «Открытые Информационные системы» - <http://www.osp.ru>
4. Журнал «BIS Journal - Информационная безопасность банков» - <https://journal.ib-bank.ru/pub/169>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Yandex браузер

LibreOffice

Kaspersky Endpoint Security 10 для Windows "Лаборатория Касперского" 26.07.2018

Профессиональные базы данных и информационные справочные системы:

1. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>

2. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

3. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>

4. Российская государственная библиотека. – URL: <https://www.rsl.ru>

5. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.