Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Северо-Западный институт управления – филиал РАНХиГС

Кафедра бизнес-информатики
(наименование кафедры)

УТВЕРЖДЕНО

Директор СЗИУ РАНХиГС
А.Д. Хлутков

ПРОГРАММА МАГИСТРАТУРЫ
Бизнес-аналитика
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса
Б1.В.ДВ.01.02 Средства защиты информации
(код и наименование РПД)

38.04.05 Бизнес-информатика
(код,наименование направления подготовки)

очная
(форма обучения)

Год набора – 2023

Санкт-Петербург, 2023г.

Автор–составитель:
Кандидат технических наук, кандидат педагогических наук, доцент, доцент кафедры бизнес-информатики Сухостат Валентина Васильевна

Заведующий кафедрой бизнес-информатики
Доктор военных наук, профессор Наумов Владимир Николаевич

РПД «Средства защиты информации» одобрена протоколом заседания кафедры бизнес-информатики № 6 от 06.03.2023 г.

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.ДВ.01.02 «Средства защиты информации» обеспечивает овладение следующими компетенциями.

Таблица 1.1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКс-2	Способен обосновывать подходы, используемые в бизнес-анализе, руководить и управлять бизнес-анализом с использованием информационно-коммуникационных технологий	ПКс-2.3	Способен реализовывать концептуальную модель бизнес-анализа BABOK

1.2.В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 1.2

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код компонента компетенции	Результаты обучения
Управление бизнес-анализом	ПКс-2.3	на уровне знаний: **Знать:** – информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; – средства и методы защиты информации в ИС предприятия на основе анализа концептуальной модели зрелости процессов компании.
		на уровне умения: **Уметь:** – определять виды и формы информации, подверженной угрозам, возможные угрозы и риски информационной безопасности; выявлять требования и ограничения информационной безопасности с учетом соответствия концептуальной модели системы; – применять средства обеспечения информационной безопасности в системах управления базами данных, компьютерных сетях на основе анализа данных, поддержки принятия решений.
		на уровне навыков: **Владеть:** – навыками использования средств защиты информации в области обеспечения защиты программ и данных при решении своих профессиональных задач.

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы /144 академ. часа.

Таблица 2

Вид работы	Трудоемкость (акад/астр.часы)
Общая трудоемкость	**144/110**
Контактная работа с преподавателем	***50/38***
Лекции	20/15
Практические занятия	28/22
Самостоятельная работа	**58/45**
Консультация	**2/1,5**
Контроль	***36/***
Формы текущего контроля	
Форма промежуточной аттестации	***Экзамен***

Место дисциплины в структуре ОП ВО

Дисциплина изучается во 2-м семестре 1-го курса. Дисциплина Б1.В.ДВ.01.01 «Средства защиты информации» относится к дисциплинам по выбору учебного плана по направлению «Бизнес-информатика» 38.04.05. Преподавание дисциплины опирается на дисциплины программы бакалавриата «Информационная безопасность», «Анализ данных», «Теория вероятностей», «Теория систем».

В свою очередь она создаёт необходимые предпосылки для освоения программ таких дисциплин, как Б1.О.05 «Управление жизненным циклом информационных систем», Б1.В.03 «Цифровая трансформация бизнеса. Инфономика», Б1.В.09 «Интеллектуальный анализ текстов и изображений».

Дисциплина закладывает теоретический и методологический фундамент для овладения умениям и навыками в ходе Б2.О.01(У) «Проектно-аналитическая практика» и Б2.О.02 (Н) «Научно-исследовательская работа».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении выпускных квалификационных работ.

3. Содержание и структура дисциплины

9. Структура дисциплины

Таблица 3

№ п/п	**Наименование тем**	**Объем дисциплины, час.**						**Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**			**СР**		
			Л/ДОТ	**ПЗ/ДОТ**	**КСР**	СРО	СП	
Тема 1	Основы безопасности автоматизированных систем предприятия	38	8/4	10/4		20		Т*
Тема 2	Средства защиты информации от несанкционированного доступа	34	6/2	8/4		20		О**
Тема 3	Методы защиты сетевых информационных технологий	34	6/2	10/4		18		Т*
Промежуточная аттестация					2*			Экзамен
Всего (акад./астр. часы):		106/82	20/15	28/22	2/1,5	58/45		36/27

Примечание:

2* - консультация, не входящая в общий объем дисциплины

Используемые сокращения:

Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся) ;

ПЗ – практические занятия (виды занятия семинарского типа за исключением лабораторных работ) ;

КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации) ;

СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях;

СП – самопроверка;

СРО – самостоятельная работа обучающегося

контрольные работы (К), опрос (О), тестирование (Т)

3.2.Содержание дисциплины

Тема 1. Основы безопасности автоматизированных систем (АС) предприятия

Проблема обеспечения безопасности АС. Место и роль АС в управлении бизнес-процессами. Основные понятия в области безопасности АС. Понятие безопасности автоматизированной информационной системы. Понятие защиты информации. Конфиденциальность, целостность, доступность. Субъекты, заинтересованные в обеспечении информационной безопасности. Уровни обеспечения информационной безопасности.

Понятие угрозы безопасности информации, АС и субъектов информационных отношений. Системная классификация угроз информационной безопасности. Понятие уязвимости АС, атаки на систему. Классификация каналов проникновения в АС и утечки информации. Неформальная модель нарушителя. Информационные риски. Управление рисками. Качественный и количественный анализ риска. Противодействие инсайдерской деятельности.

Основные принципы, меры обеспечения безопасности АС. Классификация мер и методов защиты информации. Правовые основы обеспечения безопасности АС: защищаемая информация, лицензирование, сертификация средств ЗИ и аттестация объектов информатизации. Ответственность за нарушения в сфере ЗИ.

Государственная система ЗИ. Главные направления работ по ЗИ. Структура государственной системы ЗИ. Политика безопасности организации. Способы защиты конфиденциальности, целостности и доступности в КС. Руководящие документы ФСТЭК РФ по оценке защищенности от НСД.

Тема 2. Средства защиты информации от несанкционированного доступа (НСД)

Понятие доступа, субъект и объект доступа. Понятие НСД. Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Понятие злоумышленника при решении проблем компьютерной безопасности (КБ).Назначение и возможности средств защиты информации от НСД. Основные средства и механизмы защиты АС. Компьютерные сети и управление механизмами защиты.

Аппаратно-программные средства защиты информации от НСД. Средства аппаратной поддержки, способы аутентификации. Штатные и дополнительные средства ЗИ от НСД. Системы идентификации и аутентификации: основные определения, типы, область применения, классификация. Задача идентификации пользователя. Идентификация субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Парольные системы и парольная защита. Общие подходы к построению парольных систем. Выбор паролей. Методы взлома паролей. Методы выбора паролей.

Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

Тема 3. Методы защиты сетевых информационных технологий

Типовая корпоративная сеть. Основные принципы организации сетевой защиты. Уровни информационной инфраструктуры корпоративной сети. Типичные угрозы безопасности и уязвимости сетевых информационных систем. Классификация способов несанкционированного доступа и жизненный цикл атак. Средства защиты компьютерных сетей.

Защита периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки. Туннелирование. Технология виртуальных частных сетей. Защищенные сетевые протоколы. Безопасность работы в сети Интернет. Безопасная доставка e-mail сообщений. Обнаружение и устранение уязвимостей. Сканеры безопасности. Средства анализа защищенности системного уровня.

Мониторинг событий безопасности. Классификация систем обнаружения атак.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины «Средства защиты информации» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 3.1

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Основы безопасности автоматизированных систем предприятия	Тестирование, опрос
Тема 2. Средства защиты информации от несанкционированного доступа	Тестирование, опрос
Тема 3. Методы защиты сетевых информационных технологий	Тестирование, опрос

4. 2. Типовые материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по теме 1

Типовые вопросы для опроса по теме 1

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.
2. Что понимается под риском информационной безопасности? Каковы составляющие
3. риска?
4. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа
5. и управления.
6. Каковы требования к методам оценки целесообразности затрат на обеспечение
7. безопасности АС?
8. Назовите категории затрат, связанных с безопасностью АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.
9. Дайте определение АС и безопасности АС.
10. Приведите определения информации и информационных ресурсов.
11. Перечислите категории субъектов информационных отношений.
12. Охарактеризуйте три свойства информации: конфиденциальность, целостность и доступность.
13. Сформулируйте цели защиты АС и циркулирующей в ней информации.
14. Дайте определение понятий «угроза», «уязвимость» и «атака».

15. Перечислите источники угроз ИБ.
16. Назовите каналы проникновения в автоматизированную систему и утечки информации.
17. Какие факторы лежат в основе формирования модели нарушителя?
18. Каковы цели разработки моделей угроз и нарушителей?
19. В чем разница между нарушителем и злоумышленником?
20. Перечислите основные виды мер противодействия угрозам безопасности АС. Охарактеризуйте каждую меру противодействия.
21. Перечислите достоинства и недостатки различных мер защиты.
22. Возможно ли создание идеально надежной системы защиты и почему?
23. Какие основные принципы построения систем защиты?
24. Приведите классификацию информации по достутюсти с точки зрения Федерального закона «Об информации, информационных технологиях и о защите информации».
25. Дайте определения обладателя информации и оператора информационной системы. Перечислите права и обязанности обладателя информации.
26. Что такое лицензирование? Какие виды лицензирования вам известны?
27. Для кого аттестация АИС по требованиям безопасности информации ФСТЭК России является обязательной?
28. Когда проводится аттестация АИС по требованиям безопасности информации ФСТЭК России?
29. Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.
30. Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?
31. Перечислите основные организационно-технические мероприятия в области защиты информации.
32. В чем заключаются основные задачи государственной системы защиты информации?
33. Какова структура государственной системы защиты информации? Каковы цели защиты информации?
34. В чем заключается контроль состояния защиты информации?
35. Каковы источники финансирования мероприятий по защите информации?

Типовой тест

1. Международная организация по стандартизации (ISO) под словом «система» в системе менеджмента информационной безопасности понимает:
   1) действующее устройство;
   2) приложение;
   3) процесс, программу действий или методологию.

2.Связь между индивидуальными особенностями, целями и задачами бизнеса организации при построении СМИБ обеспечивается особенным корпоративным документом:
   1) руководством BABOK;
   2) центральной концептуальной моделью по бизнес-анализу (BACCM);
   3) политикой информационной безопасности.

3.Политика информационной безопасности:
1) это система документированных управленческих решений по обеспечению ИБ организации;
2) это система документированных управленческих решений по обеспечению бизнес-процессов организации;
3) это исходный документ для разработки информационной системы организации.

4. Укажите из скольких уровней состоит общая структура нормативно-методических

документов компании в области информационной безопасности?

1) Из 1;
2) Из 3;
3) Из 5.

5. Позиция руководства в соответствии с принципами безопасности и основными бизнес-целями компании указывается в документах уровня:

1) политики ИБ;
2) частных политик, стандартов;
3) процедур, инструкций, стандартов конфигурации, журналов.

6. Аспекты информационной безопасности компании представлены в документах уровня:

1) политики ИБ;
2) частных политик, стандартов;
3) процедур, инструкций, стандартов конфигурации, журналов.

7. Методики обеспечения ИБ компании могут быть представлены документами уровня:

1) политики ИБ;
2) частных политик, стандартов;
3) процедур, инструкций, стандартов конфигурации, журналов.

8. Политика ИБ определяет:

1) стратегию ЗИ;
2) тактику ЗИ;
3) методики оперативного управления мерами снижения информационных рисков.

9.Частные политики определяют:

1) стратегию ЗИ;
2) тактику ЗИ;
3) методики оперативного управления мерами снижения информационных рисков.

10.Низкоуровневые документированные процедуры определяют:

1) стратегию ЗИ;
2) тактику ЗИ;
3) методики оперативного управления мерами снижения информационных рисков.

11. Объектам и защиты в системах и средствах информатизации и связи являются:

1) информационные ресурсы и средства и системы информатизации;
2) средства и системы информатизации и технические средства и системы;
3) информационные ресурсы, технические средства и системы и средства и системы информатизации.

12. За использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации, *Кодекс об административных правонарушениях Российской Федерации (КоАП)* устанавливает административную ответственность в виде штрафа для должностных лиц

1) 500 – 1000 руб.
2) 1000 – 2000 руб.
3) 10000 – 20000 руб.

13. К Неквалифицированной ЭП относят подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2) дает возможность определить лицо, подписавшее электронный документ;
3) содержит ключ проверки ЭП, указанный в квалификационном сертификате.

14. В Федеральном законе №63-ФЗ приведены виды электронных подписей:

1) простая

2) сложная
3) усиленная.

15. В ГОСТ Р ИСО/МЭК 15408- 2013 систематизация и классификация требований к безопасности представлена в рамках иерархии:
1) «класс» - «семейство» - «компонент» - «элемент»;
2) «семейство» - «класс» - «компонент» - «элемент»;
3) «класс» - «семейство» - «элемент» - «компонент».

16. Группа 1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всему объему информации, содержит следующее количество классов:
1) 2 класса;
2) 5 классов;
3) 6 классов.

17. Группа 2, к которой относят АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всему объему информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности, объединяет следующее количество классов:
1) 2 класса;
2) 5 классов;
3) 6 классов.

18. Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всему объему информации, размещенной на носителях одного уровня конфиденциальности содержит следующее количество классов:
1) 2 класса;
2) 5 классов;
3) 6 классов.

19. Комплекс организационно-технических мероприятий, в результате которых посредством специального документа –
1) «Аттестата соответствия»
2) «Сертификата соответствия»
3) «Знака соответствия»

подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных уполномоченными федеральными органами исполнительной власти.

20. К основным объектам банковской тайны, согласно действующему законодательству, относят:
1) банковский счет, банковский вклад;
2) банковский вклад, операции по банковскому счету;
3) банковский счет, операции по банковскому счету, банковский вклад.

Типовые оценочные материалы по теме 2

Типовые вопросы для опроса по теме 2:

1. Перечислите основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
2. В чем заключается политика безопасности организации?
3. Что такое явная и неявная компрометация ключей шифрования?
4. Какие действия должен предпринять сотрудник при компрометации ключей?
5. Каков порядок уничтожения ключей шифрования?
6. Каковы требования к пользовательским паролям ? Перечислите недостатки парольной аутентификации. Какова периодичность плановой смены пароля?

7. Охарактеризуйте в общих чертах требования к технологии антивирусной защиты.
8. О пишите алгоритм действий при обнаружении вирусов.
9. Опишите алгоритм авторизации пользователя.
10. Какие сотрудники участвуют в процессе авторизации пользователя?
11. Какова процедура авторизации? Каковы цели изготовления копий заявки об авторизации?
12. Что включает в себя физическая охрана объектов информатизации?
13. Опишите процедуру внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций системы.
14. Какие категории сотрудников имеют право внесения изменений в системное и прикладное ПО?
15. Кто имеет право вносить изменения в конфигурацию аппаратно-программных средств защиты?
16. Каков порядок экстренной :модификации технических средств?
17. Кто определяет требования к характеристикам средств защиты в разрабатываемых подсистемах?
18. Что такое фонд алгоритмов и программ?
19. Опишите порядок взаимодействия подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных подсистем.
20. Какие факторы влияют на выбор конкретных средств защиты информации?
21. Что определяет класс защищенности АС или СВТ?
22. Сколько и какие подсистемы образуют систему защищенности АС?
23. Перечислите задачи, решаемые средствами аппаратной поддержки систем защиты информации от НСД.
24. Охарактеризуйте существующие средства аппаратной поддержки
25. Какие устройства аутентификации на базе смарт-карт и/или USB-токенов вам известны?
26. Каков алгоритм аутентификации пользователя с использованием OTP-токена?
27. Что понимается под биометрической аутентификацией пользователя? Приведите примеры биометрических характеристик.
28. Охарактеризуйте стратегию безопасности Microsoft. Какие сертифицированные ФСТЭК России решения Microsoft в области безопасности вам известны? Охарактеризуйте их.
29. Каковы направления работы компании Microsoft в области биометрии?
30. Какие подходы к разграничению доступа пользователей вам известны? Кратко опишите их.
31. Опишите алгоритм работы AD RMS.
32. Какова схема работы ACS?
33. Какие средства шифрования позволяют обеспечить защиту данных от копирования и перехвата?

Тест

1. К технологии управления безопасностью НЕ предъявляют определенные требования:
    10. соответствие современному уровню развития информационных технологий;
    11. учет особенностей построения и функционирования различных подсистем АС;
    12. поддержание необходимого уровня защищенности и целостности технических средств;

2. Какие угрозы, основанные на ошибках сотрудников структурных подразделений, могут быть использованы злоумышленниками для нанесения вреда организации и ее сотрудникам?

1) Разглашение конфиденциальной информации (сведений, составляющих коммерческую тайну организации, персональных данных, паролей и др.).

2) Заражение рабочих станций вирусами, «троянскими» и другими вредоносными программами (внедрение шпионских кодов).
3) Потеря конкурентных преимуществ в результате разглашения сведений, составляющих коммерческую тайну.

3. К обеспечению безопасности информационных технологий организации должны привлекаться:
1) все сотрудники, участвующие в процессах автоматизированной обработки информации;
2) все категории обслуживающего АС персонала;
3) все категории посторонних лиц.

4. К событиям явной компрометации ключей НЕ относится:
1) утрата ключевого носителя;
2) нарушение печати на сейфе с ключевыми носителями;
3) утрата ключевого носителя с последующим обнаружением.

5. Правила парольной защиты:
1) регламентируют контроль над действиями пользователей при работе с паролями;
2) определяют требования к организации защиты автоматизированной системы от разрушающего воздействия вредоносного ПО;
3) регламентируют организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в автоматизированной системе.

6. Категорирование защищаемых ресурсов АС- необходимый элемент организации работ по обеспечению безопасности информации - предполагает:
1) типизацию принимаемых контрмер;
2) установление градаций важности (категорий) обеспечения защиты ресурсов;
3) отнесение конкретных ресурсов к соответствующим категориям.

7. Категория конфиденциальности защищаемой информации:
1) открытая;
2) высокая;
3) средняя.

8. Категория целостности защищаемой информации:
1) открытая;
2) высокая;
3) средняя.

9. Категория доступности функциональных задач:
1) открытая;
2) высокая;
3) средняя.

10. Авторизация пользователей осуществляется с применением следующих механизмов реализации разграничения доступа:
1) избирателъного управлеиия доступом с помощью атрибутивных схем, списков разрешений и т. п.;
2) полномочиого управлеиия доступом с помощью меток конфиденциальности ресурсов и уровней допуска пользователей;
3) регистрации факта попытки доступа и его параметров в системном журнале (в том числе НСД с превышением полномочий).

11. При регистрации событий безопасности в системном журнале обычно фиксируют следующую информацию:
1) дату и время события;
2) идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
3) извещение владельца информации о НСД к его данным.

12. К числу недостатков криптографических методов относят:

1) значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
2) обеспечение высокой гарантированной стойкости защиты;
3) высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены;

Типовые оценочные материалы по теме 3
Типовые вопросы для опроса по теме 3:
1. Охарактеризуйте уровни информационной инфраструктуры корпоративной сети.
2. Дайте определения угрозы, уязвимости и атаки. Охарактеризуйте на примерах взаимосвязь между этими понятиями.
3. Приведите классификационные схемы уязвимостей и атак.
4. Какой из механизмов реализации сетевых атак наиболее сложен с точки зрения обнаружения?
5. Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?
6. Какие средства защиты сетей вам известны?
7. Почему необходимо защищать периметр корпоративной сети?
8. Перечислите составляющие механизма защиты периметра сети.
9. Что такое демилитаризованная зона в применении к компьютерным сетям?
10. Дайте определение понятия межсетевого экрана. В чем заключается его функция?
11. Перечислите основные типы межсетевых экранов. Охарактеризуйте функции МЭ каждого типа, их достоинства и недостатки.
12. В чем состоит главный недостаток пакетных фильтров – разновидности межсетевых экранов?
13. В чем разница между обычным пакетным фильтром и пакетным фильтром с контролем состояния «stateful» ?
14. В чем разница между пакетным фильтром с контролем состояния «stateful», и классическим посредником сеансового уровня?
15. Каковы особенности анализа содержимого электронной почты?
16. Перечислите критерии фильтрации содержимого электронной почты.
17. Каковы особенности анализа содержимого HTTP-трафика?
18. В чем особенности распределенной архитектуры систем управления уязвимостями?
19. Какие задачи могут быть решены сетевым сканером безопасности?
20. Перечислите типы проверок, используемых в сетевых сканерах безопасности
21. Какую дополнительную критичную информацию может получить злоумышленник в результате сканирования портов?
22. Какая причина затрудняет использование в организациях сетевых сканеров безопасности?
23. Дайте определение инфраструктуры управления журналами событий.
24. Перечислите категории журналов событий.
25. Дайте характеристику протоколов syslog и SEM.
26. Опишите классификационные схемы систем обнаружения атак.
27. Какие механизмы реагирования на атаки вам известны?

Тест
1. Аналитик оценки:
1) измеряет и оценивает свидетельства оценки, предоставленными владельцами активов;
2) выбирает способ, модель оценки и определяет методику оценки ИБ;
3) проводит анализ результатов оценки и формирует отчет и рекомендации по результатам оценки.

2. Процедура страхования информационных рисков состоит из _____ этапов:
   1) 3;
   2) 4;
   3) 5.
3. Основные типы аппаратно-программных средств аутентификации:
   1) на базе смарт-карт и USB-токенов;
   2) на базе пассивных контактных и бесконтактных идентификаторов;
   3) 1) и 2).
4. Биометрические методы идентификации подразделяют на группы:
   1) статические;
   2) мобильные;
   3) динамические.
5. К статическим биометрическим методам идентификации относится распознавание:
   1) по отпечаткам пальцев;
   2) по радужной оболочке глаз;
   3) по клавиатурному почерку.
6. К динамическим биометрическим методам идентификации относится распознавание:
   1) по отпечаткам пальцев;
   2) по радужной оболочке глаз;
   3) по клавиатурному почерку.
7. К разграничению доступа существует _____ подхода:
   1) 2
   2) 3
   3) 4
8. Подключение к сетям общего пользования осуществляется организациями для решения следующих задач:
   1) обеспечить взаимодействие с удаленными филиалами и отделениями;
   2) организовать доступ к ресурсам внутренней сети мобильных пользователей;
   3) 1)и 2).
9. Корпоративная сеть - сложная система, состоящая из нескольких взаимодействующих уровней, или «слоев». Это:
   1) персонал, приложения, система управления базами данных;
   2) сеть, операционная система, система управления базами данных, персонал;
   3) приложения, система управления базами данных, сеть, операционная система, персонал.
10. Любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы называется ….
11. Действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей информационной системы называется …..
12. Классификация уязвимостей по методике CVSS:
   1) базовые, временные, связанные со средой;
   2) базовые, преходящие, связанные со средой;
   3) основные, временные, связанные со средой.
13. С точки зрения защищаемых ресурсов МЭ классифицируют как:
   1) периметровые или сетевые (network-based, защищающие целую сеть);
   2) персональные (host-based, контролирующие трафик отдельного узла);
   3) специализированные МЭ (например, для веб-приложений, виртуальных инфраструктур).
14. Недостатками электронной корпоративной почты являются:
   1) создания ситуации отказа в обслуживании и пересылки вирусов в сообщении или в прикрепленных файлах;

2) пересылки конфиденциальной информации и информации неэтичного характера и использования электронной почты в личных целях;
3) 1)и 2).

15. Критериями фильтрации для средств анализа содержимого электронной почты НЕ являются:
1) пересылка информации через веб-интерфейс;
2) подлинность адреса отправителя;
3) наличие вирусов.

16. С HTTP-трафиком НЕ связаны угрозы:
1) опасное «содержимое» - мобильный код, вирусы;
2) пересылка информации через веб-интерфейс;
3) наличие вирусов.

17. Критерием фильтрации HTTP-трафика НЕ является:
1) наличие вирусов;
2) использование трафика в личных целях;
3) URL.

18. Для организации связей между филиалами одной организации используются:
1) межкорпоративиые VPN (Extranet VPN);
2) VPN с удаленным доступом (Remote Access VPN);
3) внутрикорпоративные VPN (Intranet VPN).

19. Для организации доступа к корпоративной сети мобильных сотрудников используются:
1) межкорпоративиые VPN (Extranet VPN);
2) VPN с удаленным доступом (Remote Access VPN);
3) внутрикорпоративные VPN (Intranet VPN).

20. Для организации организации связей с партнерами и клиентами используются:
1) межкорпоративиые VPN (Extranet VPN);
2) VPN с удаленным доступом (Remote Access VPN);
3) внутрикорпоративные VPN (Intranet VPN).

21. Задание. «Построение модели угроз ИБ».

Провести идентификацию, анализ и описание основных угроз ИБ для конкретного объекта защиты по выбору обучающегося. Выбор объекта защиты согласовывается с преподавателем. Для каждой угрозы должны быть указаны активы, которым может быть нанесен ущерб в случае ее реализации, источник угрозы, факторы, способствующие возникновению и реализации угрозы ИБ, возможные последствия.

На основании модели угроз построить модель нарушителя, в которой отражаются его практические и теоретические возможности, время, место действия и другие характеристики - важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Результаты анализа должны быть структурированы и оформлены в виде отчета в среде MS Word.

Выполненное задание защищается преподавателю.

22. Задание. «Оценка риска ИБ».

Для объекта защиты, выбранного в контрольном задании 1, провести анализ и оценивание рисков ИБ, соответствующих описанным угрозам. Для каждой угрозы ИБ должны быть определены (качественно или количественно) уровень угрозы (вероятность реализации угрозы) и размер возможного ущерба (уровень негативных последствий). На основании этих значений производится определение уровня риска, ранжирование рисков и выявление критических рисков. Должны быть представлены используемые при оценке шкалы. Результаты оценки рисков оформляются в виде отчета в среде MS Word.
Выполненное задание защищается преподавателю.

5.Оценочные материалы промежуточной аттестации по дисциплине

5.1. Экзамен проводится с применением следующих методов и средств: устный опрос, тестирование, решение задач.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Показатель оценивания	Критерий оценивания
ПКс-2.3	Реализует концептуальную модель бизнес-анализа BABOK	Использует ключевые компетенции модели BACCM для решения задач в области информационной безопасности. Самостоятельно определяет потребности и рекомендации решений, которые обеспечивают ценность для заинтересованных лиц в рамках задач взаимодействия областей информационной безопасности и бизнеса

Для оценки сформированности компетенций, знаний и умений, соответствующих данным компетенциям, используются контрольные вопросы, а также задачи.

Типовые оценочные материалы промежуточной аттестации

Вопросы к экзамену по дисциплине «Средства защиты информации»

1) Актуальность решения проблемы обеспечения безопасности автоматизированных систем.
2) Вредоносное программное обеспечение. Классификация вредоносных программ.
3) Методы и средства антивирусной защиты.
4) Парольная защита. Общие подходы к построению парольных систем.
5) Системы идентификации и аутентификации: основные определения, типы, область применения, классификация.
6) Конфиденциальность, целостность, доступность. Ролевое управление доступом.
7) Дискреционное и мандатное управление доступом.
8) Понятие угрозы информационной безопасности. Основные виды и источники угроз информационной безопасности.
9) Понятие уязвимости информационной системы, атаки на систему.
10) Цифровая стеганография. Определения и методы цифровой стеганографии.
11) Стегосистема. Области применения компьютерной стеганографии.
12) Понятия и определения современной криптографии. Стойкость криптоалгоритмов.
13) Классификация криптографических алгоритмов.
14) Персональные данные. Защита персональных данных
15) Алгоритмы электронной подписи. Хеширование.
16) Государственное регулирование в сфере информационной безопасности.
17) Защищенная электронная подпись. Цифровые сертификаты.
18) Компьютерные преступления.
19) Этапы процесса осуществления атаки на информационную систему. Классификация систем обнаружения атак.

20) Способы противодействия несанкционированному сетевому и межсетевому доступу.
21) Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
22) Безопасность работы в сети Интернет. Основные угрозы при работе в Интернет.
23) Безопасная доставка e-mail сообщений.
24) Обеспечение информационной безопасности на государственном уровне.
25) .Обеспечение информационной безопасности на уровне предприятия.
26) Классификация тайн.
27) Правовые основания отнесения сведений к категории ограниченного доступа.
28) Институт стандартизации сферы информационной безопасности.
29) Национальные стандарты в области информационной безопасности и защиты информации.
30) Международные стандарты в области информационной безопасности и защиты информации.
31) Электромагнитный спектр как источник воздействия на информацию.
32) Каналы силового деструктивного воздействия (СДВ) на информацию.
33) Рекомендации по защите компьютерных систем от СДВ.
34) Классификация технических каналов утечки информации.
35) Модель и способы утечки по радиоканалу.
36) Модель и способы утечки по электрическому каналу.
37) Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу.
38) Модель и способы утечки по оптическому (оптико-электронному) каналу.
39) Модель и способы утечки по каналу ПЭМИН.
40) Классификация угроз несанкционированного доступа (НСД) к информации.
41) Категории нарушителей безопасности информации и их возможности.
42) Общая характеристика уязвимостей.
43) Способы реализации угрозы НСД к информации.
44) Понятие и обобщенная модель нетрадиционного информационного канала.
45) Методы сокрытия информации в текстовых файлах.
46) Методы сокрытия информации в графических файлах.
47) Методы сокрытия информации в звуковых файлах.
48) Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
49) Историография и классификация шифров.
50) Примеры криптографических алгоритмов.
51) Криптосистема с симметричными и несимметричными ключами.
52) Электронная цифровая подпись.
53) Мандатная и дискреционная модели доступа.
54) Процедура идентификации, аутентификации и авторизации.
55) Система паролирования.
56) Системы контроля и управления доступом.
57) Система охраны периметра.
58) Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
59) Понятие и функционал DLP-систем.
60) Объем и структура данных защищаемых DLP-системами.

Шкала оценивания

Оценка результатов производится на основе Положения о текущем контроле успеваемости обучающихся и промежуточной аттестации обегающихся по образовательным программам среднего профессионального и высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академии народною хозяйства и государственной службы при Президенте Российской Федерации», утвержденного Приказом Ректора РАНХиГС при Президенте РФ от 30.01.2018 г. № 02-66 (п.10 раздела 3 (первый абзац) и п.11), а также Решения Ученого совета Северо-западного института управления РАНХиГС при Президенте РФ от 19.06.2018, протокол № 11.

Оценка «отлично» выставляется в случае, если при устном ответе студент проявил (показал):

- глубокое и системное знание всего программного материала учебного курса, изложил ответ последовательно и убедительно;
- отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей дисциплины;
- умение правильно применять теоретические положения при решении практических вопросов и задач;
- умение самостоятельно выполнять предусмотренные программой задания;
- навык обоснования принятого решения.

Оценки «хорошо» выставляется в случае, если при устном ответе студент проявил (показал):

- знание узловых проблем программы и основного содержания лекционного курса;
- умение пользоваться концептуально-понятийным аппаратом умение преимущественно правильно применять теоретические положения при решении практических вопросов и задач,
- умение выполнять предусмотренные программой задания;
- в целом логически корректное, но не всегда точное и аргументированное изложение ответа.

Оценки «удовлетворительно» выставляется в случае, если при устном ответе студент проявил (показал):

- фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины;
- затруднения с применением теоретических положений при решении практических вопросов и задач,

Оценка «неудовлетворительно» выставляется в случае, если при устном ответе студент проявил (показал):

- незнание либо отрывочное представление учебно-программного материала;
- неумение использовать научно-понятийный аппарат и терминологию учебной дисциплины;
- неумение применять теоретические положения при решении практических вопросов и задач,
- неумение выполнять предусмотренные программой задания.

6. Методические материалы для освоения дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия. На лекциях рассматриваются наиболее сложный материал дисциплины. Для развития у магистрантов креативного мышления и логики в

каждой теме учебной дисциплины предусмотрены теоретические положения, инструментальные средства, а также примеры их использования при решении задач обеспечения информационной безопасности. Кроме того, часть теоретического материала предоставляется на самостоятельное изучение по рекомендованным источникам для формирования навыка самообучения.

Практические занятия предназначены для самостоятельной работы магистрантов по решению конкретных задач. Каждое практическое занятие сопровождается заданиями, выдаваемыми магистрантам для решения во внеаудиторное время.

Для работы с печатными и электронными ресурсами СЗИУ имеется возможность доступа к электронным ресурсам. Организация работы магистрантов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

Методические указания для обучающихся по освоению дисциплины

Обучение по дисциплине «Средства защиты информации» предполагает изучение курса на аудиторных занятиях (лекции, практические работы) и самостоятельной работы обучающихся. Семинарские занятия дисциплины «Средства защиты информации» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

- внимательно прочитайте материал предыдущей лекции;
- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
- ознакомьтесь с учебным материалом по рекомендуемой литературе;
- постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
- запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим занятиям:

- внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом;
- ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
- уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;
- готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;
- рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

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

7.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее

образование). — ISBN 978-5-534-14590-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/477968.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/469235.
3. Основы управления информационной безопасностью : учебное пособие : Допущено УМО ... / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва: Горячая линия-Телеком, 2016.- 244 с. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр.: с. 234-239. - ISBN 978-5-9912-0361-6.
4. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/476798.

Все источники основной литературы взаимозаменяемы.

7.2 Дополнительная литература

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 03.08.2021). – Режим доступа: по подписке.
2. Дронов В.Ю. Международные и отечественные стандарты по информационной безопасности : учебно-методическое пособие / Дронов В.Ю.. — Новосибирск : Новосибирский государственный технический университет, 2016. — 34 с. — ISBN 978-5-7782-3112-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91395.html (дата обращения: 03.08.2021). — Режим доступа: для авторизир. Пользователей
3. Гасанов Э.С. Самарина Е.А. Управление информационной безопасностью в корпоративной предпринимательской среде в условиях киберугроз цифровой экономики [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/

7.3.Нормативные правовые документы и иная правовая информация

Не используются

7.4. Интернет-ресурсы.

СЗИУ располагает доступом через сайт научной библиотеки http://nwapa.spb.ru/
к следующим подписным электронным ресурсам:
https://ranalytics.github.io/tsa-with-r/ch-intro-to-prophet.html

Русскоязычные ресурсы

Электронные учебники электронно - библиотечной системы (ЭБС) «Айбукс»
Электронные учебники электронно – библиотечной системы (ЭБС) «Лань»
Рекомендуется использовать следующий интернет-ресурсы
http://serg.fedosin.ru/ts.htm
http://window.edu.ru/resource/188/64188/files/chernyshov.pdf

7.5. Иные источники.

Не используются.

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

Учебная дисциплина включает использование программного обеспечения Microsoft Excel, Microsoft Word, для подготовки текстового и табличного материала.

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

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование
1.	Компьютерные классы с персональными ЭВМ, объединенными в локальные сети с выходом в Интернет
1.	Пакет Excel -2016, proffesional plus, IBM SPSS statistics, R, RStudio, Anaconda
2.	Мультимедийные средства в каждом компьютерном классе и в лекционной аудитории
3.	Браузер, сетевые коммуникационные средства для выхода в Интернет. Сервисы и службы Azure

Компьютерные классы из расчета 1 ПЭВМ для одного обучаемого. Каждому обучающемуся должна быть предоставлена возможность доступа к сетям типа Интернет в течение не менее 20% времени, отведенного на самостоятельную подготовку.