Приложение 5

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

И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.34 Системы защиты информации в мире

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2019

Тамбов, 2021

Авторы программы:
Анурьева Мария Сергеевна
Кандидат педагогических наук, доцент Михайлова Елена Михайловна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «19» декабря 2016 г. № 1612).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «22» декабря 2020 г. Протокол № 4

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «20» января 2021 г. № 1.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОК-2 Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма

ПК-25 Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- научно-исследовательская
  - сбор, изучение, систематизация и обобщение научно-технической информации, отечественного и зарубежного опыта по проблемам информационно-аналитической работы и обеспечения защиты информации
  - анализ прикладных проблем информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, защиты информации и обеспечения безопасности информационных технологий
  - разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок
  - проведение экспериментов по заданным методикам
  - выполнение прикладных научных исследований, подготовка отчетов, докладов

1.3 В результате освоения дисциплины у обучающихся должны быть сформированы следующие компетенции:

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	Знания и умения, необходимые для формирования трудового действия / компетенции
	ОК-2 Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма	Знает и понимает: процесс становления систем защиты информации в мире; состав, основные направления деятельности и особенности функционирования органов защиты информации; тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах
		Умеет (способен продемонстрировать): применять полученные знания в практической работе; использовать зарубежный опыт при разработке комплексной системы защиты информации.
		Владеет: Владеет: сведениями о современном опыте организации систем защиты информации; правовых основах защиты информации.
	ПК-25 Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования	Знает и понимает: практическую значимость нормативно-правовых документов РФ и мира; способы и методики поиска информации в сети Интернет.
		Умеет (способен продемонстрировать): самостоятельно осуществлять поиск научной литературы по исследовательской и прикладной деятельности
		Владеет:

		методиками анализа и систематизации полученной информации в результате поиска; навыком полно и кратко излагать результаты поисков по данной тематике

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОК-2 Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения
		Очная (семестр)
		2
1	История	+

ПК-25 Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		5	6	7	10
1	Основы программирования в корпоративных информационных системах	+	+	+	
2	Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности		+		
3	Преддипломная практика				+

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Системы защиты информации в мире» относится к базовой части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Системы защиты информации в мире» изучается в 5, 6, 7 семестрах.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 15 з.е.

Очная: 15 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	**540**
Контактная работа	236
Лекции (Лекции)	84
Лабораторные (Лаб. раб.)	152
Самостоятельная работа (СР)	268
Экзамен	36
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лекции	Лаб. раб.	СР	
		О	О	О	
5 семестр					
1	История защиты информации в России до XX века	4	4	6	Тестирование
2	Обеспечение национальной безопасности России в информационной сфере 1900-1917 гг.	2	4	8	Тестирование
3	Обеспечение национальной безопасности в информационной сфере в период создания советской власти, в период НЭПа и довоенный период	4	4	10	Тестирование
4	Обеспечение национальной безопасности в информационной сфере в период Великой Отечественной Войны.	2	4	10	Тестирование
5	Система безопасности СССР во второй половине 40-х – первой половине 50-х гг. XX века.	2	6	10	Тестирование

6	Организация защиты государственных секретов и система безопасности во второй половине 50-90 годов.	4	6	10	Тестирование
7	Современная система защиты информации в РФ.	4	6	10	Тестирование
8	Проблемы обеспечения информационной безопасности в России.	4	6	10	Тестирование
9	Лицензирование и сертификация деятельности в области защиты информации.	4	6	10	Тестирование
10	Организационно правовая система борьбы с терроризмом.	4	6	10	Тестирование
6 семестр					
11	Этапы развития и структура системы защиты информации в зарубежных странах.	2	4	6	Тестирование
12	Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке.	2	4	6	Тестирование
13	Состояние проблемы информационной безопасности в странах Евросоюза.	2	4	8	Тестирование
14	Система защиты информации в США.	2	4	8	Тестирование
15	Система защиты информации в Великобритании.	2	4	8	Тестирование

16	Системы защиты информации во Франции.	2	4	8	Тестирование
17	Системы защиты информации в Китае.	2	4	8	Тестирование
18	Цифровой суверенитет.	2	4	8	Тестирование
7 семестр					
19	Кибербезопасность – мир экспертов и преступников.	4	8	14	Тестирование
20	«Куб» кибербезопасности.	4	8	14	Тестирование
21	Угрозы кибербезопасности, уязвимости и атаки.	4	8	14	Тестирование
22	Криптографические методы защиты информации.	4	8	14	Тестирование
23	Обеспечение целостности данных.	4	8	14	Тестирование
24	Концепция «пяти девяток».	4	8	14	Тестирование
25	Защита домена кибербезопасности.	4	10	14	Тестирование
26	Специалисты по кибербезопасности.	6	10	16	Тестирование

Тема 1. История защиты информации в России до XX века (ОК-2)

Лекция.

Защита государственных интересов в XII – XIV вв. Защита государственных интересов в период образования русского централизованного государства. Защита государственных интересов в период сословно-представительной монархии (середина XVI в. – середина XVII в. Защита государственных интересов во второй половине XVII – XVIII вв. Защита государственных интересов в первой половине XIX в. Защита государственных интересов во второй половине XIX в. Основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма

Лабораторные работы.

Особенности организации органов по защиты национальных интересов в информационной сфере.

Задания для самостоятельной работы.

1. В чем заключались функции разрядного приказа как органа, обеспечивающего информационную безопасность государства в 16-17 веках?

2. Проанализируйте основные этапы и закономерности исторического развития России в 18 веке.

3. В чем заключались задачи Сенат в системе ЗИ в Российской империи 18 века?

4. Какие учреждения осуществляли функции по защите информации в 19 веке?

5. Как было организовано секретное делопроизводство в военном министерстве в 19 веке?

6. Что относилось к защищаемым сведениям в области коммерческой тайны в 19 веке?

Тема 2. Обеспечение национальной безопасности России в информационной сфере 1900-1917 гг. (ОК-2)

Лекция.

Введение. Защита военной тайны. Организация контрразведывательной службы. Органы по защите военной тайны. Военная цензура печатных изданий. Организация фельдъегерской связи.

Лабораторные работы.

Влияние деятельности иностранных служб на ход истории России.

Задания для самостоятельной работы.

1. По каким направлениям велась работа по защите военной тайны в начале 20 века?

2.Что выяснилось в области защиты военной тайны по началу первой мировой войны?

3.В какой момент были предприняты меры по коренному улучшению организации контрразведовательной службы и почему (начало 20 века)?

4.Назовите одну из причин бездействия российских спецслужб на сопках Манджурии.

5.Что стало причиной "катастрофы" у Мазурских озер?

6. Осуществите поиск информации, связанной с защитой военной тайны.

Тема 3. Обеспечение национальной безопасности в информационной сфере в период создания советской власти, в период НЭПа и довоенный период (ОК-2)

Лекция.

Создание ВЧК. Задачи по обеспечению безопасности ВЧК (ОГПУ). Комплектование органов и войск ОГПУ. Органы государственной безопасности как информационное ядро по обеспечению информацией высших органов государственной власти. Защита государственных интересов в период НЭПа. Защита государственных интересов в 1928 – 1941 гг. Информационная война и начало Великой отечественной войны. Действия СССР в информационной войне. Поиск, анализ и систематизирование научной информации, отечественного и зарубежного опыта по теме исследования.

Лабораторные работы.

Информационная война в довоенный период.

Задания для самостоятельной работы.

- Записать краткий конспект лекции.
- Изучить базовую и дополнительную литературу по теме лекции.
- Написать эссе.

Тематика вопросов:

1.С какой целью была основана ВЧК?

2.Почему ВЧК была переформирована в ГПУ?

3.Какие задачи выполняла ВЧК?

4.Кем был сменен Ф.Э. Дзержинский и в связи с чем?

5.Были ли у ВЧК особые полномочия, если да, то какие?

6.С какими событиями связан переход ГПУ к ОГПУ?

Тема 4. Обеспечение национальной безопасности в информационной сфере в период Великой Отечественной Войны. (ОК-2)

Лекция.

Народный комиссариат внутренних дел СССР. Состав. Независимые контрразведывательные организации СМЕРШ. Органы разведки в период ВОВ. Криптографические и технические методы защиты информации в военный период. Шифровальная аппаратура.

Лабораторные работы.

Изучение применения алгоритмов криптографической защиты данных в период ВОВ.

Задания для самостоятельной работы.

1.Для чего СССР в 1939 г. у США закупил 100 автобусов "студебеккер"?

2.Какой вклад внесли сотрудники шифровальной службы для достижения победы в Великой Отечественной войне?

3.В связи с чем и в какой степени применение шифратора "Соболь-П" повлияло на исход боя на Курской дуге?

4. Провести анализ деятельности контрразведовательных организаций СМЕРШ.

5.Что было общего у шифровальных устройств "Сова" и "Нева"?

6.Насколько стала развитой шифрослужба к концу войны?

Тема 5. Система безопасности СССР во второй половине 40-х – первой половине 50-х гг. XX века. (ОК-2)

Лекция.

Последствия войны и новые тенденции в развитии общества. Система двублокового противостояния в мире. Германская проблема. Внешняя политика СССР.Три этапа становления государственной безопасности СССР. Внешняя разведка. Военная разведка. Поиск, анализ и систематизирование научной информации, отечественного и зарубежного опыта по теме исследования.

Лабораторные работы.

Организация защиты информации в послевоенный период.

Задания для самостоятельной работы.

1. В чем состоит Главная причина неудач политики коллективной безопасности в послевоенный период?

2. Как называлось шестое управление Министерства государственной безопасности?

3. Что относится к числу весьма важных структурных преобразований органов госбезопасности второго этапа?

4. Основные задачи органов «Смерш»–НКГБ–МГБ непосредственно после завершения войны?

5. Какая задача была поставлена Правительством СССР перед внешней разведкой в первой половине 50х годов?

6. Чем занимались два управление Министерства госбезопасности (ПГУ МГБ)?

7. Сравните исторический опыт отечественных и зарубежных исселований.

1. В чем состоит Главная причина неудач политики коллективной безопасности в послевоенный период?

2. Как называлось шестое управление Министерства государственной безопасности?

3. Что относится к числу весьма важных структурных преобразований органов госбезопасности второго этапа?

4. Основные задачи органов «Смерш»–НКГБ–МГБ непосредственно после завершения войны?

5. Какая задача была поставлена Правительством СССР перед внешней разведкой в первой половине 50х годов?

6. Чем занимались два управление Министерства госбезопасности (ПГУ МГБ)?

7. Сравните исторический опыт отечественных и зарубежных исселований.

Тема 6. Организация защиты государственных секретов и система безопасности во второй половине 50-90 годов. (ПК-25)

Лекция.

Министерство Государственной Безопасности СССР. Структура МГБ. Причины реорганизаций. Комитет государственной безопасности СССР. Структура КГБ СССР. Основные задачи КГБ.

Лабораторные работы.

Изучение российской практики применения алгоритмов криптографической защиты данных на современном этапе.

Задания для самостоятельной работы.

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

Тематика вопросов:

1.В чем заключалось отличие практики МГБ от предшествующих ей структур(НКВД,ВЧК)?

2.С какой целью было создано Центральное бюро по рационализации и изобретательству?

3.Что входило в обязанности 1-го отдела 1-го главного управления МГБ?

4.Опишите основные исторические этапы развития КГБ.

Тема 7. Современная система защиты информации в РФ. (ПК-25)

Лекция.

Органы Федеральной службы безопасности. Органы Федеральной службы охраны. Органы внутренних дел. Совет Безопасности РФ. Внутренние войска Министерства внутренних дел РФ. Служба внешней разведки. Органы пограничной службы. Федеральная служба технического и экспортного контроля. Органы правительственной связи и информации.

Лабораторные работы.

Изучение государственных органов обеспечения информационной безопасности.

Задания для самостоятельной работы.

1. Перечислите основные направления деятельности ФСБ.

2. В каких сферах деятельности ФСБ активно сотрудничает с другими спецслужбами?

3. Объясните причину охраны высших лиц государства в соответствии с положениями Конституции РФ и федеральными законами.

4. Опишите структуру органов государственной охраны

5. Проанализируйте, в чём заключается деятельность ФСО, направленная на обеспечение информационной безопасности РФ

6. Какие ведомства в составе МВД входят в органы внутренних дел и полицию?

7. Какими средствами МВД обеспечивает безопасность дорожного движения?

8. На что направлена деятельность полиции?

9. По какому принципу создаются Межведомственные комиссии?

10. В чём состоит участие Учёного совета в работе Совета Безопасности РФ?

11. Перечислите основные задачи внутренних войск МВД РФ

12. Какова структура внутренних войск МВД РФ?

13. Какова роль внутренних войск МВД РФ в борьбе с терроризмом?

14. Перечислите региональные командования в составе ВВ МВД РФ

15. Какими особыми правами наделяется Государственная фельдъегерская служба для выполнения возложенных на нее задач?

16. Какие полномочия осуществляет ГФС РФ в сфере нормотворчества?

17. Кто может являться владельцем отправлений особой важности, совершенно секретных, секретных и иных служебных отправлений, доставку которых обеспечивает ГФС РФ?

18. Кто осуществляет координацию и руководство деятельностью Службы специальных объектов при Президенте РФ?

19. В интересах каких федеральных органов государственной власти Служба специальных объектов занимается мобилизационной подготовкой?

20. Что подразумевается под обеспечение мобилизационной подготовки органов государственной власти Российской Федерации Службой специальных объектов при Президенте РФ?

21. Какие документы заявитель представляет для получения лицензии в СВР России?

22. Как защищены лица, оказывающие конфиденциальное содействие СВР?

23. Кому предоставляется разведывательная информация?

24. Каковы полномочия Службы внешней разведки?

25. Как финансируется Служба внешней разведки?

26. Каково правовое положение сотрудников СВР?

27. Какие документы, необходимо предъявлять гражданам Российской Федерации при пересечении российско-украинской государственной границы?

28. Какими документами определен порядок нахождения граждан в пограничной зоне?

29. Как стать сотрудником СВР России?

30. Что входит в состав Федеральной пограничной службы РФ?

31. Какова Роль ФСТЭК в современном мире?

32. Кто осуществляет руководство деятельностью ФСТЭК?

33. Осуществите поиск информации по функционированию ФСО?

34. Каково назначение федеральных органов правительственной связи и информации?

35. Что составляет правовую основу деятельности федеральных органов правительственной связи и информации?

Тема 8. Проблемы обеспечения информационной безопасности в России. (ПК-25)

Лекция.

Что такое информационная безопасность: различные подходы к определению. Исторические предпосылки. Регуляторы в области информационной безопасности. Система сертификации по требованиям безопасности.

Лабораторные работы.

Изучение системы отечественных стандартов информационной безопасности.

Задания для самостоятельной работы.

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

- Выполнить практическую работу.

Тематика вопросов:

1. Охарактеризуйте сферу интересов в информационной безопасности для различных категорий должностей организации.

2. Что включает в себя "информационная сфера"?

3. Какие исторические предпосылки способствовали формированию современной системы защиты информации в России?

4. Перечислите сферу компетенций различных регуляторов в области информационной безопасности. В чем их компетенции пересекаются?

5. Опишите систему сертификации средств защиты информации в России. В чем отличие отечественной системы сертификации от международной?

Тема 9. Лицензирование и сертификация деятельности в области защиты информации. (ПК-25)

Лекция.

Лицензирование в области защиты информации. Аттестация объектов информатизации. Сертификация. Классификация средств защиты. Деятельность органов ФСБ РФ и ФСТЭК РФ в сертификации и лицензировании в области защиты информации. Реестр сертифицированных средств.

Лабораторные работы.

Анализ развития отечественных технических средств защиты информации.

Задания для самостоятельной работы.

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

Тематика вопросов:

1. Что составляет организационную структуру системы государственного лицензирования?

2. Перечислите общие нормы, устанавливающие порядок допуска организаций к проведению работ с информацией, составляющей государственную тайну.

3. Охарактеризуйте сферу компетенций органов, уполномоченных на ведение лицензионной деятельности.

4. Какие виды деятельности по защите информации подлежат лицензированию?

5. Что может послужить основанием для отказа в выдаче лицензии?

6. Чем лицензирование отличается от сертификации?

7. Что такое класс безопасности? Какие классы вы знаете?

Тема 10. Организационно правовая система борьбы с терроризмом. (ПК-25)

Лекция.

Правовая система борьбы с терроризмом. Обнаружение причин борьбы с терроризмом. Терминологическая база: терроризм, террорист, террористическая группа, террористическая организация, террористическая деятельность. Международная террористическая деятельность. Структурная схема взаимодействия субъектов, осуществляющих борьбу с терроризмом. Федеральная антитеррористическая комиссия. Основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма.

Лабораторные работы.

Изучение информационно-психологической войны и типов информационного оружия.

Задания для самостоятельной работы.

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

Выполнить практическую работу.

1. Чем террористическая группа отличается от террористической организации?

2. Что относят к террористической деятельности?

3. Какие органы государственной власти занимаются борьбой с терроризмом? Охарактеризуйте их компетенции в данной сфере.

4. Какие права имеют лица, в зоне проведения контртеррористической операции, проводящие эту операцию?

Тема 11. Этапы развития и структура системы защиты информации в зарубежных странах. (ПК-25)

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 12. Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке. (ПК-25)

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 13. Состояние проблемы информационной безопасности в странах Евросоюза. (ПК-25)

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 GoodPracticeGuideon 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 14. Система защиты информации в США. (ПК-25)

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 15. Система защиты информации в Великобритании. (ПК-25)

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 16. Системы защиты информации во Франции. (ПК-25)

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 17. Системы защиты информации в Китае. (ПК-25)

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 правовойсистемы ИБ Китая?

10. Каковы основные мероприятия по обеспечению ИБ Китая, осуществляемые в процессе интеграции в глобальную сеть Интернет?

Тема 18. Цифровой суверенитет. (ПК-25)

Лекция.

Эпоха слома суверенитета. Электронный суверенитет. Кибервойна. Информационный суверенитет. Разработка независимого интернет-доступа.

Лабораторные работы.

Сравнительная характеристика систем защиты информации в ведущих зарубежных странах.

Задания для самостоятельной работы.

1. Что включает в себя "электронный щит" государства?

2. Возможно ли наличие у России "электронного щита"?

3. Что включает в себя "информационный щит" государства?

4. Обладает ли Россия в настоящее время "информационным щитом"?

5. Какая страна в наибольшей степени обладает "электронным" и "информационным" щитом?

Тема 19. Кибербезопасность – мир экспертов и преступников. (ПК-25)

Лекция.

Мир кибербезопасности. Домены кибербезопасности. Кибербезопасность: злоумышленники и специалисты. Изучение общих угроз. Угрозы интернет-услугам. Угрозы ключевым отраслям промышленности. Распространение угроз кибербезопаснтси: пути распространения и уровень сложности угроз. Дополнительная поддержка безопасности: интернет-сообщества и международная сертификация. Основные этапы и закономерности исторического развития России, её место и роль в современном мире в целях формирования гражданской позиции и развития патриотизма

Лабораторные работы.

Определение кибермошенничества. Кибербезопасность. Идентификация угрозы. Определение специализации по информационной безопасности NISP/NICE.

Задания для самостоятельной работы.

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

2. Что наносит больший ущерб, внутренние угрозы или внешние угрозы? И почему?

3.Что используют любители или квалифицированные злоумышленники при внешних угрозах?

4. Что в себя включают корпоративные данные?

5. Что создает растущую угрозу для организаций, которые позволяют мобильным устройствам сотрудников подключаться к своим сетям?

6.Что такое Internet of Things (IoT) ?

7. Большие данные представляют собой как вызовы, так и возможности, основанные на трех измерениях, на каких?

8.Что такое передовая постоянная угроза (APT) и для чего преступники обычно выбирают APT?

9.Что могут отслеживать атаки алгоритма? Приведите пример.

10. Рамка рабочей силы классифицирует работу по кибербезопасности на семь категорий . На какие?

Тема 20. «Куб» кибербезопасности. (ОК-2)

Лекция.

Три измерения куба кибербезопасности: целостность (принцип целостности данных, потребности в целостности, проверка целостности), конфиденциальность (принцип конфиденциальности, защита конфиденциальных данных, управление доступов, международное законодательство) и доступность (принцип доступности,обеспечение доступности). Данные и обеспечение безопасности: типы хранилищ данных, методы передачи данных, проблемы защиты хранимых данных In-Transit, формы обработки и вычисления данных, определение состояния данных.Контрмеры по кибербезопасности. Технологии: программные гарантии безопасности, аппаратные средства защиты, сетевые технологии, облачные технологии. Создание культуры осведомленности о кибербезопасности. Политики и процедуры кибербезопасности: стандарты, методические рекомендации, процедуры.Определение категории противодействия.Система управления ИТ: модель кибербезопасности ISO.

Лабораторные работы.

Анализ принципов ИБ. Определение принципов ИБ. Определение состояния данных. Установка виртуальной машины на ПК. Изучение аутентификации, авторизации и учета. Изучение шифрования файлов и данных. Проверка целостности файлов и данных.

Задания для самостоятельной работы.

1.Что такое киберпространство?

2. Какие три возможных состояния имеют данные?

3.Чему препятствует конфиденциальность?

4.Какие существуют три типа конфиденциальной информации?

5.Что такое целостность и какие методы используются для обеспечения целостности данных?

6.Что существуют общие хеш-функции?

7.Что такое доступность данных?

8.Какие три принципа проектирования обычно включают системы высокой доступности?

9.Какие действия выполняет организация для обеспечения доступности?

10.Что такое DAS и NAS?

Тема 21. Угрозы кибербезопасности, уязвимости и атаки. (ПК-25)

Лекция.

Вредоносные программы и вредоносный код. Типы вредоносных программ: вирусы, черви, троянские кони, логические бомбы, вымогатели, бэкводы и руткиты. Защита от вредоносных программ. Атаки электронной посты и браузера: спам, spyware, adware, scareware, фишинг. Плагины браузера. Защита от атак электронной посты и браузера. Мошенничество: дайвинг, пиггирование и другие методы. Защита от мошенничества. Кибератаки: типы кибератак (отказ в обслуживании, подделки, "человек посередине", атаки с нулевым дном, ведение журнала клавиатуры). Защита от атак. Обнаружение угроз и уязвимости. Атаки и защита беспроводных и мобильных утсройств. Настройка WEP/WPA2 Psk/ WPA2 RAdius. Прикладные атаки: межсайтовый скриптинг, ввод кода, переполнение буфера, удаленное исполнение кода, элементы управления ActiveX и Java. Защита от атак приложений.

Лабораторные работы.

Определение типов вредоносного кода. Определение атак электронной почты и браузера. Определение проблем социальной инженерии. Определение кибер-атак. Определение типов приложений и атак.

Задания для самостоятельной работы.

1.Что такое кибератака?

2. Что такое вредоносное ПО?

3. Назовите три способа распространения компьютерных вирусов.

4.Что нужно сделать, чтобы защитить себя от вредоносных программ?

5. Какие цели преследует спам?

6.Что такое Spyware?

7. Чем отличается обычный фишинг от фишинг-копья?

8. Для чего предназначено отравление SEO?

9. Назовите способы устранения спама.

10.Назовите способы пиггирования (Piggybacking)

Тема 22. Криптографические методы защиты информации. (ОК-2)

Лекция.

История криптографии. Создание зашифрованного текста. Изучение шифра Виженера. Два типа шифрования: шифрование с закрытым ключом (процесс симметричного шифрования, типы, алгоритмы), шифрование с открытым ключом (ассиметричный процесс шифрования, алгоритмы). Ключевой менеджмент. Сравнение типов шифрования. Контроль доступа: типы контроля, стратегии, идентификация, методы проверки подлинности, авторизация, подотчетность, типы средства контроля безопасности. Сокрытие данные: маскирование, стеганография, обфускация.

Лабораторные работы.

Использование симметричного шифрования. Использование ассиметричного шифрования

Сравнение симметричного и ассиметричного шифрования. Определение стратегий контроля доступа. Определение методов проверки подлинности. Сравнение типов элементов управления безопасностью.

Задания для самостоятельной работы.

1.Что такое криптография?

2.Перечислите способы создания зашифрованного текста и их краткое описание.

3.Назовите и опишите два типа алгоритмов шифрования.

4.Что такое контроль физического доступа? Назовите его цель.

5. Назовите и опишите несколько средств контроля доступа.

6. Перечислите виды контроля доступа.

7. Опишите принцип работы идентификации.

8. Назовите и опишите два типа биометрических идентификаторов.

9. Что такое авторизация?

10. Что такое подотчётность?

Тема 23. Обеспечение целостности данных. (ОК-2)

Лекция.

Обеспечение целостности данных. Типы элементов управления целостностью. Цифровые подписи, сравнение алгоритмов цифровой подписи. Использование цифровых подписей. Сертификаты: создание цифрового сертификата, процесс проверки, путь сертификата. Обеспечение соблюдения целостности базы данных: проверка и требования к целостности БД. Поиск, анализ и систематизирование научной информации, отечественного и зарубежного опыта по теме исследования.

Лабораторные работы.

Определение терминологии. Cracking (взлом) паролей. Использование цифровых подписей.

Работа с цифровыми сертификатами. Организация удаленного доступа.

Задания для самостоятельной работы.

1. Что такое хеширование?

2. Перечислите свойства криптографической хэш-функции.

3. Что использует атака словаря?

4. Что такое таблица поиска?

5. Что помогает установить цифровая подпись?

6. Что такое PKI?

7. Сертификат принадлежит цепочке сертификатов, называемой … .
8. Перечислите четыре правила или ограничения целостности данных.
9. Перечислите критерии, используемые в правиле проверки.
10. Что гарантирует целостность домена?

Тема 24. Концепция «пяти девяток». (ОК-2)

Лекция.

Что такое "пять девяток"? Среды, требующие "пять девяток". Угрозу доступности. Проектирование системы высокой доступностью. Меры по улучшению доступности. Управление активами: идентификация активов, классификация активов, стандартизация активов, идентификация угроз, анализ риска. Избыточность. Системная устойчивость. Расследование инцидентов: фазы реагирования на инцидент (подготовка, обнаружение, анализ, восстановление). Технологии реагирования на инцидент: контроль доступа в сеть, системы обнаружения вторжений, системы предотвращения вторжений.аварийное восстановление: планирование восстановлений после стихийных бедствий, планирование непрерывности бизнеса.

Лабораторные работы.

Проведение анализа риска активов. Определение уровня защиты. Анализ фаз реагирования на инцидент.

Задания для самостоятельной работы.

1. Что означает пять девяток?
2. Что необходимо чтобы обеспечить высокую доступность?
3. Какие среды, требуют пять девяток.
4. Перечислите три основных принципа, которые включает в себя высокая доступность для достижения цели непрерывного доступа к данным и услугам.
5. Перечислите категории идентификации активов.
6. Что включает в себя идентификатор CVE?
7. Что такое анализ рисков?
8. Какие четыре общих способа снижения риска существуют?
9. Что делает резервный массив независимых дисков (RAID)?
10. Что является основной функцией Spanning Tree Protocol (STP)?

Тема 25. Защита домена кибербезопасности. (ПК-25)

Лекция.

Защитные системы и устройства: укрепление (безопасность ОС, управление патчами, брандмауэры, безопасная связь). Безопасность беспроводных и мобильных устройств: WEP, WPA/WPA2, взаимная аутентификация. Защита данных хоста: контроль доступа к файлам, шифрование файлов, резервное копирование системы и данных. Управление изображениями и контентом: скрининг и блокировка контен. Физическая защита рабочих станций. Безопасность серверов: безопасный удаленный доступ, административные меры, физическая защита серверов. Безопасность сети: защита сетевыхустрйост, голосовое и видеооборудование. Физическая охрана: контроль доступа и видеонаблюдение.

Лабораторные работы.

Безопасность системы Linux. Защитные системы и устройства. Серверные брандмауэры и маршрутизаторы ACL.

Задания для самостоятельной работы.

1. Что такое Microsoft Baseline Security Analyzer (MBSA)? Перечислите ее основные функции.
2. Назовите разновидности антивирусных программ. Охарактеризуйте их.
3. Перечислите преимущества использования службы автоматического обновления.
4. Назовите стандарты безопасности Wi-Fi. Какой из них наиболее эффективен?
5. Что такое контроль доступа к файлам? Назовите разрешения, доступные для файлов и папок.
6. Что такое шифрование данных? Как оно работает?
7. Назовите общие правила построения эффективных систем электроснабжения.

8. Что такое брандмауэр?
9. Что такое Voice over IP (VoIP)? Назовите устройства, необходимые для VoIP.
10. Назовите физические методы охраны предприятия.

Тема 26. Специалисты по кибербезопасности. (ПК-25)

Лекция.

Домены кибербезопасности: пользовательский домен (общие угрозы пользователей и уязвимости, управление угрозами пользователей), домен устройства (общие угрозы устройства, управление угрозами устройства), домен локальной сети (общие угрозы и управление угрозами), частный облачный домен (общие угрозы и управление угрозами), общественный облачный домен (общие угрозы и управление угрозами), домен для физических лиц (общие угрозы и управление угрозами), домен приложений (общие угрозы и управление угрозами).. Этика работы в ИБ: руководящие принципы, законы и ответственность, информационные сайты).

Лабораторные работы.

Соответствующие области кибербезопасности. Использование соответствующего инструмента ЗИ. Интеграция навыков.

Задания для самостоятельной работы.

1. Перечислите общие угрозы пользователей, обнаруженные во многих организациях.
2. Перечислите угрозы для физических установок в организации.
3. Перечислите угрозы для приложений.
4. Какие меры могут внедрять организации для защиты приложений от различных угроз.
5. Что такое этика специалиста по кибербезопасности?
6. Назовите этические системы, которые рассматривают этику с разных точек зрения.
7. Назовите десять заповедей компьютерной этики.
8. Конвенция о киберпреступности. Какие страны подписали этот договор? Назовите общую политику договора.
9. Что такое CERT. Какие услуги они предоставляют?
10. Существует ли дистрибутив безопасности на основе linux? Если да, то какое его название?

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

5 семестр

- посещаемость – 10 баллов
- текущий контроль – 72 балла
- контрольные срезы – 2 среза по 9 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Max. кол-во баллов	Методика проведения занятия и оценки
1.	История защиты информации в России до XX века	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

2.	Обеспечение национальной безопасности России в информационной сфере 1900-1917 гг.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
3.	Обеспечение национальной безопасности в информационной сфере в период создания советской власти, в период НЭПа и довоенный период	**Тестирование(контрольный срез)**	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
4.	Обеспечение национальной безопасности в информационной сфере в период Великой Отечественной Войны.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
5.	Система безопасности СССР во второй половине 40-х – первой половине 50-х гг. XX века.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
6.	Организация защиты государственных секретов и система безопасности во второй половине 50-90 годов.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
7.	Современная система защиты информации в РФ.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

8.	Проблемы обеспечения информационной безопасности в России.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
9.	Лицензирование и сертификация деятельности в области защиты информации.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
10.	Организационно правовая система борьбы с терроризмом.	**Тестирование(контрольный срез)**	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
11.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7 баллов – посещаемость студента составляет не менее 80 % занятий 5 баллов– посещаемость студента составляет не менее 50 % занятий 1 балл – посещаемость студента составляет не менее 25 % занятий
12.	Премиальные баллы		20	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 дисциплине – 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
13.	Итого за семестр		100	

6 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Max. кол-во баллов	Методика проведения занятия и оценки
1.	Этапы развития и структура системы защиты информации в зарубежных странах.	Тестирование	11	Тест состоит из вопросов с выбором ответа. 10-11 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	Становление и развитие систем защиты информации в ведущих зарубежных странах. Защита информации в XX веке.	**Тестирование(контрольный срез)**	10	Тест состоит из вопросов с выбором ответа. 10- баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
3.	Состояние проблемы информационной безопасности в странах Евросоюза.	Тестирование	11	Тест состоит из вопросов с выбором ответа. 10-11 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
4.	Система защиты информации в США.	Тестирование	12	Тест состоит из вопросов с выбором ответа. 10-12 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
5.	Система защиты информации в Великобритании.	Тестирование	12	Тест состоит из вопросов с выбором ответа. 10-12 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
6.	Системы защиты информации во Франции.	Тестирование	12	Тест состоит из вопросов с выбором ответа. 10-12 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

7.	Системы защиты информации в Китае.	Тестирование	12	Тест состоит из вопросов с выбором ответа. 10-12 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
8.	Цифровой суверенитет.	**Тестирование(контрольный срез)**	10	Тест состоит из вопросов с выбором ответа. 10 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
9.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7 баллов – посещаемость студента составляет не менее 80 % занятий 5 баллов– посещаемость студента составляет не менее 50 % занятий 1 балл – посещаемость студента составляет не менее 25 % занятий
10.	Премиальные баллы		20	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 дисциплине – 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
11.	Итого за семестр		100	

7 семестр

- посещаемость – 10 баллов
- текущий контроль – 44 балла
- контрольные срезы – 2 среза: 7 баллов, 9 баллов
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Max. кол-во баллов	Методика проведения занятия и оценки

1.	Кибербезопасность – мир экспертов и преступников.	Тестирование	7	Тест состоит из вопросов с выбором ответа. 6-7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-5 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	«Куб» кибербезопасности.	Тестирование	7	Тест состоит из вопросов с выбором ответа. 6-7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-5 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
3.	Угрозы кибербезопасности, уязвимости и атаки.	Тестирование	7	Тест состоит из вопросов с выбором ответа. 6-7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-5 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
4.	Криптографические методы защиты информации.	Тестирование	7	Тест состоит из вопросов с выбором ответа. 6-7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-5 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
5.	Обеспечение целостности данных.	Тестирование	7	Тест состоит из вопросов с выбором ответа. 6-7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-5 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
6.	Концепция «пяти девяток».	**Тестирование(контрольный срез)**	7	Тест состоит из вопросов с выбором ответа. 6-7 баллов - студент правильно отвечает более чем на 90% вопросов. 4-5 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
7.	Защита домена кибербезопасности.	Тестирование	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

8.	Специалисты по кибербезопасности.	**Тестирование(контрольный срез)**	9	Тест состоит из вопросов с выбором ответа. 9 баллов - студент правильно отвечает более чем на 90% вопросов. 7-8 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
9.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7 баллов – посещаемость студента составляет не менее 80 % занятий 5 баллов– посещаемость студента составляет не менее 50 % занятий 1 балл – посещаемость студента составляет не менее 25 % занятий
10.	Премиальные баллы		20	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 дисциплине – 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

11.	Ответ на экзамене	30	Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок; Оценка «хорошо» – ▪достаточно полные и систематизированные знания по дисциплине;▪ умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций. - Оценка «отлично» – систематизированные и гл и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.
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. История защиты информации в России до XX века

1.Как назывался общегосударственный кодекс в конце XV века?

a. нет верного ответа
b. судебник +
c. летопись
d. Конституция

2.Как называлось зашифрованное сообщение в 16 веке?
a. все перечисленное
b. грамота
c. затейное письмо +
d. зашифрованное письмо

3.Какой приказ выполнял разведывательные функции?
a. пушкарский
b. бронный
c. стрелецкий
d. посольский +

4.Высший орган власти в государственной системе управления и безопасности Великого Новгорода:
a. боярский совет
b. совет при князе
c. вече +
d. церковь

5.Какой(-ие) шифр(-ы) существовал(-и) в середине 18 века?
a. стенографический
b. универсальный
c. генеральный и индивидуальный +
d. транспозиционный

6.Для обозначения статей секретности в 19 веке применялись грифы...
a. конфиденциально
b. секретно и особой важности
c. секретно и весьма секретно +
d. секретно, весьма секретно и особой важности

7.Незаконное издание сочинений называлось...
a. цензура
b. контрафакция+
c. эмиссия
d. сочинительство

8.Какая функция защиты информации НЕ осуществлялась военно-ученым отделением в структуре ГУГШ...
a. разработка инструкций по вопросу деятельности министерства
b. предупреждение несанкционированного доступа к данным +
c. ведение секретного делопроизводства
d. управление военными агентами

9.В 19 веке в криптографических службах шифры классифицировались...

a. по отраслевому назначению
b. по степени секретности
c. все выше перечисленное+
d. по языковому принципу

Тема 2. Обеспечение национальной безопасности России в информационной сфере 1900-1917 гг.

1.Какой офицер занимался вопросами контрразведки в Петербурге в период первой мировой войны...
a. Р.Зорге
b. Р.Ханссен
c. М.Д.Бонч-Бруевич+
d. Л.П.Берия

2.В каком году канцелярия Военно-ученого комитета Генерального штаба Военного министерства подготовила секретный шестистраничный проект организации контрразведывательной службы в военном ведомстве...
a. 1917
b. 1903+
c. 1937
d. 1913

3.Кому подчинялись пограничная и таможенная стража...
a. МВД
b. контрольному бюро
c. военному ведомству
d. министерству финансов+

4.Какие вопросы регламентировал спецотдел VIII архивно-исторического отделения...
a. выдача документов
b. работы с секретными документами +
c. криптование переписки
d. организация секретной переписки

5.Кто впервые в истории реализовал на практике схему дистанционного съема акустической информации...
a. Япония+
b. Китай
c. Англия
d. Россия

6.Какими вопросами занимался восьмой стол VII отделения ведения военной статистики иностранных государств Второго Управления Генерал-Квартирмейстера...
a. ведение переписки по агентурной разведке
b. обеспечение работы прикомандированных иностранных офицеров к русской армии
c. все вышеперечисленное+
d. ведение переписки по секретным вопросам

7.В какой стране до первой мировой войны существовали военные дешифровальные органы...
a. Германия
b. Австрия

c. Россия
d. Франция+

8.Местом хранения мобилизационных планов согласно 1 типовой инструкции «Пункты хранения» являлись...
a. все вышеперечисленное+
b. карцер при гауптвахте
c. денежная кладовая гарнизонной гауптвахты
d. мобилизационный отдел штаба округа

Тема 3. Обеспечение национальной безопасности в информационной сфере в период создания советской власти, в период НЭПа и довоенный период

1.Как называлась спецслужба, основное назначение которой была борьба с контрреволюцией и саботажем с 1917-1921 г.г.
a.Народный Комиссариат Внутренних Дел (НКВД)
b. Объединенное государственное политическое управление (ОГПУ)
c. Всероссийская чрезвычайная комиссия (ВЧК)+
d. Государственное политическое управление (ГПУ)

2.Право применения внесудебных репрессий было дано по отношению к…
a. все вышеперечисленное+
b. к чекистам, совершивших должностное преступление
c. участникам вооруженных ограблений
d. уголовникам-рецидивистам, захваченных с оружием в руках

3.В каком году упразднили Всероссийская Чрезвычайная Комиссия (ВЧК)
a. 1922г+
b. 1924г
c. 1923г
d. 1921г

4.Кем назначались председатель Объединённого государственного политического управления и его заместители ..
a. лично В.И. Лениным
b. коллегией Государственного политического управления (ГПУ)
c. Советом народных комиссаров СССР;
d. Президиумом ЦИК СССР+

5.Первой акцией Всероссийская Чрезвычайная Комиссия (ВЧК) в Петрограде стало ..
a. расследование деятельности Центрального стачечного комитета+
b. расследование в профсоюзах
c. применение мер к пресечению подрывных акций
d. нет верного ответа

6.Рабочим(-и) органом (-ами) Ставки Верховного Главнокомандования являлся(-ись)..
a.все вышеперечисленное +
b. Управление наркоматов обороны
c. Генеральный штаб
d. ВМФ

7.Кто подписал руководящие указания начальника штаба верховного главнокомандования по маскировке подготовки агрессии..
a. Гитлер
b.Ленин
c. Кейтель +
d. Ведель

8.Кто был первым руководителем ЧК(ВЧК) СССР?
a. Ф.Э.Дзержинский+
b. Л.П.Берия
c. В.Р.Менжинский
d. М.Я.Ляпис

9.Как называлась главная геополитическая доктрина?
a.Рюриковичи
b. Москва-Третий Рим+
c. Москва
d. ГКО

10.Кто был главой НКВД с 1938 г.?
a. Л.П.Берия+
b. Ф.Э.Дзержинский
c. В.Р.Менжинский
d. М.Я.Ляпис

Тема 4. Обеспечение национальной безопасности в информационной сфере в период Великой Отечественной Войны.

1.Центральный орган государственного управления СССР по борьбе с преступностью в 1934-1946г.г. – это
a. Главное Управление Государственной Безопасности (ГУГБ)
b. Особое Конструкторское Бюро (ОКБ)
c. Комитет Государственной Безопасности (КГБ)
d. Народный Комиссариат Внутренних Дел (НКВД)+

2.В сфере ответственности Народный Комиссариат Внутренних Дел (НКВД) находились ...
a. выдача паспортов
b. личная безопасность граждан
c. экономическая деятельность страны
d. право вынесения приговоров во внесудебном порядке+

3.Задачей пограничных войск Народный Комиссариат Внутренних Дел (НКВД) было ...
a. борьба с диверсантами
b. все выше перечисленное+
c. выявление нарушений пограничного режима
d. охрана государственной границы

4.СМЕРШ это ...
a. название секретного документа

b. название ряда независимых друг от друга контрразведывательных организаций+
c. кодовое название операции
d. устройство для засекречивания телефонных переговоров

5.К задачам СМЕРШа НЕ относилось
a. борьба с дезертирством на фронтах
b. выполнение специальных заданий народного комиссариата обороны
c. проверка военнослужащих, бывших в плену и окружении противника
d. конвоирование военнопленных +

6.Первые разработки аппаратов секретного телефонирования в СССР относились к ...
a. 1930-1931гг
b. 1929-1930гг
c. 1927-1928гг+
d. 1928-1929гг

7.Как называлось устройство автоматического засекречивания телефонных переговоров?
a. НИИС
b. РККА
c. инвертор ЕС +
d. СМЭРШ

8.Кто руководил группой по созданию аппаратуры шифрования и оценкой стойкости аппаратуры засекречивания речевого сигнала?
a. В.И.Бекаури
b. В.А.Котельников
c. А.П.Петерсон+
d. Миткевич

Тема 5. Система безопасности СССР во второй половине 40-х – первой половине 50-х гг. XX века.
1.Органы СМЕРШ-Народный Комиссариат Государственной Безопасности(НКГБ)-Министерство Государственной Безопасности(МГБ)-МВД находились под контролем
a. Сталина
b. Ленина
c. Берии
d. Сталина и куратора ЦК+

2.Какие международные организации возникли благодаря участию СССР в послевоенные годы
a. международная демократическая федерация женщин (МДФЖ)
b. все вышеперечисленное+
c. всемирный конгресса мира
d. всемирная федерации демократической молодежи (ВФДМ)

3.Как называется совместно созданное в 1947 году информационное бюро со штаб-квартирой в городе Белграде
a. коминформ+
b. коминтерн

c.комитет Государственной Безопасности (КГБ)
d. народный Комиссариат Внутренних Дел (НКВД)

4.Во что, в марте 1946г., был преобразован Совнарком СССР?
a. верховный Совет
b. совет Министров+
c. федеральное Собрание
d. государственную Думу

5.Какие органы в октябре 1949г были переданы в Министерство государственной безопасности?
a. нет верного ответа
b. органы дознания
c. органы милиции и пограничные войска +
d. таможенная служба

6.Какая новая категория агентуры была введена в январе 1952г?
a. агенты
b. резиденты
c. контрагенты
d. спецагенты+

7.В каком году в США было создано Центральное Разведывательное Управление (ЦРУ)?
a. 1941
b. 1947+
c. 1945г
d. 1955

8.С целью предотвращения ракетно-ядерного удара по СССР в Вооруженных Силах СССР в 1951г были созданы:
a. все выше перечисленное
b. дешифровальное управление
c. штатные взводы радистов
d. штатные диверсионно-разведывательные формирования в составе армий+

Тема 6. Организация защиты государственных секретов и система безопасности во второй половине 50-90 годов.

1.В каком году при Министерстве Государственной Безопасности(МГБ) было создано Центральное бюро по рационализации и изобретательству
a. 1941г
b. 1945г
c. 1953г+
d. 1975г

2.Какого отдела в структуре Министерстве Государственной Безопасности (МГБ) на конец 1946 г. НЕ было
a. отдел «П»+
b. отдел «К»
c. отдел «А»
d. отдел «Р»

3.Кто был назначен председателем Комитета Государственной Безопасности (КГБ)
a. И.В.Сталин
b. И.А.Серов +
c. С.Н.Круглов
d. М.Д.Рюмин

4.Чем занимается отдел «К» в структуре Министерстве Государственной Безопасности (МГБ)
a. контрразведывательным обеспечением объектов атомной промышленности+
b. радиоконтрразведкой
c. борьбой с терроризмом
d. контрразведкой

5.Функция(-ии), возложенные на самостоятельное 5 управление в центральном аппарате Комитета Государственной Безопасности (КГБ)
Выберите один ответ:
a.организации работы по выявлению и изучению процессов, могущих быть использованными противником в целях идеологической диверсии
b.разработки в контакте с разведкой идеологических центров противника, антисоветских эмигрантских и националистических организаций за рубежом
c. всё вышеперечисленное +
d.выявления и пресечения враждебной деятельности антисоветских, националистических и церковно-сектантских элементов, а также предотвращения (совместно с органами МООП) массовых беспорядков

6.Говоря о приоритетах, основных направлениях и принципах перестройки в работе органов государственной безопасности В.А.Крючков определил их как
a. Закон, Гласность и Порядок
b. Закон, Правда и Гласность+
c. Закон и Гласность
d. Правда и Гласность

7.Кто был заместителем председателем Комитета Государственной Безопасности (КГБ)
a. Ф.Д.Бобков
b. А.Ф.Кадышев
c. Е.Ф.Иванов
d. М.И.Ермаков+

8.Основные задачи Комитета Государственной Безопасности (КГБ) при Союзе Министров СССР в 1954г
a. охрана руководителей партии и государства
b. организация шифрования и дешифрования дела
c. контрразведывательная работа в Советской Армии и Военно-морском флоте
d. все вышеперечисленное+

Тема 7. Современная система защиты информации в РФ.

1.Спецслужба, федеральный орган исполнительной власти РФ, осуществляющая в пределах своих полномочий решение задач по контрразведке
a. Совет безопасности РФ

b. Органы внутренних дел
c. Федеральная служба безопасности (ФСБ)+
d. Федеральная служба охраны (ФСО)

2.Что входит в органы Федеральной Службы Безопасности (ФСБ) РФ?
a. Управление ФСБ РФ по отдельным регионам и субъектам РФ
b. Федеральная служба безопасности РФ
c.Все вышеперечисленное+
d. Управление ФСБ РФ в Вооруженных Силах РФ, войсках и иных воинских формированиях

3.Цель сотрудничества Федеральной Службы Безопасности (ФСБ) РФ с Министерством Внутренних Дел (МВД), пограничной и таможенной службами, Федеральной Службы Контроля за Наркотиками (ФСКН)
a.все вышеперечисленное+
b. с незаконной миграцией
c. борьба с контрабандой и незаконным оборотом наркотиков
d. борьба с террористическими организациями

4.Кто возглавлял Службу безопасности Президента РФ в 1993-1996гг?
a.В.Г.Кулишов
b. Е.А.Муров
c. А.В.Коржаков+
d. С.М.Смирнов

5.В службу коменданта Московского Кремля входит?
a. гараж особого назначения
b. почетный кавалерийский эскорт +
c. служба охраны

6.Министерство внутренних дел было образовано?
a. 1992г+
b. 1991г
c. 1994г
d. 1995г
d. нет верного ответа

7.В единую централизованную систему органов Внутренних Дел РФ НЕ входят?
a. организации и подразделения, созданные для выполнения задач и осуществления полномочий, возложенных на МВД РФ
b. органы дознания +
c. органы Внутренних Дел(включая полицию
d. внутренние войска

8.Ведомство, составная часть МВД РФ, деятельность которого направлена на защиту жизни ?
a. ГИБДД
b. Совет безопасности
c. Внутренние войска
d. Полиция+

9.Главнокомандующий внутренними войсками Министерства Внутренних дел?

a. В.В.Путин

b. В.В.Золотов +

c. В.В.Тихонов

10.Постоянно действующие специальные органы, предназначенные для непосредственного управления объединенными силами и средствами, выделенными для пресечения диверсионно-террористических акций, а также ликвидации их последствий

a. ОГВ

b. ФСБ

c. Группа Оперативного Управления (ГрОУ);+

d. МВД

11.В каких горных районах действуют военные комендатуры Министерства Обороны РФ?

a. нет верного ответа

b. Кавказском

c. Уральском

d. Веденском и Шатайском+

12.В каком году создана Государственная Фельдъегерская Служба (ГФС)?

a. 1896г

b. 1696г

c. 1996г

d. 1796г+

13.Основной (-ыми) задачей (-ами) Государственной Фельдъегерской Службы (ГФС) РФ является

a. все перечисленное+

b. Управление территориальными органами ГФС России и обеспечивающими деятельность ГФС России организациями, созданными для решения возложенных на ГФС России задач

c.обеспечение оперативной доставки и гарантированной сохранности отправлений особой важности, совершенно секретных, секретных и иных служебных отправлений;

d. доставка корреспонденции глав зарубежных государств и глав правительств зарубежных государств, органов государственной власти государств-участников Соглашения о Межправительственной фельдъегерской связи;

14.Какие полномочия НЕ осуществляет ГФС РФ в сфере нормотворчества?

a.участвует в установленном порядке в подготовке и заключении международных договоров Российской Федерации, в том числе межведомственного характера, по вопросам, относящимся к установленной сфере деятельности; участвует в установленном порядке в подготовке и заключении международных договоров Российской Федерации, в том числе межведомственного характера, по вопросам, относящимся к установленной сфере деятельности;

b. нет верного ответа+

c.на основании и во исполнение Конституции РФ, федеральных конституционных законов, федеральных законов, актов Президента РФ и Правительства РФ самостоятельно принимает нормативные правовые акты по вопросам, относящимся к установленной сфере деятельности;

d.разрабатывает и представляет в установленном порядке Президенту РФ и в Правительство РФ проекты федеральных законов, актов Президента РФ и Правительства РФ, а также другие документы, по которым требуется решение Президента РФ и Правительства РФ, по вопросам, относящимся к установленной сфере деятельности;

15.В ведении какой службы находится Служба Специальных объектов при Президенте РФ
a. ФСБ
b. МО
c. ГУСП+
d. ФСО

16.В интересах каких федеральных органов государственной власти не занимаются мобильной подготовкой служба специальных объектов
a. нет верного ответа +
b. Верховного Суда РФ
c. палат Федерального Собрания РФ
d. Конституционного Суда РФ

17.Необходимость осуществления разведывательной деятельности определяет в пределах своих полномочий
a. Президент РФ
b. Федеральное собрание и Государственная Дума
c. Президент РФ и Федеральное Собрание+
d. Государственная Дума

18.Чем определены полномочия СВР РФ?
a. Конституцией
b.Указом Президента
c. ст.6 ФЗ «О внешней разведке»+
d. УК РФ

19.Что входит в структуру органов федеральной пограничной службы?
a. пограничная стража
b. органы пограничного контроля
c. органы внешней разведки
d. все вышеперечисленное+

20.Центральный орган управления военной разведкой в ВС РФ
a. ГРУ +
b. СВР
c. СВО
d. КГБ

21.Назначение восьмого основного управления ГРУ
a. НАТО
b. диверсионное+
c.управление военной разведки
d. управление оперативной разведки

22.Общая организация и координация работ по защите информации, обрабатываемой техническими средствами, осуществляется
a. ФСТЭК+
b. ФСО
c. ГРУ

d. ФСБ

23.Кому подведомственна служба ФСТЭК?
a. ФСО
b.ФСБ
c. МО РФ+
d. Президенту РФ

24.В задачи ФСО РФ НЕ входит….
a. организация и провождение мероприятий по предотвращению утечки информации по техническим каналам в системах специальной связи, по предотвращению несанкционированного доступа к указанным системам
b. обеспечение защиты категорированных помещений
c. защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств+
d.осуществление эксплуатации, организация и провождение мероприятий по
совершенствованию, обеспечению безопасности и надежности систем специальной связи на территории РФ, а также международной правительственной и иных видов специальной международной связи

25.Правовую основу деятельности федеральных органов правительственной связи и информации составляет
a. Конституция РФ
b.все перечисленное +
c. нормативные акты
d. Законы РФ

26.В единую систему федеральных органов правительственной связи и информации НЕ входит
a. СМИ+
b.войска
c. Федеральное агентство правительственной связи и информации при Президенте
d. научно-исследовательские организации

27.Федеральные органы правительственной связи и информации в пределах своей компетентности
a. разработка, создание и использование специальных технических средств+
b. противодействие иностранным техническим разведкам
c. обеспечивают безопасность информации в ключевых системах информационной структуры
d. нет верного ответа

28.Документальные материалы, касающиеся деятельности федеральных органов правительственной связи и информации, хранятся в
a. ФСО
b. ФСБ
c. архивах этих органов+
d. Кремле

29.Надзор за исполнением законов РФ федеральными органами правительственной связи и информации осуществляет
a. Президент
b. нет верного ответа

c. Генеральный прокурор и подчиняющиеся ему прокуроры+
d. Генеральный прокурор

Тема 8. Проблемы обеспечения информационной безопасности в России.

1.Состояние защищенности интересов предприятия в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества, государства и бизнеса – это…
a. информационная система
b. информационная безопасность+
c. информационная сфера
d. информационные технологии

2.Что такое «стейкхолдер»?
a. IT-специалист
b. заинтересованная сторона+
c. шифр
d. хранилище

3.Что шифруют системы криптозащиты?
a. информацию
b. данные+
c. информацию и данные
d. нет верного ответа

4.Как расшифровывается аббревиатура DIKW?
a. данные, информация, ключ, окно
b. дата, информация, ключ, окно
c. дата, информация, ключ, данные
d. данные, информация, знания, мудрость +

5.На каких уровнях сегодня концентрируется большинство современных атак?
a. SCADA-решения
b. ERP-, CRM-решения
c. БД;
d.все выше перечисленное+

6.Основной закон в области Информационных Технологий и Информационной Безопасности
a. Закон РФ №5485
b. ISO-IEC
c. ФЗ №149+
d. Доктрина ИБ

7.Какие органы исторически занимались вопросами информационной безопасности страны?
a. Государственная Дума
b. аппарат Президента
c. спецслужбы+
d. органы законодательной власти

8.Какие системы сертификации средств защиты существуют в РФ?
a. МО и СВР

b. ФСБ
c. все вышеперечисленное+
d. ФСТЭК

9.Что является наглядным подтверждением сертификации на продукте?
a. печать
b. надпись «Товар сертифицирован»;
c. голограмма+
d. пломба

Тема 9. Лицензирование и сертификация деятельности в области защиты информации.

1.Организационную структуру системы государственного лицензирования предприятий в области защиты информации образуют
a. предприятия-заявители
b. все перечисленное+
c. государственные органы по лицензированию
d. лицензионные центры

2.Уполномоченные органы на ведение лицензионной деятельности на право осуществления мероприятий и/или оказания услуг в области защиты ГТ
a. ФСБ,ФСО
b. ФСБ, ФСТЭК
c. ФСБ, ФСО, ФСТЭК
d. ФСБ, ФСО, СВР+

3.При работе с Конфиденциальной Информацией лицензированию НЕ подлежат следующие виды деятельности.
a. Деятельность по распространению и техническому обслуживанию шифровальных (криптографических) СЗИ
b. Деятельность по технической защите КИ.
c. Проведение экспертиз предприятий.+
d. Предоставление услуг в области шифрования информации.

4.На орган по лицензированию НЕ возлагается.
a. Приобретение, учет и хранение бланков лицензий. Неверно
b.Организация работы лицензионных центров.
c. Выдача лицензий.
d. Ведение секретных переговоров.+

5.Объекты, НЕ подлежащие обязательной аттестации
a. управление экологически опасными объектами.
b. государственная тайна.
c. ведение секретных переговоров
d. уставы организаций+

6.Помещения, предназначенные для проведения закрытых мероприятий (совещаний, конференций, заседаний, сборов, переговоров и т. п.), на которых обсуждаются вопросы, содержащие охраняемые сведения
a.закрытые помещения

b. выделенные помещения+

c. охраняемые помещения

d. все перечисленное

7.В соответствие с какой статьей Закона РФ "О государственной тайне" все средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности

a. 28 +

b. 29

c. 36

d. 47

8.Организация сертификации средств ЗИ возлагается на (выберете 1 или несколько вариантов ответа

a. ФСТЭК+

b. ФСО

c. ФСБ

Тема 10. Организационно правовая система борьбы с терроризмом.

1.Правовую систему борьбы с терроризмом составляют:

a. УК РФ

b.все выше перечисленное

c. Конституция РФ

d. ФЗ «О борьбе с терроризмом»+

2.Террористическая деятельность НЕ включает

a. законность +

b. вербовку

c. организация, планирование террористической атаки

d. финансирование террористической организации

3.Главный субъект в структуре взаимодействия субъектов, осуществляющих борьбу с терроризмом

a. Правительство+

b. ФСБ

c. МО

d. СВР

4.Какие права в зоне проведения контртеррористической операции имеют лица, проводящие указанную операцию:

a. использовать в служебных целях средства связи, включая специальные, принадлежащие гражданам и организациям независимо от форм собственности

b. задерживать и доставлять в органы внутренних дел Российской Федерации лиц, совершивших или совершающих правонарушения либо иные действия, направленные на воспрепятствование законным требованиям лиц, проводящих контртеррористическую операцию

c. проверять у граждан и должностных лиц документы, удостоверяющие их личность

d. все перечисленное+

5.Кто осуществляет защиту оружия массового поражения, ракетного, стрелкового оружия, боеприпасов и взрывных веществ:

a. СВ

b. МО+

c. ФСО
d. ФСБ

6.Чем занимается федеральная антитеррористическая комиссия (выберете один или несколько вариантов ответа).
a. формированием экспертных комиссий
b. принятием участия в подготовке международных договоров в РФ в области борьбы с терроризмом+
c. досмотром граждан и их личных вещей
d. проверкой документов, удостоверяющих личность

Тема 11. 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 70-80гг 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 г.г. 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 12. 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 13. 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 14. Система защиты информации в США.

1.В каких направлениях осуществляется деятельность системы ЗИ в США?
a. контроль за допуском персонала к секретным документом и порядком выезда секретоносителей 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 15. 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 16. 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»
c. «Волновой перехват»
d. «Внешняя угроза»

5.Какие управления входят в состав Управления Военной Разведки (DRM)
a. исследовательское
b. все перечисленное+
c. аналитическое
d. техническое

6.В компетенцию Генерального Управления Внешней Безопасности (DGSE) входит
a. проведение тайных операций
b. все вышеперечисленное+
c. 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+
c. 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 17. 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

Тема 18. Цифровой суверенитет.

1.После чего возникло понятие суверенного государства
a. Первой мировой войны
b. «Холодной» войны
c. Вестфальского мира+
d. Второй мировой войны

2.Суверенитет бывает
a. экономический и политический

b. все перечисленное+
c. военный
d. культурный

3.Новый ключевой компонент суверенитета
a. идеологический
b. культурный
c. цифровой+
d. дипломатический суверенитет

4.К электронному суверенитету относится
a. устойчивость к электронным атакам
b. защита от вирусов
c. все перечисленное+
d. защищенность от выключения инфраструктуры и ПО

5.Что НЕ входит в «электронный щит» для обеспечения суверенитета
a. собственная или контролируемая программная платформа
b. собственная или контролируемая мобильная платформа
c. собственная аппаратная платформа
d. нет верного ответа+

6.У кого есть полноценный цифровой суверенитет (выберете один или несколько вариантов ответа)
a. США+
b.Англия
c. Китай

7.«Малый информационный щит» включает
a. средства ведения надзора
b. средства защиты
c. средства оборота
d. средства влияния+

Тема 19. Кибербезопасность – мир экспертов и преступников.

1.Что представляет собой аббревиатура IoE?
a.Проницательность во всем
b. Интеллект по всему
c. Интернет ежедневно
d. Интернет вещей+

2. Какова категория кадровой структуры, которая включает узкоспециализированный обзор и оценку поступающей информации о кибербезопасности, чтобы определить, полезна ли она для разведки?
a.Анализ+
b. Охрана и защита
c. Надзор и развитие
d. Безопасное обеспечение

3. Какой тип атаки может отключить компьютер, заставляя его использовать память или перегружая свой процессор?

a. Истощение
b. APT
c. DDoS
d. Алгоритм+

4. Что означает термин «уязвимость»?
a. Потенциальная угроза, которую создает хакер
b.Машина жертвы или известная цель
c. Слабость, которая делает цель восприимчивой к атаке+
d. Компьютер, содержащий конфиденциальную информацию
e. Метод атаки для определенной цели
5. Как предотвратить киберпреступление? (Выберите два ответа.)
a. Создать систему раннего предупреждения+
b. Обмен информацией в кибер-разведке+
c. Выключить сеть
d. Нанять хакеров
e. Изменить операционную систему
6. Что может служить примером домена данных в Интернете?
a.Linkedin+
b. Cisco
c. Palo Alto
d.Juniper

7. Какой вид информации заинтересует преступников при краже данных с разных организаций. (Выберите три.)
a. Медицинская+
b. Игра
c. Место работы+
d. Полет (номер рейса)
e. Питание
f. Образование+

8. Как зовут хакера-любителя?
a. Скрипт Кидди+
b. Синяя команда
c. Красная Шапка
d. Черная шляпа

9. Какой тип атаки использует множество систем с целью довести компьютер жертвы до отказа?
a. Ping sweep
b. DoS
c. Spoof
d. DDoS+
10. Как зовут хакеров, которые взламывают для защиты чего-либо (например, для защиты политических взглядов)?
a. Белая шляпа
b.Голубая шляпа
c. Хактивист+
d. Хакер

11. Что означает термин BYOD (ПСУ)?
a. Принести свое собственное решение
b. Купи свое собственное бедствие
c. Принести свою собственную катастрофу
d. Принеси свое устройство+

Тема 20. «Куб» кибербезопасности.

1. Каковы три основополагающих принципа кибербезопасности? (Выберите три.)
a. Целостность+
b. Шифрование
c. Безопасность
d. Доступность+
e. Политика
f. Конфиденциальность+

2. Как называются любые изменения исходных данных, такие как изменение данных пользователями вручную, обработка и изменение данных программами и сбои оборудования?
a. Резервное копирование
b. Коррупция
c. Модификация+
d. Целостность
e. Удаление
f.Распространение

3. Как называется защищенная виртуальная сеть, использующая общедоступную сеть?
a. VPN+
b. IDS
c. MPLS
d. NAC
e. IPS
f.Брандмауэр

4. Какие существуют службы безопасности для контроля доступа? (Выберите три.)
a. Аутентификация+
b. Доступ
c.Ведение журнала учета+
d. Отвержение
e. Доступность
f. Авторизация+

5. Какие два метода помогают обеспечить доступность системы? (Выберите два.)
a. Обслуживание оборудования+
b. Огнетушители
c. Отказоустойчивость системы
d. Проверка целостности
e. Создание системных резервных копий
f. Своевременное обновление операционных систем+

6. Какие три задачи выполняет комплексная политика безопасности? (Выберите три.)
a. Не имеет юридической силы
b. Полезен для управления
c. Дает сотрудникам службы безопасности поддержку+
d. Неопределенность
e. Определяет правовые последствия нарушений+
f. Устанавливает правила для ожидаемого поведения+

7. Какие существуют три состояния данных? (выберите три варианта)
a. В облаке
b. Отложенный
c. В работе (в процессе)+
d. В пути (когда данные загружаются)+
e. Зашифрованный
f. В состоянии покоя+

8. Какие законы кибербезопасности защищают вас от организации, которая может захотеть поделиться вашими конфиденциальными данными?
a.Конфиденциальность+
b.Аутентификация
c. Невозвращение
d.Целостность

9. Каковы две общие хэш-функции? (Выберите два.)
a. RSA
b.Blowfish
c. RC4
d.ECC
e.SHA+
f.MD5+

10. Какие два метода помогают обеспечить целостность данных? (Выберите два.)
a.Авторизация
b. Проверка целостности данных+
c. Конфиденциальность
d. Доступность
e. Отрицание
f. Хэширование+

11. Какой механизм организации могут использовать для предотвращения случайных изменений авторизованными пользователями?
a. Контроль версий+
b. Резервное копирование
c. Хэширование
d. Шифрование
e. SHA-1

12. Какая служба определяет, к каким ресурсам пользователь может получить доступ наряду с операциями, которые может выполнять пользователь?

a. Аутентификация
b. Авторизация+
c. Ведение журнала учета
d.Токен
e. Биометрические данные

13. Какие три принципа проектирования помогают обеспечить высокую доступность? (Выберите три.)
a. Устранение отдельных точек отказа+
b. Проверка соответствия данных
c. Обеспечение надежного кроссовера+
d. Обнаружение сбоев по мере их возникновения+
e. Обеспечение конфиденциальности
f. Использование шифрования

14. Какие три метода используются для проверки подлинности? (Выберите три.)
a. Что вы делаете
b. Где вы находитесь
c. То, чем вы (например: увлекаетесь)+
d. То, что у вас есть+
e. То, что вы знаете+

15. Что такое метод отправки информации с одного устройства на другой с помощью съемного носителя?
a. Пакет
b. Беспроводная сеть
c. Инфракрасная сеть
d. Проводная сеть
e. Кросснет+
f. Локальная сеть

16. Какие два метода обеспечивают конфиденциальность? (Выберите два.)
a. Доступность
b. Целостность
c. Безотказность
d.Авторизация
e. Аутентификация+
f. Шифрование+

17. Что определено первым в кибербезопасности?
a. Знания
b. Цели+
c. Защитные меры
d. Инструменты
e. Правила

18. Какой принцип предотвращает раскрытие информации посторонним лицам, ресурсам и процессам?
a. Безотказность

b. Конфиденциальность+
c. Целостность
d. Ведение журнала учета
e. Доступность

19. Какое имя присваивается устройству хранения, подключенному к сети?
a. NAS+
b. Облако
c. SAN
d. DAS
e. RAID

20. Какие существуют типы конфиденциальной информации? (Выберите три.)
a. Бизнес+
b. Личная информация+
c. Общедоступная
d. Опубликованная
e. Секретная
f. Рассекреченная

Тема 21. Угрозы кибербезопасности, уязвимости и атаки.

1. Какой термин используется, когда злоумышленник отправляет мошенническое письмо, замаскированное под законный, надежный источник?
a. Троянский конь
b. Фишинг+
c. Вишинг
d. Социальная инженерия
e. Черный ход

2. Как называется тип программного обеспечения, который генерирует доход путем создания раздражающих всплывающих окон?
a. Всплывающие окна
b. Трекеры
c. Шпионское ПО
d. Рекламное ПО+

3. Как называется уязвимость, которая позволяет злоумышленникам внедрять скрипты на веб-страницы, просматриваемые пользователями?
a. Ввод XML
b. SQL-инъекция
c. Межсайтовый скриптинг+
d. Переполнение буфера

4. Какой тип атаки нацелен на базу данных SQL, используя поле ввода пользователя?
a. Межсайтовый скриптинг+
b. SQL-инъекция
c. Ввод XML
d. Переполнение буфера

5. Какие тактики используются в социальной инженерии для получения личной информации от ничего не подозревающей цели? (Выберите два.)
a. Честность
b. Целостность
c. Срочность+
d. Запугивание+
e. Сострадание

.6. В чем разница между вирусом и червем?
a. Вирусы скрываются в законных программах, а черви нет.
b. Черви самореплицируются, но вирусы этого не делают.+
c. Черви требуют файл хоста, а вирусы нет.
d. Вирусы самореплицируются, а черви нет.

7. Что модифицирует руткит?
a. Экранную заставку
b. Операционную систему+
c. Блокнот
d. Программы
e. Microsoft Word

8. Какие две причины объясняют, почему WEP является слабым протоколом?(Выберите два.)
a. Ключ передается в открытом виде.+
b. Все в сети используют другой ключ.
c. Настройки по умолчанию не могут быть изменены.
d. WEP использует те же функции шифрования, что и Bluetooth.
e. Ключ статичен и повторяется в перегруженной сети.+

9. Какой термин описывает отправку короткого обманчивого SMS-сообщения, используемого для обмана цели при посещении веб-сайта?
a. Нелегальное ПО
b. Смишинг+
c. Спам
d. Подражание

.10. Что происходит на компьютере, когда данные выходят за пределы буфера?
a. Межсайтовый скриптинг
b.Переполнение буфера+
c. SQL-инъекция
d. Системное исключение
11. Злоумышленник сидит перед магазином и по беспроводной сети копирует электронные письма и списки контактов с близлежащих ничего не подозревающих пользовательских устройств. Что это такое?
a. Smishing
b. RF jamming
c. Bluesnarfing+
d. Bluejacking

12. Компьютер представляет пользователю экран с просьбой об оплате, прежде чем данные пользователя могут быть доступны для того же пользователя. Что это за вредоносное ПО?
a. Тип выкупа+
b. Тип логической бомбы
c. Тип вируса
d. Тип червя
13. Как называется программа или программный код, который обходит обычную аутентификацию?
a. Червь
b. Вирус
c. Троянский конь
d. Вымогатели
e. Бэкдор+

14. Каковы два общих показателя спам-почты? (Выберите два.)
a. В электронном письме есть слова с ошибками или знаки пунктуации или и то, и другое.+
b. Письмо от друга.
c. В письме нет темы.+
d. Письмо от вашего руководителя.
e. В нем есть ключевые слова.
f. В электронном письме есть вложение, которое является квитанцией для недавней покупки.

15. В чем смысл термина «логическая бомба»?
a. Вредоносный вирус
b. Вредоносный червь
c. Вредоносная программа, которая скрывается в законной программе
d. Вредоносная программа, которая использует триггер для пробуждения вредоносного кода+

16. Преступник использует программное обеспечение для получения информации о компьютере пользователя. Как называется этот тип программного обеспечения?
a. Вирус
b. Фишинг
c. Шпионское ПО+
d. Рекламное ПО

17. Какой термин используется для взлома электронной почты, путем отправки письма, предназначенного для конкретного лица, работающего в финансовом учреждении?
a. Направленный фишинг+
b. Целевой фишинг
c. Вишинг
d. Спам
e. Шпионское ПО

18. Какие два способа защитить компьютер от вредоносного ПО? (Выберите два.)
a. Удалить неиспользуемое программное обеспечение.
b. Использовать антивирусное программное обеспечение.+
c. Очистить кеш браузера.
d. Постоянно обновлять программное обеспечение.+
e. Дефрагментировать жесткий диск.

Тема 22. Криптографические методы защиты информации.

1. Какой 128-битный алгоритм шифрования блочных шифров используется правительством США для защиты секретной информации?

a. Цезарь
b. 3DES
c. Skipjack
d. Vignere
e. AES+

2. Предупреждающий баннер, в котором перечислены отрицательные результаты нарушения политики компании, отображается каждый раз, когда пользователь компьютера входит в систему. Какой тип контроля доступа реализован?

a. Превентивный
b. Детективный
c. Сдерживающий+
d. Маскировка

3. Каково имя метода, в котором буквы переупорядочены для создания зашифрованного текста?

a. Перестановка+
b. Замена
c. Шифр Вернама
d. Загадка

4)Обфускация – это:

a.Создание сообщения, которое говорит одно, но означает что-то другое для определенной аудитории
b.Обнаружение скрытой информации в графическом файле
c. Сделать сообщение запутанным, поэтому его трудно понять+

5. Какой термин используется для описания скрытия данных в другом файле, таком как графический, звуковой или другой текстовый файл?

a. Скрытность
b. Стеганография+
c. Путаница
d. Маскировка

6. Какой термин используется для описания технологии, которая заменяет конфиденциальную информацию с помощью нечувствительной версии?

a. Подавление
b. Сокращение
c. Мгла
d. Маскировка+
e. Скрытность

7. Какой тип шифра способен зашифровать блок обычного текста фиксированной длины в 128-битный блок зашифрованного текста в любой момент времени?

a.Симметрия
b. Блочный тип
c. Трансформирования
d. Хэш

e. Поток +

8. Какой тип шифрования шифрует открытый текст один байт или один бит за раз?
a. Загадка
b.Эллиптический
c. Хэш
d. Поток+
e. Блочный тип

9. Пароль – это:
a. То, что вы знаете+
b.То, чем вы прикасаетесь
c. То, что вы ощущаете

10. Какой асимметричный алгоритм обеспечивает электронный способ обмена ключами для обмена секретным ключом?
a. Хэширование
b. WEP
c. DES
d.RSA
e. Diffie-Hellman+

11. Какие три устройства представляют собой примеры контроля физического доступа? (Выберите три.)
a. Маршрутизаторы
b. Видеокамеры+
c. Серверы
d. Магнитная карта+
e. Замки+
f. Межсетевые экраны

12. Какой алгоритм шифрования использует один ключ для шифрования данных и другой ключ для дешифрования данных?
a. Асимметрии+
b. Перестановки
c. Шифр Вернама
d. Симметрии

13. Какой термин используется для описания науки создания и взлома секретных кодов?
a.Подражание
b. Спуфинг
c. Факторизация
d. Джамминг
e. Криптология+

14. Какие два термина используются для описания ключей шифрования? (Выберите два.)
a. Ключевое пространство+
b. Длина ключа+
c. Кейлоггинг

d. Ключевая случайность

15. Какой алгоритм шифрования используется NSA и включает в себя использование эллиптических кривых для создания цифровой подписи и обмена ключами?
a. ECC+
b. Эль-Гамаль
c. IDEA
d. AES
e. RSA

16. Какие три процесса являются примерами логического контроля доступа?(Выберите три.)
a. Система обнаружения вторжений (IDS) для наблюдения за подозрительной сетевой активностью+
b. Ограждения для защиты периметра здания
c. Биометрические данные для проверки физических характеристик+
d. Магнитные карты для доступа к запрещенной зоне
e. Охранники для мониторинга экранов безопасности+
f. Брандмауэры для мониторинга трафика

17. Какой алгоритм шифрования использует один и тот же предварительный общий ключ для шифрования и дешифрования данных?
a. Асимметрия
b. Хэш
c. Шифр Вернама
d.Симметрия+

18. Какие три протокола используют асимметричные ключевые алгоритмы? (Выберите три.)
a.Расширенный стандарт шифрования (AES)
b. Безопасный протокол передачи файлов (SFTP)
c. Безопасная оболочка (SSH)+
d. Уровень защищенных сокетов (SSL)+
e. Довольно хорошая конфиденциальность (PGP)+
f. Telnet

19. Каковы три примера административных средств контроля доступа? (Выберите три.)
a .Система обнаружения вторжений (IDS)
b. Политика и процедура+
c. Прием на работу+
d. Защитно-караульная служба
e. Проверка данных
f. Шифрование

20. Какой термин описывает технологию, которая защищает программное обеспечение от несанкционированного доступа или модификации?
a. Товарный знак
b. Водяные знаки+
c. Авторские права
d. Контроль доступа

Тема 23. Обеспечение целостности данных.

1.Пользователь создал новую программу и хочет распространять ее всем в компании. Пользователь хочет убедиться, что при загрузке программы программа не будет изменена во время транзита. Что пользователь может сделать, чтобы программа не изменялась при загрузке?

a. Отключите антивирус на всех компьютерах.

b. Установите программу на отдельные компьютеры.

c. Зашифруйте программу и требуйте пароль после ее загрузки.

d. Распределите программу на флэш-накопителе.

e. Создайте хэш файла программы, который можно использовать для проверки целостности файла после его загрузки.+

2.Определите три ситуации, в которых может быть применена функция хэширования.(Выберите три.)

a. PKI+

b. IPsec+

c. WPA

d. DES

e. PPoE

f. CHAP+

3.Пользователь является администратором базы данных для компании. Пользователю было предложено внедрить правило целостности, в котором говорится, что каждая таблица должна иметь первичный ключ и что столбец или столбцы, выбранные как первичный ключ, должны быть уникальными, а не нулевыми. Какое требование целостности реализуется пользователем?

a. Целостность объекта+

b.Целостность домена

c. Целостность аномалий

d. Ссылочная целостность

4. Какова цель CSPRNG?

a. Чтобы компьютер не был зомби

b. Для обеспечения веб-сайта

c. Для получения соли+

d. Обрабатывать хеш-запросы

5. Каков стандарт для инфраструктуры открытого ключа для управления цифровыми сертификатами?

a. NIST SP800

b. x.503

c. x.509+

d. PKI

6. Какова сила использования функции хеширования?

a. Он имеет выход переменной длины.

b. Он не используется в безопасности.

c. Это односторонняя функция и не обратимая.+

d. Он может принимать только сообщение с фиксированной длиной.

7. Можно создать два разных файла, имеющих одинаковый вывод. Пользователь загружает обновленный драйвер для видеокарты с веб-сайта. Появляется предупреждающее сообщение о том, что драйвер не одобрен. Чего не хватает в этой части программного обеспечения?

a. Действительный идентификатор
b. Исходный код
c. Цифровая подпись+
d. Распознавание кода

8.Пользователь оценивает инфраструктуру безопасности компании и замечает, что некоторые системы аутентификации не используют передовые методы, когда дело доходит до хранения паролей. Пользователь может быстро взломать пароли и получить доступ к конфиденциальным данным. Пользователь хочет представить рекомендации компании о правильной реализации соления, чтобы избежать методов взлома паролей. Каковы три наилучшие практики внедрения соления? (Выберите три.)
a. Для каждого пароля должна использоваться одна и та же соль.
b. Соль должна быть уникальной для каждого пароля.+
c. Соль нельзя использовать повторно.+
d. Соли не являются эффективной передовой практикой.
e. Соли должны быть короткими.
f. Соль должна быть уникальной.+

9. Пользователю было предложено внедрить IPsec для входящих внешних подключений. Пользователь планирует использовать SHA-1 как часть реализации. Пользователь хочет обеспечить целостность и подлинность соединения. Какой инструмент безопасности может использовать пользователь?
a. MD5
b. SHA256
c. HMAC+
d. ISAKMP

10. Следователь находит USB-накопитель на месте преступления и хочет представить его в качестве доказательства в суде. Следователь берет USB-накопитель и создает его криминалистический образ и берет хэш как оригинального USB-устройства, так и созданного образа. Что следователь пытается доказать о USB-накопителе, когда доказательства представлены в суде?
a. Следователь нашел USB-накопитель и смог сделать его копию.
b. Точную копию устройства сделать нельзя.
c. Все данные есть.
d. Данные на изображении являются точной копией, и ничто не было изменено процессом.+

11. Каковы три типа атак, которые можно предотвратить с помощью соления? (Выберите три.)
a. Радужные таблицы+
b. Плечевой серфинг
c. Таблицы обратного поиска+
d. Социальная инженерия
e. Таблицы поиска+
f. Фишинг
g. Угадывание

12. Какие три алгоритма цифровой подписи, одобренные NIST? (Выберите три.)
a. SHA256
b. RSA+
c. ECDSA+
d. DSA+

e. MD5
f. SHA1

13. Каков пошаговый процесс создания цифровой подписи?

a. Создайте дайджест сообщения; зашифруйте дайджест с закрытым ключом отправителя; и объедините сообщение, зашифрованный дайджест и открытый ключ вместе для подписания документа.+

b. Создайте дайджест сообщения; зашифруйте дайджест открытым ключом отправителя; и объедините сообщение, зашифрованный дайджест и открытый ключ вместе, чтобы подписать документ.

c. Создайте сообщение, зашифруйте его хэшем MD5 и отправьте пакет с открытым ключом.

d. Создайте хэш SHA-1; зашифруйте хэш с закрытым ключом отправителя; и объедините сообщение, зашифрованный хэш и открытый ключ вместе с подписанным документом.

14. Алиса и Боб используют один и тот же пароль для входа в сеть компании. Это означает, что оба будут иметь одинаковый хэш для своих паролей. Что может быть реализовано для предотвращения того, чтобы оба хэша паролей были одинаковыми?

a. Соление+
b. RSA
c. Псевдослучайный генератор
d. Перчение

15. Какой метод пытается использовать все возможные пароли до тех пор, пока не будет найдено совпадение?

a. Брут форс.+
b. Радужные таблицы
c. Криптография
d. Словарь
e. Облако
f. День рождения

16. Каковы три критерия проверки правильности для правила валидации? (Выберите три.)

a. Ключ
b. Диапазон+
c. Тип
d. Размер+
e. Шифрование
f. Формат+

17. Пользователь проинструктирован боссом, чтобы найти лучший метод для защиты паролей в пути. Пользователь исследовал несколько способов сделать это и остановился на использовании HMAC. Какие ключевые элементы необходимы для реализации HMAC?

a. IPsec и контрольная сумма
b. Дайджест сообщения и асимметричный ключ
c. Симметричный ключ и асимметричный ключ
d. Секретный ключ и дайджест сообщений+

18. Пользователь подключается к серверу электронной коммерции для покупки некоторых виджетов для компании. Пользователь подключается к сайту и замечает, что в строке состояния безопасности браузера нет блокировки. Сайт запрашивает имя пользователя и пароль, и пользователь может войти в систему. Какова опасность при продолжении этой транзакции?

a. Программное обеспечение блокировщика объявлений препятствует правильной работе панели безопасности и, следовательно, нет никакой опасности для транзакции.

b. Сертификат с сайта истек, но по-прежнему безопасен.

c. Для выполнения транзакции пользователь использует неправильный браузер.

d. Сайт не использует цифровой сертификат для обеспечения транзакции, в результате чего все становится ясным.+

19. Недавнее письмо, отправленное по всей компании, заявило, что произойдут изменения в политике безопасности. Сотрудник службы безопасности, который, как предполагалось, отправил сообщение, заявил, что сообщение не было отправлено из службы безопасности, и компания может быть жертвой подделанного письма. Что могло быть добавлено в сообщение, чтобы сообщение действительно пришло от человека?

a. Асимметричный ключ

b. Хэширование

c. Расторжение

d. Цифровая подпись+

20. Недавнее нарушение в компании было связано с возможностью хакера получить доступ к корпоративной базе данных через веб-сайт компании, используя неверные данные в форме входа в систему. В чем проблема с веб-сайтом компании?

a. Плохая проверка ввода+

b. Плохое имя пользователя

c. Отсутствие исправлений операционной системы

d. Слабое шифрование

Тема 24. Концепция «пяти девяток».

1. Нарушение безопасности произошло в крупной корпорации. Группа инцидентов ответила и выполнила свой план реагирования на инциденты. На каком этапе используются извлеченные уроки?

a.Обнаружение

b. Политика сдерживания

c. Восстановление

d. Подготовка

e. После инцидента+

f. Анализирование

2. Пользователю предлагается оценить центр обработки данных для повышения доступности для клиентов. Пользователь замечает, что есть только одно подключение к интернет-провайдеру, некоторые из оборудования не имеют гарантии, нет запасных частей, и никто не контролировал ИБП, который срабатывал дважды в течение одного месяца. Какие три недостатка в высокой доступности идентифицированы пользователем? (Выберите три.)

a. Одиночные точки отказа+

b. Отказ от проектирования для надежности+

c. Неспособность предотвратить инциденты безопасности

d. Отказ защиты от плохого обслуживания

e. Неспособность обнаруживать ошибки по мере их возникновения+

f. Неспособность определить проблемы управления

3. Группе было предложено создать план реагирования на инциденты в случае инцидентов с безопасностью. На каком этапе плана реагирования на инциденты команда получает одобрение руководства плана?
a. Восстановление
b. Обнаружение
c. После инцидента
d. Политика сдерживания
e. Подготовка+
f. Анализ

4. Пользователю предлагается оценить положение безопасности компании. Пользователь просматривает прошлые попытки проникнуть в компанию и оценивает угрозы и риски для создания отчета. Какой тип анализа риска может выполнить пользователь?
a. Мнение
b. Задача
c. Качественный+
d. Субъективный

5. Пользователь должен добавить избыточность к маршрутизаторам в компании. Какие три варианта пользователь может использовать? (Выберите три.)
a. GLBP+
b. PTS
c. IPFIX
d. RAID
e. VRRP+
f. HSRP+

6. Пользователь покупает новый сервер для дата-центра компании. Пользователь хочет разбить диск с четностью на трех дисках. Какой уровень RAID должен выполнить пользователь?
a. 1+0
b. 1
c. 0
d. 5+

7. Пользователю предлагается создать план аварийного восстановления для компании. У пользователя должно быть несколько вопросов, на которые отвечает руководство для продолжения. Какие три вопроса должны задать пользователю управление в рамках процесса создания плана? (Выберите три.)
a. Требует ли процесс утверждения?
b. Как долго проходит процесс?
c. Может ли человек выполнить этот процесс?
d. Кто несет ответственность за процесс+
e. Каков процесс?+
f. Где человек выполняет этот процесс?+

8. Компания обеспокоена трафиком, который протекает через сеть. Существует опасение, что существует вредоносная программа, которая существует, которая не блокируется или не устраняется антивирусом. Какую технологию можно внедрить для обнаружения потенциального вредоносного трафика в сети?

a. IDS+
b. NAC
c. IPS
d. Брандмауэр

9. Пользователь выполнил шестимесячный проект для определения всех местоположений данных и каталогизации местоположения. Следующим шагом будет классификация данных и получение некоторых критериев чувствительности данных. Какие два шага могут предпринять пользователь, чтобы классифицировать данные? (Выберите два.)
a. Определение разрешения для данных.
b. Определение пользователя данных.
c. Определить, как часто копируются данные.
d. Рассмотреть все данные одинаково.
e. Определить чувствительность данных.+
f. Установить владельца данных.+

10. Пользователь был нанят компанией для предоставления высокодоступной сетевой инфраструктуры. Пользователь хочет построить избыточность в сети в случае отказа коммутатора, но хочет предотвратить цикл 2-го уровня. Что бы пользователь реализовал в сети?
a. Протокол связующего дерева+
b. VRRP
c. HSRP
d. GLBP

11. Пользователь оценивает сетевую инфраструктуру компании. Пользователь отметил множество резервных систем и устройств на месте, но нет общей оценки сети. В отчете пользователь подчеркнул методы и конфигурации, необходимые в целом, чтобы сделать отказоустойчивость сети. Какой тип дизайна пользователь подчеркивает?
a. Комплексный
b. Основное дерево
c. Устойчивость+
d. Доступность

12. Пользователь пересматривает сеть для небольшой компании и хочет обеспечить безопасность по разумной цене. Пользователь развертывает новый брандмауэр с поддержкой приложений с возможностями обнаружения вторжений в ISP-соединении. Пользователь устанавливает второй брандмауэр, чтобы отделить сеть компании от общедоступной сети. Кроме того, пользователь устанавливает IPS во внутренней сети компании. Какой подход выполняет пользователь?
a. Слоистый+
b. Риск на основе
c. Атака
d. Структурированный

13. Пользователю предлагается провести анализ рисков компании. Пользователь запрашивает базу данных активов компании, которая содержит список всего оборудования. Пользователь использует эту информацию как часть анализа риска. Какой тип анализа риска может быть выполнен?
a. Качественный
b. Аппаратные средства
c. Количественный+
d. Коэффициент воздействия

14. Пользователь был нанят в качестве нового сотрудника службы безопасности. Одним из первых проектов стало проведение инвентаризации активов компании и создание комплексной базы данных. Какие три части информации пользователь хотел бы захватить в базе данных активов? (Выберите три.)

a. Аппаратные сетевые устройства+

b. Пароли

c. Группы

d. Операционные системы+

e. Пользователи

f. Рабочие станции+

15. Пользователь выполняет обычную проверку серверного оборудования в центре данных компании. Несколько серверов используют отдельные диски для размещения операционных систем и нескольких типов подключенных решений хранения данных для хранения данных. Пользователь хочет предложить лучшее решение для обеспечения отказоустойчивости во время сбоя накопителя. Какое решение лучше?

a. UPS

b. Резервное копирование

c. RAID+

d.Автономная резервная копия

16. Генеральный директор компании обеспокоен тем, что если нарушение данных должно произойти, и данные клиента подвергаются, компания может быть предъявлен иск. Генеральный директор принимает решение о покупке страховки для компании. Какой тип снижения рисков внедряет генеральный директор?

a. Смягчение

b. Перенесение+

c. Сокращение

d.Уклонение

17. Пользователь является консультантом, который нанят для подготовки доклада Конгрессу о том, какие отрасли должны быть обязаны поддерживать доступность. Какие три отрасли должны быть включены Пользователем в отчет? (Выберите три.)

a. Розничная торговля

b. Финансы+

c. Общественная безопасность+

d. Питание

e. Здравоохранение+

f. Образование

Тема 25. Защита домена кибербезопасности.

1. В чем разница между HIDS и брандмауэром(firewall)?

a. Брандмауэр (firewall) разрешает и запрещает трафик на основе правил, а HIDS контролирует сетевой трафик.

b. HIDS блокирует вторжения, тогда как брандмауэр их фильтрует.

c. HIDS отслеживает операционные системы на хост-компьютерах и обрабатывает активность файловой системы. Брандмауэры разрешают или запрещают трафик между компьютером и другими системами.+

d. HIDS работает как IPS, тогда как брандмауэр просто отслеживает трафик.

e. Брандмауэр выполняет фильтрацию пакетов и поэтому ограничен в эффективности, тогда как HIDS блокирует вторжения.

2. Пользователь обращается в службу поддержки с жалобой на то, что пароль для доступа к беспроводной сети изменился без предупреждения. Пользователь может изменить пароль, но через час происходит то же самое. Что может произойти в этой ситуации?

a. Политика паролей

b. Посторонняя точка доступа+

c. Ноутбук пользователя

d. Слабый пароль

e. Ошибка пользователя

3. Какая служба преобразует определенный веб-адрес в IP-адрес целевого веб-сервера?

a. DNS+

b. NTP

c. DHCP

d. ICMP

4. Менеджер отдела подозревает, что кто-то пытается взломать компьютеры ночью. Вас просят выяснить, так ли это. Какое ведение журнала вы бы включили?

a. Аудит+

b. Windows

c. Операционная система

d. Системный журнал

5. После аудита безопасности для организации было установлено, что несколько учетных записей имеют привилегированный доступ к системам и устройствам. Какие три рекомендации по защите привилегированных учетных записей должны быть включены в отчет аудита? (Выберите три варианта ответа.)

a. Только ИТ-директор должен иметь привилегированный доступ.

b. Никто не должен иметь привилегированный доступ.

c. Применять принцип наименьших привилегий.+

d. Уменьшите количество привилегированных учетных записей.+

e. Безопасное хранение паролей.+

f. Только менеджеры должны иметь привилегированный доступ.

6. Пользователю предлагается проанализировать текущее состояние операционной системы компьютера. С чем следует сравнивать текущую операционную систему для выявления потенциальных уязвимостей?

a. Черный список

b. Базовый уровень+

c. Сканирование уязвимостей

d. Пентест

e. Белый список

7. Какие три элемента являются вредоносными программами? (Выберите три.)

a. APT

b. Вирус+

c. Троянский конь+

d. Кейлоггер+

e. Электронная почта
f. Вложения

8. Администратор небольшого центра обработки данных хочет иметь гибкий, безопасный способ удаленного подключения к серверам. Какой протокол лучше всего использовать?
a. Secure Shell+
b. Remote Desktop
c. Secure Copy
d. Telnet

9. Пользователь обращается в службу поддержки с жалобами на то, что приложение установлено на компьютер и приложение не может подключиться к Интернету. Нет никаких антивирусных предупреждений, и пользователь может просматривать Интернет. Какова наиболее вероятная причина проблемы?
a. Компьютерный файервол+
b. Необходимо перезагрузить систему
c. Отсутствуют разрешения
d. Приложение повреждено

10. Компании могут иметь различные операционные центры, которые обрабатывают различные проблемы с ИТ-операциями. Если проблема связана с сетевой инфраструктурой, какой операционный центр будет ответственным?
a. HVAC
b. NOC+
c. HR
d. SOC

11. Пользователь делает запрос на внедрение службы управления исправления для компании. В рамках заявки пользователь должен предоставить обоснование для запроса. Какие три причины могут использовать пользователь для обоснования запроса? (Выберите три.)
a. Необходимость подключения систем непосредственно к Интернету
b.Возможность выбора обновлений пользователями
c. Оповещать, когда происходят обновления+
d.Возможность получения отчетов по системам+
e. Нет возможности для пользователей отключать обновления+
f. Вероятность экономии на хранении

12. В компании много пользователей, которые дистанционно работают. Необходимо найти решение, чтобы можно было установить безопасный канал связи между удаленным местоположением пользователей и компанией. Какое хорошее решение для этой ситуации?
a. Модем
b. Оптоволокно
c. VPN+
d. T1
e. PPP

13. Каковы три типа проблем с питанием, которые должен беспокоить техника? (Выберите три.)
a. Искра
b. Скачок напряжения+
c. Отключение+

d. Обесточивание+
e. Затуманивание
f. Мерцание

14. Новый компьютер вынимается из коробки, запускается и подключается к Интернету. Патчи (исправления) были загружены и установлены. Обновлен антивирус. Что можно сделать, чтобы еще больше улучшить защиту операционной системы?
a. Установите аппаратный брандмауэр.
b. Выключите брандмауэр.
c. Отключите компьютер от сети.
d. Удалите ненужные программы и службы.+
e. Удалите учетную запись администратора.
f. Присвойте компьютеру неразрешимый адрес.

15. Почему WPA2 лучше WPA?
a. Поддерживает TKIP
b. Снижение скорости
c. Обязательное использование алгоритмов AES+
d. Сокращение времени обработки

16. Почему WEP сегодня не используется в беспроводных сетях?
a. Отсутствие шифрования
b. Потому что этот метод старый
c. Отсутствие поддержки
d. Использование понятных текстовых паролей
e. Легко взломать+

17. ИТ-директор хочет защитить данные на ноутбуках компании, внедряя шифрование файлов. Техник определяет лучший способ шифрования каждого жесткого диска с помощью Windows BitLocker. Какие две вещи необходимы для реализации этого решения? (Выберите два.)
a. TPM+
b. Управление паролями
c. Резервное копирование
d. Создать два тома+
e. EFS
f. USB- накопитель

18. Менеджер поддержки настольных систем хочет минимизировать время простоя для рабочих станций, которые вызывают сбои или имеют другие проблемы, связанные с программным обеспечением. Каковы три преимущества использования клонирования диска? (Выберите три.)
a. Сокращение численности персонала
b. Обеспечить совместимость системы
c. Может обеспечить полное резервное копирование системы+
d. Простота развертывания новых компьютеров в организации+
e. Обеспечить чистоту машины+
f. Создать большее разнообразие

19. Компания хочет реализовать биометрический доступ к своему центру обработки данных. Компания обеспокоена тем, что люди могут обходить систему, будучи ложно принятой в качестве законных пользователей. Какая ошибка - ложное принятие?

a. CER

b. Ложное отклонение

c. Type II+

d. Type I

20. Пользователь предлагает приобрести решение для управления патчами для компании. Пользователь хочет указать причины, по которым компания должна тратить деньги на решение. Какие преимущества дает управление патчами?(Выберите три.)

a. Администраторы могут утверждать или отклонять исправления.+

b. Патчи могут быть выбраны пользователем.

c. Патчи можно писать быстро.

d. Компьютеры требуют подключения к Интернету для получения патчей.

e. Обновления не обойти.+

f. Обновления могут быть принудительно задействованы в системах немедленно.+

21. Стажер начал работать в группе поддержки. Одна из обязанностей - установить локальную политику для паролей на рабочих станциях. Какой инструмент лучше всего использовать?

a. Политика паролей

b. grpol.msc

c. Политика учетной записи

d. Системное администрирование

e. secpol.msc+

Тема 26. Специалисты по кибербезопасности.

1. Профессионалу безопасности предлагается провести анализ текущего состояния сети компании. Какой инструмент будет использовать профессионал безопасности для сканирования сети только для рисков безопасности?

a. Сканер уязвимостей+

b. Вредоносные программы

c. PenTest

d. Пакетный анализатор

2. Компания пытается снизить затраты на развертывание коммерческого программного обеспечения и рассматривает облачную службу. Какая служба на основе облаков будет лучше всего размещать программное обеспечение?

a. PACXH

b. SaaS+

c. PaaS

d. IaaS

3. В организации реализована частная облачная инфраструктура. Администратору безопасности предлагается защитить инфраструктуру от потенциальных угроз. Какие три тактики могут быть реализованы для защиты частного облака?(Выберите три.)

a. Отключить брандмауэры.

b. Отключить сканирование портов.+

c. Нанять консультанта.

d. Проверьте входящий и исходящий трафик.+

e. Предоставить административные права.
f. Обновляйте устройства с исправлениями безопасности и исправлениями.+

4. Нарушение происходит в компании, которая обрабатывает информацию о кредитных картах. Какой отраслевой закон регулирует защиту данных кредитных карт?
a. SOX
b. PCI DSS+
c. CPA
d. GLBA

5. Каковы две потенциальные угрозы для приложений? (Выберите два.)
a. Социальная инженерия
b. Потеря данных+
c. Несанкционированный доступ+
d. Перебои

6. У компании было несколько инцидентов, связанных с пользователями, загружающими несанкционированное программное обеспечение, использующими несанкционированные веб-сайты и персональные USB-устройства. CIO хочет создать схему управления пользовательскими угрозами. Какие три вещи могут быть введены в действие для управления угрозами? (Выберите три.)
a. Применять дисциплинарные меры.
b. Изменение на слабые клиенты
c. Обеспечить подготовку по вопросам безопасности.+
d. Использовать фильтрацию содержимого.+
e. Отключить доступ к CD и USB.+
f. Мониторинг всех действий пользователей.

7. As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?
a. GLBA+
b. FIRPA
c. SOX
d. PCI

8. Какие три услуги предоставляет CERT? (Выберите три.)
a. Разработка инструментов, продуктов и методов анализа уязвимостей+
b. Устранение уязвимостей программного обеспечения+
c. Обеспечение соблюдения стандартов программного обеспечения
d. Разработка инструментов, продуктов и методов проведения судебных экспертиз+
e. Создание вредоносных программ
f. Разработка инструментов атаки

9. Неавторизованные посетители вошли в офис компании и гуляют по зданию. Какие две меры могут быть приняты для предотвращения несанкционированного доступа посетителей в здание? (Выберите два.)
a. Закрыть на ключ кабинеты+
b. Регулярно проводить обучение по вопросам безопасности.
c. Запретить выход из здания в рабочее время.+
d. Установить правила и процедуры для гостей, посещающих здание.

10. Так как человек является специалистом по безопасности, то есть возможность иметь доступ к конфиденциальным данным и активам. Что должен понимать специалист по безопасности, чтобы принимать обоснованные этические решения?
a. Поставщики облачных услуг
b. Потенциальный бонус
c. Партнерские объединения
d. Законы, регулирующие данные+
e. Потенциальная выгода

11. Если человек сознательно получает доступ к правительственному компьютеру без разрешения, какие федеральные законы будут действовать в отношении этого человека?
a. CFAA+
b. GLBA
c. ECPA
d. SOX

12. Почему Kali Linux является популярным выбором при тестировании сетевой безопасности организации?
a. Это инструмент сетевого сканирования, который ставит приоритеты на поиски провалов безопасности.
b. Его можно использовать для проверки слабых мест, используя только вредоносные программы.
c. Его можно использовать для перехвата и регистрации сетевого трафика.
d. Это дистрибутив безопасности Linux с открытым исходным кодом и содержит более 300 инструментов.+

13. Какие три исключения для раскрытия информации относятся к FOIA? (Выберите три.)
a. Национальная безопасность и внешняя политика+
b. Записи правоохранительных органов, в которых фигурирует одна из перечисленных проблем+
c. Негеологическая информация о дырах
d. Информация, специально не освобожденная законом
e. Публичная информация финансовых учреждений
f. Конфиденциальная деловая информация+

14. Какие два элемента можно найти на веб-сайте Internet Storm Center? (Выберите два.)
a. Отчеты информационной защиты+
b. Историческая справка
c. Текущие законы+
d. InfoSec вакансии

15. Администратор школы обеспокоен разглашением информации о школьнике из-за нарушения. В соответствии с каким законом обеспечивается защита информации учащихся?
a. FERPA+
b. CIPA
c. HIPPA
d. COPPA

16. Что можно использовать для оценки угроз с помощью счета воздействия, чтобы подчеркнуть важные уязвимости?
a. NVD+
b. ACSC

c. CERT
d. ISC

17. Каковы три широкие категории позиций информационной безопасности? (Выберите три.)
a. Наблюдатели+
b. Исполнители
c. Строители+
d. Искатели
e. Создатели
f. Определители+
18. Аудитору предлагается оценить локальную сеть компании на предмет потенциальных угроз. На какие три потенциальные угрозы может обратить внимание аудитор? (Выберите три.)
a. Несанкционированное сканирование портов и зондирование сети+
b. Политика допустимого использования
c. Комплексный пароль
d. Неправильно настроенный брандмауэр+
e. Закрытые системы
f. Разблокированный доступ к сетевому оборудованию+

19. Консультант нанимается, чтобы дать рекомендации по управлению угрозами устройств в компании. Какие три общие рекомендации можно сделать? (Выберите три.)
a. Включить мультимедийные устройства.
b. Обеспечение строгой кадровой политики.
c. Отключить права администратора для пользователей.+
d. Включить автоматическое антивирусное сканирование.+
e. Включение блокировки экрана+
f. Удаление фильтрации содержимого.

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ОК-2, ПК-25)

1. Этапы развития системы защиты информации.
2. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.
3. Типы современного информационного оружия.
4. Государственные органы обеспечения национальной безопасности США.
5. Представление об информационном противоборстве в Китае.
6. Практика компании IBM в области защиты информации.
7. Практика компании CiscoSystems в разработке сетевой политики безопасности.

Типовые задания для зачета (ОК-2, ПК-25)

1. Укажите операционную систему, наиболее часто подвергающуюся вирусным атакам.
a. Windows
b. Unix
c. Linux

2. В соответствии с Указом Президента России Гостехкомиссия в настоящее время именуется ...
a. ФСБ
b. ФСТЭК

c. СВР
d. ФАПСИ
3. Что НЕ входит в «электронный щит» для обеспечения цифрового суверенитета
a. собственная или контролируемая программная платформа
b. собственная или контролируемая мобильная платформа
c. собственная аппаратная платформа
d. нет верного ответа

4. Кто изобрел машину с вращательными шифровальными дисками с различным количеством букв?
a. Ж.-Ф.Шампольон
b. Д.Вадсворт
c. А.Тьюринг
d. Ч.Уитстон

5. К какому времени относят появление первых специализированных антивирусных программ?
a. начало 80-х гг
b. вторая половина 80-х гг
c. начало 90-х гг
d. вторая половина 70-х гг

Типовые вопросы экзамена (ОК-2, ПК-25)

1. Этапы развития системы защиты информации.
2. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.
3. Типы современного информационного оружия.
4. Государственные органы обеспечения национальной безопасности США.
5. Представление об информационном противоборстве в Китае.
6. Практика компании IBM в области защиты информации.
7. Практика компании CiscoSystems в разработке сетевой политики безопасности.

Типовые задания для экзамена (ОК-2, ПК-25)

1. Укажите операционную систему, наиболее часто подвергающуюся вирусным атакам.
a. Windows
b. Unix
c. Linux

2. В соответствии с Указом Президента России Гостехкомиссия в настоящее время именуется ...
a. ФСБ
b. ФСТЭК
c. СВР
d. ФАПСИ
3. Что НЕ входит в «электронный щит» для обеспечения цифрового суверенитета
a. собственная или контролируемая программная платформа
b. собственная или контролируемая мобильная платформа
c. собственная аппаратная платформа
d. нет верного ответа

4. Кто изобрел машину с вращательными шифровальными дисками с различным количеством букв?
a. Ж.-Ф.Шампольон

b. Д.Вадсворт
c. А.Тьюринг
d. Ч.Уитстон

5. К какому времени относят появление первых специализированных антивирусных программ?
a. начало 80-х гг
b. вторая половина 80-х гг
c. начало 90-х гг
d. вторая половина 70-х гг

4.4. Шкала оценивания промежуточной аттестации

Зачет

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ОК-2	Демонстрирует высокий уровень знаний процесса становления систем защиты информации в мире. Эффективно использует зарубежный опыт при разработке комплексной системы защиты информации. Свободно ориентируется в составе, основных направлениях деятельности и особенности функционирования органов защиты информации.¶Может сформулировать тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах.¶
	ПК-25	Свободно ориентируется в нормативно-правовых документов РФ и мира. Способен продемонстрировать способы и методики поиска информации в сети Интернет. Эффективно осуществляет поиск научной литературы по исследовательской и прикладной деятельности. Анализирует и систематизирует большие объемы информации. ¶Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу.¶
«не зачтено» (0 - 49 баллов)	ОК-2	Демонстрирует не достаточный уровень знаний процесса становления систем защиты информации в мире. Не способен использовать зарубежный опыт при разработке комплексной системы защиты информации. Не ориентируется в составе, основных направлениях деятельности и особенности функционирования органов защиты информации. Не может сформулировать тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах.
	ПК-25	Не ориентируется в нормативно-правовых документов РФ и мира. Не способен продемонстрировать способы и методики поиска информации в сети Интернет. Не осуществляет поиск научной литературы по исследовательской и прикладной деятельности. Не способен анализировать и систематизировать большие объемы информации.¶Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом¶

Экзамен

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

«отлично» (85 - 100 баллов)	ОК-2	Демонстрирует высокий уровень знаний процесса становления систем защиты информации в мире. Эффективно использует зарубежный опыт при разработке комплексной системы защиты информации. Свободно ориентируется в составе, основных направлениях деятельности и особенности функционирования органов защиты информации.¶Может сформулировать тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах.¶
	ПК-25	Свободно ориентируется в нормативно-правовых документов РФ и мира. Способен продемонстрировать способы и методики поиска информации в сети Интернет. Эффективно осуществляет поиск научной литературы по исследовательской и прикладной деятельности. Анализирует и систематизирует большие объемы информации. ¶Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу.¶
«хорошо» (70 - 84 баллов)	ОК-2	Демонстрирует достаточный уровень знаний процесса становления систем защиты информации в мире. Может использовать зарубежный опыт при разработке комплексной системы защиты информации. Достаточно свободно ориентируется в в составе, основных направлениях деятельности и особенности функционирования органов защиты информации. Может сформулировать тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах.
	ПК-25	Достаточно свободно ориентируется в нормативно-правовых документов РФ и мира. Способен продемонстрировать способы и методики поиска информации в сети Интернет. Осуществляет поиск научной литературы по исследовательской и прикладной деятельности. Анализирует и систематизирует большие объемы информации.¶Ответ построен логично, материал излагается хорошим языком. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений¶
«удовлетворительно» (50 - 69 баллов)	ОК-2	Демонстрирует не достаточный уровень знаний процесса становления систем защиты информации в мире. Не способен эффективно использовать зарубежный опыт при разработке комплексной системы защиты информации. Слабо ориентируется в составе, основных направлениях деятельности и особенности функционирования органов защиты информации. Затрудняется сформулировать тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах.
	ПК-25	Не достаточно ориентируется в нормативно-правовых документов РФ и мира. С затруднениями способен продемонстрировать способы и методики поиска информации в сети Интернет. Осуществляет поиск научной литературы по исследовательской и прикладной деятельности. Не способен к анализу и систематизации больших объемов информации.¶Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. Вопросы, задаваемые преподавателем, вызывают затруднения.¶

«неудовлетворительно» (менее 50 баллов)	ОК-2	Демонстрирует не достаточный уровень знаний процесса становления систем защиты информации в мире. Не способен использовать зарубежный опыт при разработке комплексной системы защиты информации. Не ориентируется в составе, основных направлениях деятельности и особенности функционирования органов защиты информации. Не может сформулировать тенденции и перспективы развития систем защиты информации в России и ведущих зарубежных странах.
	ПК-25	Не ориентируется в нормативно-правовых документов РФ и мира. Не способен продемонстрировать способы и методики поиска информации в сети Интернет. Не осуществляет поиск научной литературы по исследовательской и прикладной деятельности. Не способен анализировать и систематизировать большие объемы информации.¶Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом¶

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 презентаци, 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. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

2. 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)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

2. 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

3. 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

4. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов. - Весь срок охраны авторского права; Аудит информационной безопасности. - Брянск: Брянский государственный технический университет, 2012. - 268 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: http://www.iprbookshop.ru/6991.html

5. 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. 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

6.3 Иные источники:

1. Курс «Основы информационной безопасности» - https://www.intuit.ru/studies/courses/10/10/info

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 программное обеспечение:

Консультант Плюс

Google Chrome

Microsoft Windows 10

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: http://biblio.tsutmb.ru/elektronnyij-katalog
2. Электронная библиотека РФФИ. – URL: https://www.rfbr.ru/rffi/ru/library
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: https://www.studentlibrary.ru
4. Российская государственная библиотека. – URL: https://www.rsl.ru
5. Российская национальная библиотека. – URL: http://nlr.ru
6. Президентская библиотека имени Б.Н. Ельцина. – URL: https://www.prlib.ru
7. Научная электронная библиотека eLIBRARY.ru. – URL: https://elibrary.ru
8. Научная электронная библиотека Российской академии естествознания. – URL: https://www.monographies.ru
9. Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru

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.