Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Направление подготовки: 10.04.01 «Информационная безопасность»

Магистерская программа «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2023

Смоленск

Методические материалы составил:
канд. экон. наук, доцент кафедры
«Информационные технологии в экономике и управлении» _____ О.В. Булыгина

«20» _января_ 2023 г.

Заведующий кафедрой «Информационные технологии в экономике и управлении»:

_____ __д-р техн. наук, профессор_М.И. Дли__
подпись ФИО

«25» _января_ 2023 г.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

ВВЕДЕНИЕ

Дисциплина направлена на формирование у студентов теоретических знаний и практических навыков решения профессиональной деятельности в области обеспечения информационной безопасности защиты информации. Ее изучение позволит сформировать компетентности, которые будут необходимы при освоении программы магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого, проектного и научно-исследовательского типов в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся с российскими нормативными правовыми документами, международными и отечественными стандартами в области обеспечения информационной безопасности;
- дать представление об угрозах, рисках и уязвимостях информационной безопасности;
- сформировать умение проводить анализ проблем информационной безопасности;
- сформировать навыки разработки концепции и политики информационной безопасности;
- сформировать умение разрабатывать стратегию построения и внедрения системы управления информационной безопасностью;
- сформировать практические навыки разработки технического задания на создание системы обеспечения информационной безопасности;
- научить выполнять оценку экономической эффективности системы обеспечения информационной безопасности предприятия.

В процессе изучения дисциплины развиваются универсальная компетенция: способность осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1), и две общепрофессиональные компетенции: способность обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание (ОПК-1) и способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности (ОПК-3).

В процессе изучения дисциплины студенты получат:

знания:

- методов обследования организации (УК-1);
- критериев качества информации (УК-1);
- видов информационных ресурсов (УК-1);
- принципов системного и процессного подхода к управлению информационной безопасностью (УК-1);
- видов стратегий построения и внедрения системы управления информационной безопасностью (УК-1);

- требований нормативных правовых актов и методических документов для рассматриваемого объекта информатизации (ОПК-1);
- структуры и содержания технического задания на создание системы обеспечения информационной безопасности (ОПК-1);
- состава организационно-распорядительных документов по обеспечению информационной безопасности (ОПК-3);
- российских нормативных правовых документов, международных и отечественных стандартов в области обеспечения информационной безопасности (ОПК-3);
- содержания концепции и политик информационной безопасности (ОПК-3);

умения:

- проводить анализ проблем информационной безопасности (УК-1);
- формировать критерии для поиска информации для решения исследуемой проблемы (УК-1);
- критически оценивать надежность источников информации (УК-1);
- планировать систему управления информационной безопасностью (УК-1);
- разрабатывать стратегию построения и внедрения системы управления информационной безопасностью (УК-1);
- разрабатывать требования к системе управления информационной безопасности (ОПК-1);
- разрабатывать техническое задание на создание системы обеспечения информационной безопасности (ОПК-1);
- собирать и структурировать информацию для разработки организационно-распорядительных документов по обеспечению информационной безопасности (ОПК-3);
- выбирать стандарт, по которому будут разрабатываться организационно-распорядительные документы по обеспечению информационной безопасности (ОПК-3);
- определять необходимые виды частных политик информационной безопасности (ОПК-3);

владение:

- навыками анализа и формирования причинно-следственных связей в исследуемой проблеме (УК-1);
- навыками устранения пробелов в информации, необходимой для решения исследуемой проблемы (УК-1);
- навыками работы с различными источниками информации, необходимой для решения исследуемой проблемы (УК-1);
- навыками выбора подхода к внедрению системы управления информационной безопасностью (УК-1);
- навыками исследования проблем реализации стратегии построения и внедрения системы управления информационной безопасностью (УК-1);
- навыками анализа активов организации, их угроз информационной безопасности и уязвимостей (ОПК-1);
- навыками выбора инструментальных средств для реализации элементов защиты информации (ОПК-1);
- навыками анализа потребностей в документальном обеспечении информационной безопасности (ОПК-3);
- навыками сравнительного анализа различных подходов к документальному обеспечению информационной безопасности (ОПК-3);
- навыками разработки набора организационно-распорядительных документов по обеспечению информационной безопасности (ОПК-3).

Знания и навыки, полученные студентами при изучении дисциплины «Управление информационной безопасностью», используются ими при изучении других дисциплин программы магистратуры, а также при проведении научных исследований.

1 ОБЩИЕ СВЕДЕНИЯ О САМОСТОЯТЕЛЬНОЙ РАБОТЕ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

Методическое обеспечение самостоятельной работы студентов разработано на основе локального акта филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске «Положение об организации самостоятельной работы студентов».

Целями самостоятельной работы студентов являются:

– систематизация и закрепление знаний, умений и навыков;

– углубление и расширение теоретических знаний;

– развитие умений использовать справочную документацию и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации.

Основным принципом организации самостоятельной работы студентов является комплексный подход, направленный на формирование навыков творческой деятельности студента в аудитории, при внеаудиторных контактах с преподавателем на консультациях и в ходе домашней подготовки.

В учебном процессе выделяют **два вида самостоятельной работы**: ***аудиторная*** – самостоятельная работа выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию; ***внеаудиторная*** – самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Аудиторная самостоятельная работа студентов осуществляется под руководством и контролем преподавателя на лекциях и лабораторных занятиях.

При выполнении заданий ***внеаудиторной самостоятельной работы*** студент должен:

– строго выполнять весь объем заданий самостоятельной работы;

– предоставить преподавателю выполненные задания на проверку;

– после изучения каждой темы готовиться к устным опросам;

– готовиться к лабораторным работам;

– выполнять все задания, независимо от пропуска занятий по уважительным или неуважительным причинам.

В таблице 1 приведены виды и трудоемкость внеаудиторной самостоятельной работы студентов по дисциплине «Управление информационной безопасностью».

Методика самостоятельной работы по дисциплине предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов, в том числе связанных с ограничением возможностей здоровья.

Таблица 1 - Виды внеаудиторной самостоятельной работы студентов по дисциплине «Управление информационной безопасностью»

Вид работ	Трудоёмкость, ЗЕТ, час
Изучение материалов лекций	0,47 ЗЕТ, 17 час
Подготовка к защите лабораторной работы	0,5 ЗЕТ, 18 час
Самостоятельное изучение дополнительных материалов дисциплины (СРС)	0,14 ЗЕТ, 5 час
Всего (в соответствии с УП)	**1,11 ЗЕТ, 40 час**
Подготовка к экзамену	**1 ЗЕТ, 36 час**

Виды и часы, отводимые на каждый вид внеаудиторной самостоятельной работы студентов, соответствуют разделам 3 и 4 рабочей программы дисциплины.

2 ПОДГОТОВКА СТУДЕНТОВ К ЛЕКЦИЯМ

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы.

Слушание и запись лекций – сложный вид вузовской аудиторной работы, который дополняется внеаудиторной самостоятельной работой студентов – подготовка к лекциям. Основным требованием, предъявляемым к такой работе, является, прежде всего, систематичность ее проведения.

Подготовка студента к лекции включает следующие этапы:

– печать выдач демонстрационных слайдов предстоящей лекции, подготовленных лектором;

– знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе;

– составление краткого конспекта на основе материалов, предоставленных преподавателем, и запись на полях непонятных или спорных вопросов;

– техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

– заполнение пробелов в конспекте сведениями, который студент не успел записать, или дополнительным материалом из источников информации, рекомендованных лектором;

– выполнение заданий преподавателя

В таблице 2 приведены задания для подготовки студентов к лекциям по дисциплине «Управление информационной безопасностью».

Таблица 2 – Задания для подготовки студентов к лекциям по дисциплине

Наименование лекций (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
Лекция 1. Ключевые вопросы информационной безопасности (1 час)	Основные составляющие информационной безопасности.
Лекция 2. Информационная безопасность в системе национальной безопасности России (1 час)	Основные понятия ФЗ №187 «О безопасности критической информационной инфраструктуры Российской Федерации».
Лекция 3. Стандартизация процессов управления информационной безопасностью (1 час)	Понятие оценочных стандартов и технических спецификаций.
Лекция 4. Классификация угроз информационной безопасности (1 час)	Понятие угрозы и уязвимости информационной безопасности.
Лекция 5. Модель нарушителя информационной безопасности (1 час)	Понятие нарушителя информационной безопасности.
Лекция 6. Документальное обеспечение управления информационной безопасностью (1 час)	Зарубежные подходы к документированию информационной безопасности.
Лекция 7. Система управления информационной безопасностью (1 час)	Уровни обеспечения информационной безопасности.
Лекция 8. Корпоративная и частные политики информационной безопасности (1 час)	Административная и техническая политика информационной безопасности.
Лекция 9. Процессы управления информаци-	Управление инцидентами информаци-

онной безопасностью (1 час)	онной безопасности.
Лекция 10. Организационные вопросы управления информационной безопасностью (1 час)	Ролевая структура системы управления информационной безопасностью.
Лекция 11. Технические аспекты управления информационной безопасностью (1 час)	Классификация объектов защиты информации.
Лекция 12. Программные средства управления информационной безопасностью (1 час)	Программные средства поддержки аудита информационной безопасности.
Лекция 13. Идентификация и анализ информационных рисков (1 час)	Классификация источников рисков информационной безопасности.
Лекция 14. Методы управления информационными рисками (1 час)	Уровни управления информационными рисками.
Лекция 15. Аудит информационной безопасности (1 час)	Понятие внутреннего и внешнего аудита информационной безопасности.
Лекция 16. Оценка экономической эффективности деятельности по управлению информационной безопасностью (1 час)	Показатели оценки процессов системы управления информационной безопасностью.
Лекция 17. Измерение информационной безопасности. Оценка зрелости процессов управления информационной безопасностью (1 час)	Уровни зрелости процессов обеспечения информационной безопасности.
Итого: 17 часов	

Техническое оформление записей в конспекте предполагает использование знаков акцентирование и цвета.

Знаки акцентирования применяются для выделения, привлечения особого внимания к отдельным частям текста конспекта, а также для пояснения роли этого места в тексте. Примерами знаков акцентирования являются: ! – особое внимание; !! – повышенное внимание; !!! – особенно важно; ? – неясно, следует обратиться за консультацией к преподавателю или к учебной литературе; NB – (от лат. nota bene) – взять на заметку для дальнейшей проработки; ↕ - противоречие; ↑ - см. выше, повтор; ∑ или ∫ - итог, заключительная мысль; Д.С. – материал для справки (а не для запоминания); √, > - сделать вставку в текст, дополнить его; P.S. – постскриптум (от латинского post scriptum), дополнение; ставится если лектор, возвращаясь к ранее изложенному, рекомендует дополнить текст.

Заголовки разделов, подразделов необходимо выделять с помощью цвета. Но не следует применять много цветов, желательно не более трех – четырех. Применение цвета существенно ускоряет записи по сравнению с другими способами выделения тем же цветом, которым выполняется основная часть конспекта. Но основное назначение использования цвета, улучшить восприятие и запоминание конспекта.

Результаты выполнения заданий фиксируются в тетрадях для конспектов лекций.

Формой контроля данного вида самостоятельной работы студентов является проверка конспектов лекций и дополнительных теоретических материалов. Порядок выполнения пропущенных работ по уважительным и неуважительным причинам оговариваются преподавателем индивидуально с каждым студентом.

3 ПОДГОТОВКА СТУДЕНТОВ К ЛАБОРАТОРНЫМ РАБОТАМ

Самостоятельная подготовка студентов к лабораторным работам заключается в изучении конспекта соответствующей лекции (если она читалась по данной теме), чтении соответствующего раздела учебника и дополнительных источников.

Главными задачами этой подготовки являются:

- повторение теоретических знаний, усвоенных в рамках аудиторной работы;
- расширение и углубление знаний по теме занятия;
- закрепление практических навыков, полученных на предыдущих аудиторных занятиях.

Знания, умения и навыки, полученные в процессе такой самостоятельной работы, являются базой для выполнения и защиты лабораторных работ.

Подготовка студентов к защите лабораторных работ включает в себя следующие этапы:

– оформление отчета по предыдущей лабораторной работе и подготовка к его защите;

– ознакомление с методическими указаниями по выполнению предстоящей лабораторной работы;

– проработка теоретического материала по теме лабораторной работы с использованием конспекта лекций и рекомендованных источников;

– ответы на вопросы для самопроверки.

В таблице 3 приведены задания для самостоятельной подготовки студентов к выполнению и вопросы к защите лабораторных работ по дисциплине «Управление информационной безопасностью».

Таблица 3 – Задания для самостоятельной подготовки студентов к выполнению и вопросы к защите лабораторных работ по дисциплине

Наименование лабораторных работ (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
Лабораторная работа 1-2. Анализ бизнес-процессов предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Понятие бизнес-процесса. 2. Методологии моделирования бизнес-процессов. 3. Средства моделирования бизнес-процессов. 4. Виды организационных структур.
Лабораторная работа 3-4. Анализ информационных потоков и ИТ-инфраструктуры предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Понятие и характеристики информационного потока. 2. Классификация информационных потоков. 3. Понятие ИТ-инфраструктуры. 4. Структура ИТ-инфраструктуры предприятия.
Лабораторная работа 5-6. Анализ внутренних и внешних угроз информационной безопасности (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Классификация угроз информационной безопасности. 2. Понятие доступности, целостности и конфиденциальности информации. 3. Классификация методов реализации угроз. 4. Классификация уязвимостей безопасности.

Наименование лабораторных работ (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
Лабораторная работа 7-8. Построение модели нарушителя (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Понятие нарушителя информационной безопасности. 2. Внутренние и внешние нарушители. 3. Классификация нарушителей по уровню возможностей. 4. Классификация нарушителей по месту действий.
Лабораторная работа 9-10. Анализ информационных рисков предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. ГОСТ Р ИСО/МЭК 27005-2010 2. Понятие риска информационной безопасности. 3. Классификация рисков информационной безопасности. 4. Методы оценки риска информационной безопасности.
Лабораторная работа 11-12. Разработка концепции информационной безопасности предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. ГОСР Р ИСО/МЭК 17799-2005. 2. Классификация объектов защиты информации. 3. Меры обеспечения информационной безопасности. 4. Средства обеспечения информационной безопасности.
Лабораторная работа 13-14. Разработка политики информационной безопасности предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. ГОСТ Р ИСО/МЭК 27001-2006. 2. Содержание политики информационной безопасности. 3. Виды частных политик информационной безопасности. 4. Трастовые модели.
Лабораторная работа 15-16. Разработка технического задания на создание системы обеспечения информационной безопасности предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. ГОСТ Р 51583-2014 2. Структура технического задания. 3. Примеры требований к надежности ИС. 4. Примеры требований по защите персональных данных.
Лабораторная работа 17. Оценка экономической эффективности системы обеспечения информационной безопасности предприятия (2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Оценка информационной безопасности на основе модели

Наименование лабораторных работ (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
	зрелости процессов. 2. Оценка информационной безопасности по эталону. 3. Риск-ориентированная оценка информационной безопасности. 4. Методика совокупной стоимости владения компании Gartner Group.
Итого: 18 часов	

4 САМОСТОЯТЕЛЬНОЕ ИЗУЧЕНИЕ ДОПОЛНИТЕЛЬНЫХ МАТЕРИАЛОВ ДИСЦИПЛИНЫ

Самостоятельная работа с учебниками, учебными пособиями, научной и справочной литературой, материалами периодических изданий и Интернет-ресурсами, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов собственное отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме дисциплины, что позволяет студентам проявить свою индивидуальность в рамках выполнения заданий, выявить широкий спектр мнений по изучаемой проблеме. Умение работать с литературой означает научиться осмысленно пользоваться источниками. Прежде чем приступить к освоению научной литературы, рекомендуется чтение учебников и учебных пособий.

Наиболее эффективным методом работы с литературными источниками является метод кодирования: прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке. Чтобы основательно обработать информацию и закодировать ее для хранения, важно произвести целый ряд мыслительных операций: прокомментировать новые данные; оценить их значение; поставить вопросы; сопоставить полученные сведения с ранее известными. Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения.

Изучение научной, учебной и иной литературы требует ведения рабочих записей.

Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

План - первооснова, каркас какой-либо письменной работы, определяющие последовательность изложения материала. План является наиболее краткой и потому самой доступной и распространенной формой записей содержания исходного источника информации. По существу, это перечень основных вопросов, рассматриваемых в источнике. План может быть простым и развернутым. Их отличие состоит в степени детализации содержания и, соответственно, в объеме. Преимущества плана состоят в следующем:

- план позволяет наилучшим образом уяснить логику мысли автора, упрощает понимание главных моментов произведения;

- план позволяет быстро и глубоко проникнуть в сущность построения произведения и, следовательно, гораздо легче ориентироваться в его содержании;

- план позволяет – при последующем возвращении к нему – быстрее обычного вспомнить прочитанное;

- с помощью плана гораздо удобнее отыскивать в источнике нужные места, факты, цитаты и т. д.

Выписки - небольшие фрагменты текста (неполные и полные предложения, отдельные абзацы, а также дословные и близкие к дословной записи об излагаемых в нем фактах), содержащие в себе квинтэссенцию содержания прочитанного. Выписки представляют собой более сложную форму записей содержания исходного источника информации. По сути, выписки – не что иное, как цитаты, заимствованные из текста. Выписки позволяют в концентрированной форме и с максимальной точностью воспроизвести в произвольном (чаще последовательном) порядке наиболее важные мысли автора, статистические и даталогические сведения. В отдельных случаях - когда это оправданно с точки зрения продолжения работы над текстом – вполне допустимо заменять цитирование изложением, близким к дословному.

Тезисы – сжатое изложение содержания изученного материала в утвердительной (реже опровергающей) форме. Отличие тезисов от обычных выписок состоит в следующем:

- тезисам присуща значительно более высокая степень концентрации материала;
- в тезисах отмечается преобладание выводов над общими рассуждениями;
- тезисы записываются близко к оригинальному тексту, без использования прямого цитирования.

Основное преимущество тезисов в том, что они незаменимы для подготовки глубокой и всесторонней аргументации письменной работы любой сложности, а также для подготовки выступлений на защите, докладов и пр.

Аннотация – краткое изложение основного содержания исходного источника информации, дающее о нем обобщенное представление. К написанию аннотаций прибегают в тех случаях, когда подлинная ценность и пригодность исходного источника информации исполнителю письменной работы окончательно неясна, но в то же время о нем необходимо оставить краткую запись с обобщающей характеристикой. Для указанной цели и используется аннотация. Характерной особенностью аннотации наряду с краткостью и обобщенностью ее содержания является и то, что пишется аннотация всегда после того, как (хотя бы в предварительном порядке) завершено ознакомление с содержанием исходного источника информации. Кроме того, пишется аннотация почти исключительно своими словами и лишь в крайне редких случаях содержит в себе небольшие выдержки оригинального текста.

Резюме – краткая оценка изученного содержания исходного источника информации, полученная, прежде всего, на основе содержащихся в нем выводов. Резюме весьма сходно по своей сути с аннотацией. Однако, в отличие от последней, текст резюме концентрирует в себе данные не из основного содержания исходного источника информации, а из его заключительной части, прежде всего выводов. Но, как и в случае с аннотацией, резюме излагается своими словами - выдержки из оригинального текста в нем практически не встречаются.

Конспект - сложная запись содержания исходного текста, включающая в себя заимствования (цитаты) наиболее примечательных мест в сочетании с планом источника, а также сжатый анализ записанного материала и выводы по нему. Для работы над конспектом следует:

- определить структуру конспектируемого материала, чему в значительной мере способствует письменное ведение плана по ходу изучения оригинального текста;
- в соответствии со структурой конспекта произвести отбор и последующую запись наиболее существенного содержания оригинального текста — в форме цитат или в изложении, близком к оригиналу;
- выполнить анализ записей и на его основе – дополнение записей собственными замечаниями, соображениями (располагать все это следует на полях тетради для записей или на отдельных листах-вкладках);
- завершить формулирование и запись выводов по каждой из частей оригинального текста, а также общих выводов.

Систематизация изученных источников позволяет повысить эффективность их анализа и обобщения. Итогом этой работы должна стать логически выстроенная система сведений по существу исследуемого вопроса. Необходимо из всего материала выделить существующие точки зрения на проблему, проанализировать их, сравнить, дать им оценку. В записях и конспектах студенту очень важно указывать названия источников, авторов, год издания.

В таблице 4 приведено распределение трудоемкости работ по самостоятельному изучению дополнительных материалов по дисциплине «Управление информационной безопасностью».

Для выполнения задания по самостоятельному изучению дополнительных теоретических материалов по дисциплине студенту необходимо прочитать рекомендованную литературу и законспектировать основные положения изученных источников, полностью раскрыв содержание тем, указанных в таблице 4.

Таблица 4 – Распределение трудоемкости работ по самостоятельному изучению дополнительных материалов по дисциплине

Темы для самостоятельного изучения дополнительных материалов	Трудоемкость, час
Тема 1. Стандарт COBIT.	1 час
Тема 2. Характеристики информации.	1 час
Тема 3. Методический документ Гостехкомиссии "Специальные требования и рекомендации по технической защите конфиденциальной информации".	1 час
Тема 4. Подход корпорации *Microsoft* к управлению безопасностью.	1 час
Тема 5. Обеспечение безопасности персональных данных.	1 час
Итого	**5 часов**

Рекомендуемая литература для самостоятельного изучения дополнительных материалов дисциплины

Основная литература

1 Аверченков В.И. Служба защиты информации: организация и управление: [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – М.: ФЛИНТА, 2016. – 186 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=93356

2 Гультяева Т.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Т.А. Гультяева; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=574729

3 Шилов А.К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / А.К. Шилов; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=500065

Дополнительная литература:

1 Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. – М.: ФЛИНТА, 2016. – 269 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=93245

2 Бекетнова Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем [Электронный ресурс]: учебное пособие / Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова; Финансовый университет при Правительстве Рос-

сийской Федерации. – Москва: Прометей, 2018. – 173 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=494850

3 Веселов Г.Е. Менеджмент риска информационной безопасности [Электронный ресурс]: учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 109 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=493331

4 Дронова Г.А. Управление информационной безопасностью [Электронный ресурс]: учебно-методическое пособие / Г.А. Дронова. – Новосибирск: Новосибирский государственный технический университет, 2016. – 28 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=575356

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1 Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа: http://www.consultant.ru/online/

2 Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа: http://government.ru/department/387/events/

3 Официальный сайт Росстата [электронный ресурс] — Режим доступа: www.gks.ru/

4 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа: http://geoline-tech.com/top-20-sites-about-information-security/

5 Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа: http://dorlov.blogspot.com/p/blog-page_3151.html

6 Информационная безопасность [электронный ресурс] — Режим доступа: http://www.securrity.ru/

7 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа: https://proglib.io/p/information-security-guide/

8 Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа: https://habr.com/ru/hub/infosecurity/

9 База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа: http://wiki.informationsecurity.club/doku.php/main

10 Информационная безопасность. Защита данных [электронный ресурс] — Режим доступа: http://all-ib.ru/

4 ПОДГОТОВКА К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЭКЗАМЕНУ)

Каждый учебный семестр заканчивается зачетно-экзаменационной сессией. Подготовка к промежуточной аттестации является самостоятельной работой студента. Основное в подготовке к сессии – повторение всего учебного материала дисциплины.

В соответствии с учебным планом формой промежуточной аттестации по дисциплине «Управление информационной безопасностью» является экзамен.

Трудоемкость подготовки к экзамену составляет 36 часов. В таблице 5 приведено распределение трудоемкости работ по подготовке к экзамену по темам дисциплины «Управление информационной безопасностью»

Если студент плохо работал в семестре, пропускал лекции, слушал их невнимательно, не конспектировал, не изучал рекомендованную литературу, то в процессе подготовки к

сессии ему придется не повторять уже знакомое, а заново в короткий срок изучать весь учебный материал. Все это невозможно эффективно сделать из-за нехватки времени, что неизбежно скажется на итоговой оценке.

За месяц до экзамена преподаватель выдает студентам программу экзамена, содержащую вопросы, выносимые на промежуточную аттестацию.

Таблица 5 – Распределение трудоемкости работ по подготовке к экзамену по темам дисциплины

Тема дисциплины	Трудоемкость, час	Номера вопросов в перечне
1. Ключевые вопросы информационной безопасности	2 часа	1,6,7
2. Информационная безопасность в системе национальной безопасности России	2 часа	3,4,5
3. Стандартизация процессов управления информационной безопасностью	3 часа	8
4. Классификация угроз информационной безопасности	2 часа	22,23
5. Модель нарушителя информационной безопасности	1 час	10
6. Документальное обеспечение управления информационной безопасностью	2 часа	9,27
7. Система управления информационной безопасностью	2 часа	2,13,14
8. Корпоративная и частные политики информационной безопасности	3 часа	10,11,12
9. Процессы управления информационной безопасностью	2 часа	15,16
10. Организационные вопросы управления информационной безопасностью	2 часа	19,20
11. Технические аспекты управления информационной безопасностью	2 часа	21
12. Программные средства управления информационной безопасностью	3 часа	17,18
13. Идентификация и анализ информационных рисков	2 часа	24,25
14. Методы управления информационными рисками	2 часа	26
15. Аудит информационной безопасности	2 часа	28
16. Оценка экономической эффективности деятельности по управлению информационной безопасностью	2 часа	29,30
17. Измерение информационной безопасности. Оценка зрелости процессов управления информационной безопасностью	2 часа	31,32
Итого	**36 часов**	**-**

Вопросы для подготовки к экзамену
по дисциплине «Управление информационной безопасностью»

1. Понятие и задачи информационной безопасности.
2. Уровни обеспечения информационной безопасности.
3. Правовая защита информации.
4. Место информационной безопасности в системе национальной безопасности.
5. Политика обеспечения информационной безопасности Российской Федерации.
6. Современные проблемы информационной безопасности.
7. Модель информационной безопасности организации.
8. Стандартизация процессов управления информационной безопасностью.

9. Состав организационно-распорядительных документов по обеспечению информационной безопасности.
10. Концепция информационной безопасности.
11. Корпоративная политика информационной безопасности.
12. Частные политики информационной безопасности.
13. Система управления информационной безопасностью.
14. Стратегии построения системы управления информационной безопасностью.
15. Процессный подход к управлению информационной безопасностью.
16. Ресурсы, результаты, владельцы процесса управления информационной безопасностью.
17. Программные средства управления информационной безопасностью.
18. Содержание технического задания на создание системы обеспечения информационной безопасности предприятия.
19. Организационные вопросы управления информационной безопасностью.
20. Состав и основные функции службы безопасности организации.
21. Технические аспекты управления информационной безопасностью.
22. Классификация угроз информационной безопасности.
23. Классификация уязвимостей.
24. Классификация информационных рисков.
25. Идентификация и анализ информационных рисков.
26. Методы оценивания информационных рисков.
27. Обеспечение безопасности персональных данных.
28. Аудит информационной безопасности.
29. Экономическая оценка обеспечения информационной безопасности.
30. Методика совокупной стоимости владения компании *Gartner Group.*
31. Измерение информационной безопасности.
32. Модели зрелости процессов управления информационной безопасностью.

Пример практических заданий (задач), выносимых на экзамен, для проверки практических умений и навыков студентов по дисциплине

Провести расчет информационных рисков на основе данных таблицы 6, приведенной ниже:

1) рассчитать общий уровень угроз по ресурсу;
2) определить общий риск по ресурсу.

Критерий критичности для программно-аппаратной защиты – 30 000 руб.
Критерий критичности для организационной защиты – 40 000 руб.
Критерий критичности для инженерно-технической защиты – 1 000 000 руб.

Таблица 6 – Исходные данные

Защи-та	Угроза	Уязвимость	Вероятность реализации, %	Критичность, %
Программно-аппаратная	Несанкционированный доступ к информации, хранящейся на сервере	Хранение данных на сервере в незашифрованном виде	50	70
		Отсутствие межсетевых экранов	30	50
	Потеря информации из-за вирусов и шпионских программ	Отсутствие постоянно обновляемого антивирусного программного обеспечения, межсетевого экрана	60	40
		Использование нелицензионного программного обеспечения	50	40

		Отсутствие ограничения доступа к внешней сети	10	30
	Несанкционированный доступ к информации, хранящейся на АРМ	Недостаточность системы аутентификации пользователей	40	60
		Отсутствие средств защиты от несанкционированного доступа по сети	50	50
Организационная	Физический доступ нарушителя к документам	Недостатки в организации контрольно-пропускного режима на предприятии	70	80
		Отсутствие видеонаблюдения	40	60
	Разглашение конфиденциальной информации	Отсутствие соглашения о неразглашении конфиденциальной информации	30	30
		Нечеткое распределение ответственности за документы между сотрудниками предприятия	70	50
	Несанкционированное копирование и печать конфиденциальных документов	Нечеткая организация конфиденциального документооборота	70	50
		Неконтролируемый доступ сотрудников к копировальной технике	70	50
Инженерно-техническая	Съем информации за счет ПЭМИН	Отсутствие генераторов зашумления, экранирования	10	30
		Превышение уровня опасного сигнала за пределами контролируемой зоны	15	40
	Съем информации с телефонной линии	Отсутствие устройств контроля напряжения телефонной линии	30	40
		Не проводятся специальные обследования и проверки при установке нового оборудования, а также при проведении совещаний	20	40
	Пожар	Уязвимости в системе противопожарной сигнализации, истечение срока эксплуатации огнетушителей	70	90
		Отсутствие несгораемого сейфа	20	60

Оценка по экзамену выводится с учетом совокупного результата освоения всех компетенций по дисциплине «Управление информационной безопасностью» (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23).

Критерии оценки результатов сформированности компетенций при использовании различных форм контроля.

Критерии оценивания результатов уровня сформированности компетенций по выполнению лабораторных работ:

Оценки «отлично» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с учетом ГОСТ и требований кафедры, убедительно, полно и развернуто отвечает на вопросы при защите.

Оценки «хорошо» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с учетом ГОСТ и требований кафедры, практически отвечает на вопросы во время защиты.

Оценки «удовлетворительно» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с незначительными отклонениями в требо-

ваниях ГОСТ и кафедры, ошибается в ответах на вопросы во время защиты, но исправляет ошибки при ответе на наводящие вопросы.

Оценки «неудовлетворительно» заслуживает студент, который выполнил не все задания, не обосновал выполнение элементов заданий (не привел цифровые данные, неправильно провел расчеты, не привел факты и пр.), оформил работу с грубыми нарушениями ГОСТ и требований кафедры, практически не отвечает на вопросы во время защиты.

Критерии оценивания экзамена:

Оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявивший творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практические задания.

Оценки «хорошо» заслуживает студент, обнаруживший полное знание материала изученной дисциплины, успешно выполняющий предусмотренные задания, усвоивший основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы, правильно выполнившему практические задания, но допустившему при этом непринципиальные ошибки.

Оценки «удовлетворительно» заслуживает студент, обнаруживший знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей профессиональной деятельности, справляющийся с выполнением заданий, знакомый с основной литературой, рекомендованной рабочей программой дисциплины; допустивший погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающий необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнивший другие практические задания из того же раздела дисциплины.

Оценка «неудовлетворительно» выставляется студенту, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент отказался сдавать зачет или нарушил правила сдачи зачета (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).