Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.ДЭ.07.01
Организация и управление службой защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 64
самостоятельная работа 43,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Контактная работа на аттестации	0,2	0,2	0,2	0,2
В том числе в форме практ.подготовки	8	8	8	8
Итого ауд.	64	64	64	64
Контактная работа	64,2	64,2	64,2	64,2
Сам. работа	43,8	43,8	43,8	43,8
Итого	108	108	108	108

Программу составил(и):
к.т.н., доцент, Капустин С.А.

Рецензент(ы):
д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Организация и управление службой защиты информации

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины «Организация и управление службой
1.2	защиты информации» является изучение структуры, логической организации и
1.3	системы управления службой защиты информации как основного звена систем
1.4	защиты информации.

Задачи: определение места службы защиты информации в системе
безопасности предприятия; объяснение функций службы защиты информации;
обоснование оптимальной структуры и штатного состава службы
защиты информации в зависимости от решаемых задач и выполняемых функций;
установление организационных основ и принципов деятельности
службы защиты информации;
разрешение общих и специфических вопросов подбора, расстановки и
обучения кадров, организации труда сотрудников службы защиты информации;
раскрытие принципов, методов и технологии управления службы защиты
информации

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДЭ.07
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Экономика защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика: Преддипломная практика
2.2.3	Производственная практика: Эксплуатационная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения

ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах

ПК-9.1: Формулирование правил работы персонала со средствами защиты информации

Знать

Уровень 1	Минимальный необходимый уровень знаний формулировки правил работы персонала со средствами защиты информации
Уровень 2	Уровень знаний формулировки правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний формулировки правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, без ошибок

ПК-9.2: Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему

Уметь

Уровень 1	Продемонстрированы основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации

Владеть

Уровень 1	Имеется минимальный набор навыков сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты

	информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1					
1.1	Структура службы информационной безопасности /Лек/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Структура службы информационной безопасности /Пр/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	3
1.3	Структура службы информационно й безопасности /Ср/	6	8,8	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.4	Функции основных групп службы безопасности /Лек/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.5	Функции основных групп службы безопасности /Пр/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
1.6	Функции основных групп службы безопасности /Ср/	6	8,8	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.7	Цели и задачи службы информационной безопасности /Лек/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.8	Цели и задачи службы информационной безопасности /Пр/	6	4	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
1.9	Цели и задачи службы информационной безопасности /Ср/	6	8,8	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.10	Организационны е основы и принципы деятельности службы информационной безопасности /Лек/	6	4	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.11	Организационны е основы и принципы деятельности службы информационной безопасности /Пр/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1

1.12	Организационны е основы и принципы деятельности службы информационно й безопасности /Ср/	6	8,6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.13	Лицензирование видов деятельности службы безопасности. /Лек/	6	4	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.14	Лицензирование видов деятельности службы безопасности. /Пр/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
1.15	Лицензирование видов деятельности службы безопасности. /Ср/	6	8,8	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.16	Управление службой защиты информации. /Лек/	6	6	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.17	Управление службой защиты информации. /Пр/	6	4	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
	Раздел 2. Промежуточная аттестация					
2.1	Зачет /КА/	6	0,2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Какие задачи выполняет служба защиты информации?
2. Каковы основные принципы организации службы защиты информации?
3. Какие этапы включает в себя процесс управления службой защиты информации?
4. Какие методы и инструменты используются для организации и управления службой защиты информации?
5. Что такое риск-анализ информационной безопасности и как он проводится?
6. Какие международные стандарты и нормативные требования существуют в области информационной безопасности?
7. Какие меры физической безопасности могут быть реализованы в организации?
8. Какие методы используются для обеспечения конфиденциальности информации?
9. Каковы основные фазы планирования и развертывания службы защиты информации?
10. Какие меры принимаются для обнаружения и предотвращения внутренних угроз информационной безопасности?
11. Какова роль службы защиты информации в процессе управления инцидентами информационной безопасности?
12. Какие основные вызовы и проблемы возникают при управлении службой защиты информации?
13. Как проводится оценка эффективности работы службы защиты информации?
14. Какие требования предъявляются к персоналу службы защиты информации?
15. Каким образом ведется обучение и развитие персонала службы защиты информации?
16. Какие технологии и системы используются для защиты информации в организации?
17. Какие меры предпринимаются для обеспечения целостности и доступности информации?
18. Какие регуляторные акты и законодательство регулируют область информационной безопасности?
19. Какова роль руководителя в организации и управлении службой защиты информации?
20. Какие методы используются для оценки и управления рисками в области информационной безопасности?
21. Что такое бизнес-планирование информационной безопасности и как оно проводится?
22. Какие меры принимаются для обеспечения безопасности сетевых систем и инфраструктуры?
23. Какие основные принципы применяются при разработке политик и процедур информационной безопасности?
24. Какие стандарты и методологии используются для оценки уровня защиты информации?
25. Какие требования предъявляются к защите информации при использовании облачных сервисов?
26. Каким образом проводится аудит информационной безопасности в организации?
27. Какие меры принимаются для защиты информации при работе с внешними поставщиками услуг?
28. Как проводится управление изменениями связанными с информационной безопасностью?
29. Как организуется реагирование на инциденты и аварии в области информационной безопасности?
30. Какие методы используются для обучения сотрудников организации основам информационной безопасности?

5.2. Темы письменных работ

1. Организация службы защиты информации: принципы и методы.
2. Управление инцидентами информационной безопасности: эффективные практики и стратегии.
3. Роли и обязанности персонала службы защиты информации.
4. Аудит информационной безопасности: методологии и процедуры.
5. Управление рисками в области информационной безопасности: подходы и инструменты.
6. Планирование и развертывание службы защиты информации в организации.
7. Защита информации при использовании облачных сервисов: требования и рекомендации.
8. Физическая безопасность информации: основные меры и методы.
9. Кибербезопасность: вызовы и стратегии для организации.
10. Правовые аспекты информационной безопасности: нормативные требования и законодательство.
11. Управление изменениями в области информационной безопасности: методы и лучшие практики.
12. Обучение и развитие персонала службы защиты информации: подходы и эффективность.
13. Интеграция систем защиты информации: архитектура и методы.
14. Процессы контроля и мониторинга информационной безопасности.
15. Международные стандарты и нормативные требования информационной безопасности.
16. Эффективное управление рисками внутренних угроз информационной безопасности.
17. Роль руководителя в организации и управлении службой защиты информации.
18. Бизнес-планирование информационной безопасности: стратегии и практики.
19. Методы оценки и управления уровнем защиты информации.
20. Обеспечение безопасности сетевых систем и инфраструктуры: подходы и технологии.

5.3. Фонд оценочных средств

Совокупность аппаратных, программных и специальных компонент вычислительных сетей, реализующих функции защиты и обеспечения безопасности Что такое ядро безопасности?

1) ядро безопасности

2) информационная безопасность

3) угрозы безопасности информации

4) уязвимость информации

Понятие защищенной системы обработки информации.

1) система, использующая механическую блокировку доступа

2) система с вооруженной охраной

3) система, не имеющая доступ в сеть

4) система, отвечающая тому или иному стандарту информационной безопасности

Запрашиваемый ресурс никогда не будет получен, или может вызывать задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным - это…

1) угроза нарушения конфиденциальности

2) угроза нарушения целостности

3) угроза нарушения доступности

4) метод дисассемблирования

На каком принципе основан непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы?

1) на принципе гибкости системы

2) на принципе разумной достаточности

3) на принципе открытости алгоритмов и механизмов защиты

4) на принципе непрерывности защиты

Технические средства, математические методы, модели, алгоритмы и программы - это…

1) юридические меры защиты информации

2) организационно-правовые меры защиты информации

3) технико-математические меры защиты информации

4) политика безопасности

Состояние защищенности информации, хранимой и обрабатываемой в автоматизированной системе, от негативного воздействия на нее

1) ядро безопасности

2) информационная безопасность

3) угрозы безопасности информации

4) уязвимость информации

Совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности - это…

1) политика безопасности (Security Policy)

2) качество информации

3) уязвимость информации

4) конфиденциальность информации

Каковы возможные угрозы информационной безопасности автоматизированной системы по природе возникновения?

1) случайные

2) естественные (не зависят от человека), искусственные (деятельность человека)

3) умышленные

4) отказ системы электропитания

В чем заключается принцип разумной достаточности защиты в автоматизированной системе?

1) экономическая целесообразность и временная достаточность

2) защита только на уровне информации

3) проверка степени защищенности по факту угроз

4) минимальный штат сотрудников

Совокупность законов и других нормативно-правовых актов, с помощью которых достигается необходимая защита информации - это…

1) организационно-правовые меры защиты информации

2) технико-математические меры защиты информации

3) комплексная система защиты информации

4) юридические меры защиты информации

События или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации

1) ядро безопасности

2) информационная безопасность

3) угрозы безопасности информации

4) уязвимость информации

Понятие дискреционного или произвольного управления доступом (Discretionary Access Control).

1) возможность удаленного доступа к ресурсам

2) управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов

3) использование биометрических свойств пользователей

4) доступ без использования пароля

Каковы возможные угрозы информационной безопасности автоматизированной системы по степени преднамеренности?

1) технический персонал

2) сбой программного обеспечения

3) случайные, преднамеренные

4) отказ системы электропитания

На каком принципе основана замена средств защиты автоматизированной системы на новые в соответствии с изменившимися условиями?

1) на принципе достаточности

2) на принципе гибкости защиты

3) на принципе комплексности

4) на принципе системности

Организационно-правовая система мер необходима для…

1) организации работ по разработке системы защиты информации

2) создания баз данных

3) создания антивирусных программ

4) разработки юридических законов

Возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации

1) уязвимость информации

2) информационная безопасность

3) угрозы безопасности информации

4) ядро безопасности

Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочия доступа к ней

1) информация, доступная в течение рабочего времени

2) конфиденциальности информации

3) информация справочного характера

4) информация, доступная всем работникам данного предприятия

Каковы уровни доступа к хранимой, обрабатываемой и защищаемой автоматизированной системе информации?

1) доступность, целостность

2) администратор, пользователь

3) дискреционный, мандатный

4) носители информации, средства взаимодействия с носителями; представление информации, содержание информации

На каком принципе строится защита автоматизированной системы за счет секретности структурной организации и алгоритмов функционирования ее подсистем?

1) на принципе комплексности

2) на принципе простоты применения защитных мер

3) на принципе открытости алгоритмов защиты

4) на принципе непрерывности

Методы защиты от копирования информации:

1) отключение принтера

2) удаление из компьютера накопителей для гибких CD-дисков

3) нестандартное форматирование носителя информации.

4) архивирование файлов

Процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности Понятие защиты информации.

1) ядро безопасности

2) информационная безопасность

3) угрозы безопасности информации

4) защита информации

Понятие целостности информации.

1) размещение информации на одном носителе, сервере

2) размещение информации, доступной ограниченному числу лиц

3) свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов

4) существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

Каковы принципы построения защиты в автоматизированных системах?

1) системность, комплексность, непрерывность защиты, разумная достаточность, гибкость управления и применения, открытость алгоритмов и механизмов защиты, простота применения защитных мер и средств

2) отсутствие технического персонала

3) малые габариты устройств

4) низкая стоимость

На каком принципе интуитивно понятны и просты в использовании механизмы защиты автоматизированной системы (исключены дополнительные затраты легальных пользователей)?

1) на принципе непрерывности

2) на принципе простоты защиты

3) на принципе комплексности

4) на принципе гибкости

Шифрование, архивация, использование самогенерирующих кодов, «обман» дизассемблера - это…

1) методы защиты от копирования

2) методы защиты от дизассемблирования

3) организация мандатного доступа

4) нет верного варианта

Организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач - это…

1) автоматизированная система обработки информации

2) комплексная защита информации

3) качество информации

4) уязвимость информации

Информация становится известной тому, кто не располагает полномочиями доступа к ней - это…

1) угроза нарушения целостности

2) угроза нарушения конфиденциальности

3) угроза нарушения доступности

4) угроза нарушения непрерывности защиты

На каком принципе основана защита компьютерных систем, предполагающая необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов?

1) на принципе непрерывности защиты

2) на принципе гибкости защиты

3) на принципе системности защиты

4) на принципе разумной достаточности

Каковы виды мер обеспечения информационной безопасности в автоматизированных системах?

1) организационно-правовые, технико-математические, юридические

2) защита паролем

3) привлечение службы безопасности

4) использование антивирусных программ

С помощью каких программ осуществляют отладку и дизассемблирование?

1) электронные таблицы

2) редакторы графических изображений

3) программы-симуляторы

4) отладчики

К правовым методам, обеспечивающим информационную безопасность, относятся:
Разработка аппаратных средств обеспечения правовых данных
Разработка и установка во всех компьютерных правовых сетях журналов учета действий
Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Основными источниками угроз информационной безопасности являются все указанное в списке:
Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

Виды информационной безопасности:
Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

Цели информационной безопасности – своевременное обнаружение, предупреждение:
несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

Основные объекты информационной безопасности:
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

Основными рисками информационной безопасности являются:
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

К основным принципам обеспечения информационной безопасности относится:
Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

Основными субъектами информационной безопасности являются:
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы

Принципом информационной безопасности является принцип недопущения:
Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

Принципом политики информационной безопасности является принцип:
Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

Принципом политики информационной безопасности является принцип:
Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы

Принципом политики информационной безопасности является
принцип:
Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
-Совместимых, однотипных программно-технических средств сети, системы

К основным типам средств воздействия на компьютерную сеть
относится:
Компьютерный сбой
Логические закладки («мины»)
Аварийное отключение питания

Когда получен спам по e-mail с приложенным файлом, следует:
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес
генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его

Принцип Кирхгофа:
Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
Секретность закрытого сообщения определяется секретностью ключа

ЭЦП – это:
Электронно-цифровой преобразователь
Электронно-цифровая подпись
Электронно-цифровой процессор

Наиболее распространены угрозы информационной безопасности
корпоративной системы:
Покупка нелицензионного ПО
Ошибки эксплуатации и неумышленного изменения режима работы
системы
Сознательного внедрения сетевых вирусов

Наиболее распространены угрозы информационной безопасности
сети:
Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934814
Л1.2	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document?id=360289
Л1.3	Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: https://znanium.com/catalog/document?id=367588

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2018, URL: https://znanium.com/catalog/document?id=302894
Л2.2	Панфилова О.А., Крюкова Д.Ю., Наимов А.Н., Мухин В.В.	Информационная безопасность и защита информации: Учебное пособие	Вологда: федеральное казенное образовательное учреждение высшего образования «Вологодский институт права и экономики Федеральной службы исполнения наказаний», 2018, URL: https://znanium.com/catalog/document?id=370184

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Интернет университет информационных технологий ИНТУИТ . - Режим доступа: https://www.intuit.ru/studies/courses
Э2	Естественно-научный образовательный портал . - Режим доступа: http://www.en.edu.ru/
Э3	Федеральный центр информационно-образовательных ресурсов . - Режим доступа: http://fcior.edu.ru/
Э4	Единое окно доступа к образовательным ресурсам Единое окно доступа к образовательным ресурсам. - Режим доступа: http://window.edu.ru
Э5	Электронная библиотечная система Znanium . - Режим доступа: http://new.znanium.com/
Э6	Электронная библиотечная система Ibooks . - Режим доступа: http://www.ibooks.ru
Э7	Электронная библиотечная система BOOK.ru . - Режим доступа: http://www.book.ru
Э8	Электронные ресурсы Академии ИМСИТ . - Режим доступа: http://eios.imsit.ru/
Э9	Web-ресурс «Официальный сайт Академии ИМСИТ . - Режим доступа: http://imsit.ru

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

6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL

6.3.2. Перечень профессиональных баз данных и информационных справочных систем

6.3.2.1	Кодекс – Профессиональные справочные системы https://kodeks.ru
6.3.2.2	Консультант Плюс http://www.consultant.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
123	Кабинет информационной безопасности	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
114а	Лаборатория программно-аппаратных средств защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

	работы обучающихся)	Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	
126	Подразделение защиты информации: Лаборатория технических средств обучения	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер типа "Моноблок" с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение, комплект учебно-методической документации

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Организация и управление службой защиты информации». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только

знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Организация и управление службой защиты информации».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями