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
Аналитическое обеспечение информационной безопасности
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса
Б1.В.07 «Моделирование информационной безопасности. Управление рисками»
(код и наименование РПД)

38.04.05 Бизнес-информатика
(код,наименование направления подготовки)

очная
(форма обучения)

Год набора – 2024

Санкт-Петербург, 2024г.

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

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

РПД «Моделирование информационной безопасности. Управление рисками» 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.07 «Моделирование информационной безопасности. Управление рисками» обеспечивает овладение следующими компетенциями:

Таблица 1.1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКс-2	Способен обосновывать подходы и требования к системе обеспечения информационной безопасности, оценивать уровни безопасности компьютерных систем и сетей	ПКс-2.3	Способен оценивать уровни безопасности компьютерных систем и сетей

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

Таблица 1.2

ОТФ/ТФ *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения
Выполнение трудовых функций E формирование требований к защите информации в автоматизированных системах и F аналитическое обеспечение разработки стратегии изменений организации в соответствии с обобщенными трудовыми функциями профессиональных стандартов 06.033 «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ» и 08.037 «БИЗНЕС-АНАЛИТИК» соответственно.	ПКс-2.3	на уровне знаний*:* **Знать:** – основные положения теоретических основ моделирования процессов и систем защиты информации; – основные подходы и требования к системе обеспечения информационной безопасности; на уровне умений: **Уметь:** – применять инструментальные программные средства моделирования и проектирования моделей; – оценивать уровни безопасности компьютерных систем и сетей; на уровне навыков: **Владеть:** – методикой проведения экспериментов, анализа результатов компьютерного моделирования процессов и систем защиты информации и оценки уровня безопасности компьютерных систем и сетей.

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	28/21
Самостоятельная работа	**58/45**
Контроль	***36/***
Формы текущего контроля	
Форма промежуточной аттестации	***Экзамен***

Место дисциплины в структуре ОП ВО

Дисциплина изучается в 3-м семестре 2-го курса. Дисциплина Б1.В..07 «Моделирование информационной безопасности. Управление рисками» относится к части дисциплин, формируемых участниками образовательных отношений учебного плана по направлению «Бизнес-информатика» 38.04.05 образовательной программы «Аналитическое обеспечение информационной безопасности». Преподавание дисциплины опирается на дисциплины программы магистратуры Б1.О.04 «Средства информационной безопасности», Б1.О.07 «Аналитическая поддержка принятия решений».

Дисциплина закладывает теоретический и методологический фундамент для овладения умениям и навыками в ходе овладения дисциплинами (модулями) по выбору 3 (ДВ.3), 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	
Тема 1	Теоретические основы моделирования информационной безопасности	34	6	8		20	Т(О)*
Тема 2	Методологические основы моделирования информационной безопасности	38	8	10		20	О(Т)**
Тема 3	Управление рисками	34	6	10		18	Т(О)*
Промежуточная аттестация					2*		Экзамен
Всего (акад./астр. часы):		106/82	20/15	28/22	2/1,5	58/45	36/27

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)[1];
ЛР – лабораторные работы (вид занятий семинарского типа)[2];
ПЗ – практические занятия (виды занятий семинарского типа за исключением лабораторных работ)[3];
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)[4];
ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.
СРО – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.
Примечание:
** – разработчик указывает формы заданий текущего контроля успеваемости (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.), с применением которых ведется мониторинг успешности освоения образовательной программы обучающимися*
*** – разработчик указывает формы промежуточной аттестации: экзамен (Экз), зачет (З)/ зачет с оценкой (ЗО).*
Используемые сокращения и примечания включаются после каждой из заполняемых таблиц.

3.2. Содержание дисциплины

Тема 1. Теоретические основы моделирования информационной безопасности

Основы системного анализа и теории системного моделирования. Цели и задачи системного анализа. Модель как философская категория. Множественность моделей систем. Процедуры системного анализа. Понятие модели. Цели моделирования. Классификация моделей. Принципы системного моделирования. Общий порядок разработки моделей.

Эвристические методы моделирования. Классификация. Индивидуальные и коллективные методы. Инструментальные средства.

Натурные методы моделирования. Классификация. Испытание как метод моделирования систем. Инструментальные средства.

Аналитические методы моделирования. Классификация. Математическое и статическое

---

[1] Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

[2] См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

[3] См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

[4] Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

моделирование. Порядок построения и анализа аналитических моделей.

Тема 2. Методологические основы моделирования информационной безопасности.

Структурные технологии моделирования процессов и систем защиты информации. Концепция структурного моделирования процессов и систем защиты информации. Программные средства структурного моделирования, их возможности и особенности использования.

Объектно-ориентированные технологии моделирования процессов и систем защиты информации. Концепция объектно-ориентированного моделирования процессов и систем защиты информации. Программные средства объектно-ориентированного моделирования, их возможности и особенности использования.

Имитационные технологии моделирования процессов и систем защиты информации. Концепция имитационного моделирования процессов и систем защиты информации. Программные средства имитационного моделирования, их возможности и особенности использования.

Интегрированные технологии моделирования процессов и систем защиты информации. Концепция интеграции технологий процессов и систем защиты информации. Интегрированные программные средства моделирования, их возможности и особенности использования.

Тема 3. Управление рисками.

Оценка риска. Идентификация и анализ риска. Методологические основы управления рисками на объекте. Система управления рисками на предприятии. Стандарты в области управления рисками.

4. Материалы текущего контроля успеваемости обучающихся

В ходе реализации дисциплины Б1.В.07. «Моделирование информационной безопасности. Управление рисками» используются следующие **методы текущего контроля успеваемости** обучающихся:

Таблица 3.1

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Теоретические основы моделирования информационной безопасности	Тестирование, опрос
Тема 2. Методологические основы моделирования информационной безопасности	Реферат, опрос
Тема 3. Управление рисками	Тестирование, опрос

4.1.2. Экзамен проводится по вопросам изучаемых тем, учитывая итоги выполнения заданий текущего контроля.

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Типовые оценочные материалы по теме 1

Типовые вопросы для опроса по теме 1

1. Дать определение понятию «система», «подсистема».
2. Назвать основные закономерности функционирования и развития сложных систем.
3. Что такое структура системы?
4. Назвать основные методики системного анализа.
5. Каковы этапы методики Business Process Management – BPM?
6. Определите понятие «модель».
7. Раскрыть основные принципы моделирования.
8. Назвать типовые этапы и стадии моделирования при разработке и исследовании моделей любой природы.

9. Какие модели относятся к эвристическим?
10. Раскрыть формы моделей типа мозговой атаки?
11. Раскрыть сущность методов типа сценариев.
12. Какие модели относятся к натурным?
13. С какой целью проводятся эксперименты?
14. В чем заключается специфика и условия реализации натурных испытаний?
15. Какие модели относятся к аналитическим? В чем заключается особенность аналитических методов?
16. Раскрыть достоинства и недостатки аналитических методов?
17. Дать характеристику математических, статистических, теоретико-множественных, логических, лингвистических, семиотических и графических методов.
18. Какие методы исследования аналитических систем известны?
19. В чем заключаются особенности детерминированных, стохастических модлей?
20. Какова область использования статистических методов прогнозирования?

Тест:

1. Процесс познания, связанный с сожданием и исследованием моделей, называется:
    1) моделированием;
    2) алгоритмизацией;
    3) проектированием.
2. Новый объект, отражающий существенные особенности изучаемого объекта, процесса или явления, называется:
    1) предметной областью;
    2) моделью;
    3) сущностью.
3. К эвристическим методам программирования относятся :
    1) методы типа мозговой атаки;
    2) объектно-ориентированные методы;
    3) имитационные.
4. Метод мозговой атаки – это то же самое, что и:
    1) эксперимент;
    2) коллективная генерация идей;
    3) структурно-функциональное моделирование
5. Методы типа дерева целей относятся к группе методов:
    1) структуризации;
    2) мозговой атаки;
    3) сценариев.
6. Укажите разработчика линейки программ STATISTICA:
    1) StatSoft;
    2) MapleSoft;
    3) Wolfram Research;
    4) IBM.
7. Какая процедура MS Excel дает доступ к команде «Скользящее среднее»?
    1) Данные → Анализ данных
    2) Формулы → Окно контрольного значения
    3) Формулы → Параметры вычислений
    4) Данные → Поиск решения

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

1. Раскрыть сущность концепции структурного моделирования процессов и систем защиты информации.
2. Каковы программные средства структурного моделирования вы можете назвать?
3. Раскрыть возможности и особенности использования программных средств структурного моделирования.
4. Раскрыть сущность концепции объектно-ориентированного моделирования процессов и систем защиты информации.
5. Назвать программные средства объектно-ориентированного моделирования.
6. объектно-ориентированного моделирования.
7. Раскрыть сущность концепции имитационного моделирования процессов и систем защиты информации.
8. Назвать программные средства имитационного моделирования.
9. Раскрыть возможности и особенности использования программных средств имитационного моделирования.
10. Раскрыть сущность концепции интеграции технологий процессов и систем защиты информации.
11. Назвать интегрированные программные средства моделирования.
12. Раскрыть возможности и особенности использования интегрированных программных средств.

Типовые темы рефератов с последующей защитой и обсуждением

1. Моделирование систем массового обслуживания в телекоммуникационных системах.
2. Модели принятия решений.
3. Модели взаимодействия двух популяций.
4. Модели безопасности на основе дискреционной политики.
5. Модели безопасности на основе мандатной политики.
6. Модели безопасности на основе тематической политики.
7. Модели безопасности на основе ролевой политики.
8. Автоматные и теоретико-вероятностные модели невлияния и невыводимости.
9. Построение математических моделей угроз ИБ, нарушителя ИБ, защиты ИБ в сетях и системах телекоммуникаций.
10. Модели и технологии обеспечения целостности данных.
11. Модели безопасности в распределенных системах.
12. Моделирование систем управления

Типовые оценочные материалы по теме 3
Типовые вопросы для опроса по теме 3:

1. Методики анализа рисков ИБ. Инвентаризация активов.
2. Понятие актива. Типы активов. Источники информации об активах организации.
3. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками.
4. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.
5. Оценка рисков ИБ. Идентификация и анализ риска.
6. Планирование мер по обработке выявленных рисков ИБ.

7. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.
8. Система управления рисками на предприятии.

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. Оценка рисков – это общий процесс
    1) анализа и оценивания рисков;
    2) идентификации и определения величины рисков;
    3) присвоение значений вероятности и последствий риска.
4. Анализ рисков состоит;
    1) из идентификации рисков;
    2) из определения величины (уровня) рисков;
    3) из ранжирования рисков.
5. 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.
6. Оценка ИБ на основе экономических показателей – 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.
7. 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.

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.

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 устно по билетам.

5.2 Оценочные материалы промежуточной аттестации

Таблица 5.2.1

Компонент компетенции	Промежуточный/ключевой индикатор оценивания	Критерий оценивания
Способен оценивать уровни безопасности компьютерных систем и сетей	Использует инструментальные программные средства моделирования и проектирования моделей для решения задач в оценивании уровней безопасности компьютерных систем и сетей.	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 Б1.В. 07 «Моделирование информационной безопасности. Управление рисками»

1) Понятие модели. Цели, задачи и принципы моделирования.
2) Структурные технологии моделирования. Синтаксис и семантика IDEF0-диаграмм.
3) Классификация моделей по признаку физической сущности моделирующих объектов.
4) Основные этапы имитационного моделирования. Технология моделирования в ARENA/
5) Общая характеристика эвристических методов моделирования.
6) Структурные технологии моделирования. Принципы моделирования в IDEF0. Декомпозиция.
7) Общая характеристика аналитических методов моделирования.
8) Структурные технологии моделирования. Синтаксис и семантика IDEF0 – диаграмм.
9) Математические модели. Формы записи математических моделей.
10) Структурные технологии моделирования. Основные правила построения IDEF0 – диаграмм.
11) Натурное моделирование. Типовые схемы испытаний.
12) Структурные технологии моделирования. Туннелирование стрелок в IDEF0-диаграммах.
13) Общий порядок разработки моделей. Типовые этапы и стадии моделирования.
14) Иерархическая структура модельных представлений в объектно-ориентированном моделировании.

15) Признаки классификации моделей.
16) Объектно-ориентированное моделирование. Использование языка UML.
17) Назначение и содержание экспериментального этапа моделирования.
18) Диаграммы языка UML. Виды и назначение.
19) Назначение и содержание экспериментального этапа моделирования.
20) Интегрированные методы моделирования. Сущность интеграции.
21) Компьютерные технологии моделирования. Обзор.
22) Сущность методологии АРИС.
23) Методы экспертных оценок. Проблемы применения.
24) Понятие имитационного моделирования. Целесообразность применения имитационного моделирования.
25) Диаграммы языка UML. Виды диаграмм.
26) Методология АРИС. Особенности.
27) Методы экспертных оценок. Способы устранения недостатков методов.
28) UML. Диаграмма вариантов использования.
29) Имитационное моделирование. Способы продвижения модельного времени.
30) Экспертные оценки. Особенности использования метода.
31) Целесообразность и особенности применения иммитационного моделирования.
32) Ключевые принципы использования UML.
33) Эвристические методы моделирования. Мозговой штурм. Особенности использования.
34) Сущности в языке UML. Типы сущностей.
35) Принцип системности интеграции. Системообразующие свойства сложной системы.
36) Отношения в языке UML. Типы отношений.
37) Преимущества методологии АРИС.
38) Диаграммы поведения в зыке UML. Назначение и использование.
39) Основные типы представлений в методологии АРИС.
40) UML. Концептуальная модель.
41) Уровни детализации моделей в АРИС.
42) Виды методов типа «мозговой атаки».
43) Разновидности имитационных моделей.
44) Практическое применение КГИ (коллективной генерации идей).
45) Моделирование систем массового обслуживания.
46) Методы экспертных оценок. Виды шкал, используемых для обработки ответов экспертов.
47) ARENA. Язык моделирования и анимационная система.
48) Методики анализа рисков ИБ. Инвентаризация активов.
49) Понятие актива. Типы активов. Источники информации об активах организации.
50) Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками.
51) Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.
52) Оценка рисков ИБ. Идентификация и анализ риска.
53) Планирование мер по обработке выявленных рисков ИБ.
54) Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.
55) Система управления рисками на предприятии.

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»).

Обучение по дисциплине «Моделирование информационной безопасности. Управление рисками» предполагает изучение курса на аудиторных занятиях (лекции, практические работы) и самостоятельной работы обучающихся. Семинарские занятия дисциплины «Моделирование информационной безопасности. Управление рисками» 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 следующих рекомендациях:

- 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.
- посещение консультаций преподавателя.

Подготовка реферата (НИР) по плану:

- разработка и анализ теории;
- разработка моделей исследуемого объекта. Преобразование моделей;
- разработка научной документации, разработка промежуточного отчета;
- проведение дополнительных исследований;
- обработка результатов экспериментов. Разработка промежуточного отчета;
- сопоставление результатов анализа информационных источников и результатов теоретических и экспериментальных исследований;
- оценка эффективности полученных результатов;
- разработка рекомендаций по использованию результатов;
- разработка заключительного отчета.

Процедура осуществления контроля выполнения задания проводится по критериям.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 02.04.2023).

2. Панарина, М. М. Корпоративная безопасность: система управления рисками и комплаенс в компании : учебное пособие для вузов / М. М. Панарина. — Москва : Издательство Юрайт, 2023. — 158 с. — (Высшее образование). — ISBN 978-5-534-15342-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520423 (дата обращения: 02.04.2023).

3. Моделирование процессов и систем: учебник и практикум для вузов / Е. В. Стельмашонок, В. Л. Стельмашонок, Л. А. Еникеева, С. А. Соколовская ; под редакцией Е. В. Стельмашонок. — Москва : Издательство Юрайт, 2023. — 289 с. — (Высшее образование). — ISBN 978-5-534-04653-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511904 (дата обращения: 02.04.2023).

4. Воронцовский, А. В. Управление рисками: учебник и практикум для вузов / А. В. Воронцовский. — 2-е изд. — Москва : Издательство Юрайт, 2023. — 485 с. — (Высшее образование). — ISBN 978-5-534-12206-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511534 (дата обращения: 02.04.2023).

7.2 Дополнительная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519780 (дата обращения: 02.04.2023).

2. 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.

3. 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

4. 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.

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»

Электронные учебники электронно – библиотечной системы (ЭБС) «Юрайт»

Электронные учебники электронно – библиотечной системы (ЭБС) «Знаниум»

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 пакет программ MS Office 2013, 2016, справочная электронная система «Гарант» 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) Office 365, Teams, Moodle

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
2.	Пакет Excel -2016, proffesional plus, IBM SPSS statistics, R, RStudio, Anaconda
3.	Мультимедийные средства в каждом компьютерном классе и в лекционной аудитории
4.	Браузер, сетевые коммуникационные средства для выхода в Интернет. Сервисы и службы Azure
5.	Arena Student Version
6.	ARIS Education
7.	Business Studio
8.	IBM RationalIRose

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.