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.01.01 Управление информационной безопасностью
(код и наименование РПД)

38.04.05 Бизнес-информатика
(код,наименование направления подготовки)

очная
(форма обучения)

Год набора – 2022

Санкт-Петербург, 2022г.

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 «Управление информационной безопасностью» одобрена протоколом заседания кафедры бизнес-информатики № 9 от 04.07.2022 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся
5. Оценочные материалы промежуточной аттестации по дисциплине
6. Методические материалы для освоения дисциплины
7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"
   7.1. Основная литература
   7.2. Дополнительная литература
   7.3. Нормативные правовые документы и иная правовая информация
   7.4. Интернет-ресурсы
   7.5. Иные источники
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

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

1.1. Дисциплина Б1.В.ДВ.01.01 «Управление информационной безопасностью» 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	Реализовывает концептуальную модель бизнес-анализа BABOK

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:** – области знаний для выполнения задач классификации активов предприятия, угроз и уязвимостей информационной безопасности бизнес-аналитиком; – виды архитектур предприятия, знать концептуальную модель зрелости процессов компании для обеспечения информационной безопасности.
		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 программные средства анализа данных, поддержки принятия решений для решения задач обеспечения информационной безопасности предприятия.
		на уровне навыков: **Владеть:** – навыками разработки политик информационной безопасности, методами анализа, оценки зрелости процессов информационной безопасности компании на базе концептуальной модели по бизнес-анализу.

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 «Управление информационной безопасностью» относится к выбору дисциплинам 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

3.1.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 управления информационной безопасностью предприятия.	38	8	10/4		20		Т*
Тема 2	Система менеджмента информационной безопасности	34	6	8/4		20		О**
Тема 3	Управление рисками и оценка информационной безопасности компании	34	6	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 управления информационной безопасностью предприятия

Основные направления обеспечения информационной безопасности организации. Риск-ориентированный подход. Понятие корпоративной политики безопасности. Основные требования и подходы к разработке политики безопасности. Многоуровневый подход.

Управления информационной безопасностью на основе соответствий требованиям (compliance management). Анализ упущений (gap-анализ). Модель непрерывного совершенствования (замкнутый цикл менеджмента PDCA).

Процессный подход к обеспечению информационной безопасности. Суть процессного подхода. Классификация и атрибуты процессов. Процессы управления и обеспечения информационной безопасности. Эталонная модель процесса для управления ИБ (ГОСТ Р 57640-2017, ISO/IEC TS 33052:2016). Проблемы внедрения процессного подхода.

Тема 2. Система менеджмента информационной безопасности

Уровни организации деятельности по обеспечению информационной безопасности компании, и общая структура стандартов информационной безопасности. Оценочные стандарты информационной безопасности («Оранжевая книга», ITSEC, ISO/IEC 15408 «Общие критерии»). Статус стандартов ISO/IEC в РФ.

«Лучшие практики» информационной безопасности (стандарты BSI, BS 7799 / ISO/IEC 17799, 27002).

Стандарты менеджмента информационной безопасности. Состав и структура серии международных стандартов ISO/IEC 2700x. Российские гармонизированные стандарты.

Национальные стандарты и стандарты саморегулируемых организаций в сфере управления информационной безопасностью и информационными технологиями (BS-100, NIST 800, ITIL, ISM 3, Cobit). Сервис-ориентированный и процессно-ориентированный подходы к управлению ИБ и ИТ. Концепция корпоративного управления информационной безопасностью (IS Governance).

Эволюция модели информационной безопасности.

Построение системы менеджмента информационной безопасности (СМИБ) на основе ISO/IEC 27001. Организационная структура системы менеджмента информационной безопасности. Система частных менеджментов. Сертификация соответствия СМИБ ISO/IEC 27001.

Тема 3. Управление рисками и оценка информационной безопасности компании

Риск как объект управления. Управление рисками информационной безопасности на основе ISO 27005. Управление рисками на основе ГОСТ Р ИСО 31000. Методы анализа риска ГОСТ Р ИСО/МЭК 31010. Процедуры оценки и обработки рисков. Методология оценки рисков ИБ.

Виды и способы оценки информационной безопасности. Процесс оценки (аудита) ИБ. Метрики информационной безопасности (ISO/IEC 27004, NIST 800-55).

Оценка процессов информационной безопасности на основе моделей зрелости (ГОСТ Р ИСО/МЭК 33020-2017, ISO 21827, ISO 15504).

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины «Предсказательная аналитика» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 3.1

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Основы управления информационной безопасностью предприятия	Тестирование, опрос
Тема 2. Система менеджмента информационной безопасности	Тестирование, опрос
Тема 3. Управление рисками и оценка информационной безопасности компании	Тестирование, опрос

4. 2. Типовые материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по теме 1

Типовые вопросы для опроса по теме 1

1. В чем заключается традиционный взгляд на информационную безопасность?
2. Охарактеризуйте сущность политики информационной безопасности компании.
3. Что лежит в основе риск-ориентированного подхода к обеспечению информационной безопасности?
4. Каково предназначение и средства разведочный Прогнозирование временных рядов? Дайте характеристику диаграммы «ящик с усами»
5. Назовите какие операции выполняются при агрегировании данных.
6. Приведите примеры использования статистических пакетов для разведочного анализа.
7. Назовите и выполните сравнительный анализ графических средств анализа. Дайте характеристику биржевых диаграмм.

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.Менеджмент на основе соответствия (Compliance management) – это

1) **управление, основанное на соблюдении требований внешних и внутренних нормативных актов;**
2) **управление, основанное на соблюдении требований внешних нормативных актов;**
3) **управление, основанное на соблюдении требований внутренних нормативных актов.**

12.Подход к оценке соответствия включает следующие этапы gap-анализа:

1) **определение состояния «Как должно быть» (To-be);**
2) **определение состояния «Как есть» (As-is);**
3) **разработка плана перехода;**
4) **эксплуатация системы.**

13.На стадии определения состояния «Как должно быть»

1) **выявляют объекты защиты в терминах управления рисками;**
2) **очерчивают границы, в рамках которых будет выстраиваться СМИБ;**
3) **разрабатывают частные политики или процедуры.**

14.Стандартный подход ISO к построению СМИБ основан на модели PDCA. Какие элементы соответствуют модели PDCA?.

1) **планирование (Plan);**
2) **изменение (Change);**
3) **выполнение (Do);**
4) **решение (Solution);**
5) **проверка (Check);**
6) **совершенствование (Akt).**

15. Результатом анализа упущений (gap-analysis) является:
1) создание списка несоответствий;
2) **пересмотр целевых состояний («Как должно быть»);**
3) **выработка рекомендаций по устранению несоответствий;**
4) **определение «плана перехода».**

16.Стандарты ИБ условно разделяются на:
1) **информационные, технологические, оценочные;**
2) **технологические, оценочные, «лучшие практики» и стандарты управления ИБ;**
3) **«лучшие практики» и стандарты управления ИБ, технические, оценочные.**

17.В сферу стратегического управления ИБ (Governance) в Cobit 5 входят:
1) **контроль продуктивности (Monitor);**
2) **разграничение зон стратегического управления (Governance) и текущего управления (Management);**
3) **определение стратегического направления (Direct);**
4) **оценка потребностей всех заинтересованных сторон (Evaluate).**

18.Основными принципами Cobit 5 for IS являются:
1) **защита бизнеса;**
2) **поддержка бизнеса;**
3) **согласованность стратегии ИБ и бизнеса;**
4) **поощрение ответственного поведения в сфере ИБ.**

19.Определенный набор различных видов деятельности, которые в совокупности создают результат (продукт, в том числе информационный), имеющий ценность для конечного потребителя (клиента, заказчика) – это
1) **бизнес-система;**
2) **клиент процесса;**
3) **бизнес-процесс.**

20….– это методология, идентифицирующая процессы в организации так, чтобы их взаимосвязи были понятны, видимы и измеримы, а итоговая совокупность процессов понималась как единая система реализации деятельности организации.
1) **Процессный подход;**
2) **Многоуровневый подход;**
3) **Риск-ориентированный подход.**

Ключи:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
3)	3)	1)	2)	1)	2)	3)	1)	2)	3)
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
1)	1),2),3)	1), 2)	1),3),5),6)	4)	2)	1),3),4)	1),2),4)	3)	1)

Типовые оценочные материалы по теме 2
Типовые вопросы для опроса по теме 2:

1. Что понимается под управлением бизнес-процессами? Его цели.
2. Что в себя включает менеджмент?
3. Из каких подсистем состоит система менеджмента?
4. Что является областью действия системы менеджмента?

5. Назовите элементы системы менеджмента.
6. Что включает в себя управление ИБ?
7. Чем является СМИБ по отношению к системе менеджмента организации согласно ISO/IEC 27001?
8. В чем заключается цикл модели PDCA для СМИБ?
9. Перечислите шаги этапа планирования СМИБ в соответствии с требованиями стандарта ISO/IEC 27001.
10. Дайте характеристику этапу планирования СМИБ согласно ISO/IEC 27001.
11. Охарактеризуйте аспекты анализа выбранной области деятельности организации, которая будет охвачена СМИБ.
12. Когда следует начинать работы по созданию СМИБ?
13. Какие ключевые процессы должны быть охвачены разрабатываемыми и реализуемыми политиками?
14. Какой стандарт подробно описывает запуск, планирование и определение проекта внедрения СМИБ?
15. Какие процедуры контроля устанавливаются на этапе реализации СМИБ?
16. Дайте характеристику организационной структуре и основным принципам СМИБ.
17. Дайте характеристику этапам подготовки к сертификации СМИБ компании на соответствие требованиям ISO/IEC 27001.
18. В чем заключается мониторинг и измерения безопасности для СМИБ компании?
19. С какой целью вводится процесс измерения в цикл СМИБ проекта или организации?
20. Что должно создавать основу для формирования решений по совершенствованию СМИБ организации?

Тест

1. На верхнем уровне управления организацией управление бизнес-процессами предполагает реализацию … целей. Выберите:
   1) тактических;
   2) стратегических;
   3) операционных.
2. Стратегия управления определяет:
   1) направление и способ использования средств для достижения поставленной цели;
   2) методы и приемы для достижения поставленной цели в конкретных условиях;
   3) повышение эффективности и продуктивности бизнес-процессов.
3. Система менеджмента состоит из
   1) управляемой подсистемы (объекта управления);
   2) управляемой подсистемы (субъекта управления);
   3) управляющей подсистемы (объекта управления);
   4) управляющей подсистемы (субъекта управления).
4. Управление ИБ – это циклический процесс, **НЕ** включающий:
   1) осознание степени необходимости защиты информации и постановку задач;
   2) сбор и анализ данных о состоянии ИБ в организации;
   3) организационную структуру.
5. В качестве входных данных СМИБ использует:
   1) требования в области ИБ;
   2) ожидания заинтересованных сторон;
   3) результаты обеспечения ИБ.
6. Стандарт ISO/IEC 27001 сертифицирует:
   1) процесс;

2) компанию;

3) систему защиты.

7. Граница СМИБ по отношению к системе управления непрерывностью бизнеса (Business continuity management - BCM) очерчивается выражением:

1) $СМИБ \subseteq BCM$;

2) $СМИБ \supset BCM$;

3) $СМИБ \cap BCM$ **= защита критичных бизнес-процессов организации от крупных сбоев и аварий ИС;**

8. Область действия СМИБ включает в себя:

1) все бизнес-процессы организации;

2) некоторые бизнес-процессы организации;

3) определенные бизнес-процессы организации.

9. Разрабатываемые и реализуемые политики безопасности должны охватывать ключевые процессы:

1) основных бизнес-процессов организации;

2) инфраструктурных процессов организации;

3) бизнес-процессов управления организации;

4) процессов развития.

10. К процедурам контроля **НЕ** относится:

1) мониторинг и проверка осуществления защитных мер;

2) регулярный пересмотр оценки риска через запланированные промежутки времени;

3) модернизация СМИБ.

11. Директор по ИБ организации согласно ISO/IEC 27001:

1) решает стратегические задачи компании;

2) способствует развитию бизнеса в русле направления ИБ;

3) несет ответственность за процессы управления в области ИБ.

12. Подготовка сотрудников организации: обучение, тренинги, повышение осведомленности входит:

1) в работы по внедрению механизмов контроля;

2) в работы по оценке информационных рисков;

3) в работы по предварительному аудиту СМИБ.

Ключи:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
2)	1)	1), 4)	3)	1), 2)	1)	3)	3)	3)	3)	1), 2)	1)

Типовые оценочные материалы по теме 3

Типовые вопросы для опроса по теме 3:

1. Дайте определение риска как возможности.
2. Охарактеризовать риск как опасность или угрозу.
3. Дайте характеристику риску как неопределенности.
4. В рамках какой концепции рассматриваются риски информационной безопасности. Какова цель управления в данном случае?
5. Какой подход принят к определению риска в стандартах управления рисками информационной безопасности?
6. Виды рисков, их особенности.
7. Охарактеризуйте функции риска в предпринимательской деятельности.
8. Кого относят к субъектам риска? Назовите уровни субъектов, для которых возникает экономический риск.
9. Какие подходы существуют к классификации рисков?

10. Дать характеристику типам предпринимательского риска по уровню принятия решений, по источнику риска в бизнесе, по возможности управления и в зависимости от возможного результата риска.

11. Привести классификацию рисков в зависимости от основной причины возникновения.

12. Дать характеристику информационным, коммерческим и финансовым рискам.

13. В чем заключается сущность управления риском?

14. Назовите методы, на основе которых осуществляется управление риском.

15. Дайте характеристику концепции минимизации риска.

16. Назовите основные положения концепции приемлемого риска.

17. Дайте характеристику концепции риска как ресурса.

18. Принципы управления рисками на основе ГОСТ Р ОСО 31000.

19. Управление рисками информационной безопасности на основе ISO 27005.

20. Назовите цель и виды оценки ИБ. Процесс оценки ИБ.

21. Дайте характеристику эволюционной модели зрелости процессов информационной безопасности.

Тест

1. Риски информационной безопасности рассматриваются в рамках концепции
   1) риска как возможности;
   2) риска как опасности;
   3) риска как неопределенности.
2. При описании риска указывается:
   1) в чем заключается его влияние на бизнес;
   2) насколько вероятно возникновение данного рискового события;
   3) 1)и 2).
3. Тяжесть ущерба как негативное влияние на бизнес-деятельность компании описывается:
   1) информационными активами;
   2) уязвимостями;
   3) угрозами ИБ.
4. Вероятность возникновения угрозы с учетом принимаемых мер ЗИ описывается:
   1) информационными активами;
   2) уязвимостями;
   3) существующими мерами снижения риска.
5. Простота и возможность обойтись минимальными затратами ресурсов при проведении анализа и контроля рисков является преимуществом:
   1) стратегии базовой безопасности;
   2) стратегии неформального анализа;
   3) стратегии полного анализа риска.
6. Экспертная оценка величины рисков – преимущество:
   1) стратегии базовой безопасности;
   2) стратегии неформального анализа;
   3) стратегии комбинированного анализа риска.
7. Проведение высокоуровнего анализа рисков – преимущество:
   1) стратегии полного подробного анализа риска;
   2) стратегии неформального анализа рисков;
   3) стратегии комбинированного анализа риска.
8. Процесс менеджмента рисков ИБ НЕ включает:
   1) подготовку документации СМИБ к сертификации;
   2) определение контекста;
   3) информирование о рисках.
9. Оценка рисков – это общий процесс

1) анализа и оценивания рисков;
2) идентификации и определения величины рисков;
3) присвоение значений вероятности и последствий риска.

10. Анализ рисков состоит;
    1) из идентификации рисков;
    2) из определения величины (уровня) рисков;
    3) из ранжирования рисков.
11. Оценка ИБ заключается в выработке оценочного суждения относительно:
    1) отлаженности процессов обеспечения ИБ;
    2) адекватности используемых защитных мер;
    3) целесообразности инвестиций для обеспечения необходимого уровня ИБ;
    4) 1), 2), 3).
12. Результатом способа оценки соответствия (compliance) ИБ является:
    1) оценка способности организации эффективно управлять рисками ИБ для достижения своих целей;
    2) оценка необходимости обеспечения или совершенствования ИБ на сонове критериев получаемой выгоды, преимуществ и затрат для бизнеса;
    3) оценка степени соответствия системы ЗИ эталону и предложения по устранению недостатков.
13. Риск-ориентированная оценка ИБ организации – это:
    1) оценка способности организации эффективно управлять рисками ИБ для достижения своих целей;
    2) оценка необходимости обеспечения или совершенствования ИБ на сонове критериев получаемой выгоды, преимуществ и затрат для бизнеса;
    3) оценка степени соответствия системы ЗИ эталону и предложения по устранению недостатков.
14. Оценка ИБ на основе экономических показаетелей – это:
    1) оценка способности организации эффективно управлять рисками ИБ для достижения своих целей;
    2) оценка необходимости обеспечения или совершенствования ИБ на сонове критериев получаемой выгоды, преимуществ и затрат для бизнеса;
    3) оценка степени соответствия системы ЗИ эталону и предложения по устранению недостатков.
15. Модель оценки:
    1) определяет сферу оценки (контекст оценки ИБ в рамках критерия оценки, контролируемые факторы (параметры) объекта оценки);
    2) устанавливает показатели оценки ИБ;
    3) формирует цель оценки.
16. 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.
17. Программа измерений ИБ является элементом:
    1) системы мониторинга и анализа СМИБ;
    2) системы поддержки и улучшения СМИБ;
    3) системы внедрения и функционирования СМИБ.
18. Методы анализа рисков ИБ. Метод Дельфи:
    1) предназначен для получения обобщенного мнения группы экспертов за счет согласованиянезависимых мнений оценок;

2) предназначен для идентификации потенциальных опасностей и проблем (риска) для лдей, оборудования, окружающей среды и/или достижения целей организации;

3) предназначен для сбора большего количестваразнообразных идей для нализа риска.

19. Методы анализа риска. Анализ уровней защиты:

1) направлен на анализ достаточности мер по управлению или снижению риска;

2) является сочетаниемметодов дерева несправностей и дерева событий;

3) схематический способ описания анализа пути развития опасного события от причин до последствий.

20. Методы анализа риска. В ситуации, когда будующее сосотояние системы зависит только от ее текущего состояния, применим

1) метод Монте-Карло;

2) Байесовский анализ и сеть Байеса;

3) Марковский анализ.

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. 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.

Ключи

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2)	3)	1), 3)	2), 3)	1)	2)	3)	1)	1)	1), 2)
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
4)	3)	1)	2)	1), 2)	2), 3)	1)	1)	1)	3)

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1.Экзамен проводится с применением следующих методов (средств): устный опрос, тестирование. Для оценки сформированности компетенций, знаний и умений, соответствующих данным компетенциям, используются контрольные вопросы, а также задачи.

5.2.Оценочные материалы промежуточной аттестации

Компонент компетенции	Промежуточный/ключевой индикатор	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

Типовые оценочные материалы промежуточной аттестации

Вопросы к экзамену по дисциплине «Управление информационной безопасностью»

1. Риск-ориентированный подход к управлению ИБ организации.
2. Понятие корпоративной политики безопасности. Многоуровневый подход.
3. Управления информационной безопасностью на основе соответствия требованиям (compliance management).
4. Анализ упущений (gap-анализ).
5. Модель непрерывного совершенствования (замкнутый цикл менеджмента PDCA).
6. Уровни организации деятельности по обеспечению ИБ компании и общая структура стандартов ИБ.
7. Стандарт «Оранжевая книга».
8. Стандарт ITSEC.
9. Стандарт ISO/IEC 15408 «Общие критерии».
10. «Лучшие практики» информационной безопасности ISO/IEC 27002. Статус стандартов ISO/IEC в РФ.
11. Стандарты менеджмента информационной безопасности. Состав и структура серии международных стандартов ISO/IEC 2700x.
12. Сервис-ориентированный и процессно-ориентированный подходы к управлению ИБ и ИТ.
13. Концепция корпоративного управления информационной безопасностью (IS Governance) в стандарте Cobit 5.
14. Эволюция модели информационной безопасности.
15. Свойства систем. Иерархические системы.
16. Понятие процесса. Свойства процессов. Суть управления процессом
17. Структурный (функциональный) и процессный подход к управлению.
18. Классификация и атрибуты процессов.
19. Эталонная модель процесса для управления ИБ.
20. Проблемы и ошибки при внедрении процессного подхода к управлению ИБ.
21. Понятие и состав системы менеджмента.
22. Принципы построения системы менеджмента ИБ на основе ISO/IEC 27001.
23. Этапы построения системы менеджмента ИБ на основе ISO/IEC 27001.
24. Организационная структура системы менеджмента ИБ.
25. Определение контекста и области действия системы менеджмента ИБ.
26. Процедура сертификации соответствия СМИБ требованиям ISO/IEC 27001.

27. Процесс управления рисками ИБ на основе ISO 27005.
28. Итерационная процедура оценки рисков ИБ.
29. Виды обработки рисков ИБ.
30. Методики оценки рисков ИБ.
31. Виды и способы оценки ИБ компании.
32. Этапы процесса оценки (аудита) ИБ.
33. Роли в процессе оценки (аудита) ИБ.
34. Измерения ИБ ISO/IEC 27004
35. Понятие зрелости и уровней возможности. Модели зрелости.
36. Оценка процессов ИБ на основе моделей уровней возможностей.
37. Оценка процессов разработки средств ЗИ на основе моделей зрелости

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.

Оценка «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 по освоению 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 «Управление информационной безопасностью» предполагает изучение курса на аудиторных занятиях (лекции, практические работы) и самостоятельной работы обучающихся. Семинарские занятия дисциплины «Управление информационной безопасностью» 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.

Выполнение задания:

Повторение лекционного материала, изучение нормативной литературы (текста стандарта), использование рекомендуемой литературы.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"

7.1. Основная литература

1. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/1021744
2. Веселов Г.Е. Менеджмент риска информационной безопасности: учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. — Электрон. дан. - Таганрог:Южный федеральный университет, 2016. - 107 с.
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.

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/
4. Суханов А.В., Смирнов А.С., Хитов С.Б. Управление информационной безопасностью предприятий оборонно-промышленного комплекса в контексте стандарта ISO 27001:2013 [Электронный ресурс] – URL: http://eds.a.ebscohost.com/

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.