МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
Московский политехнический университет

УТВЕРЖДАЮ
Декан транспортного факультета
_____ /П. Итурралде/
«28» 08 2021 г.

Рабочая программа дисциплины
Информационная безопасность

Специальность

23.05.01 Наземные транспортно-технологические средства

Профиль подготовки (образовательная программа)

«Компьютерное моделирование транспортных средств»

Квалификация (степень) выпускника
инженер

Форма обучения
Очная

Москва 2021

1. Цели освоения дисциплины

К **основным целям** освоения дисциплины «Информационная безопасность» следует отнести:

- раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности;
- определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации;
- классификация и характеристика составляющих информационной безопасности и защиты информации.

К **основным задачам** освоения дисциплины «Информационная безопасность» следует отнести:

- раскрытие понятийного аппарата в области информационной безопасности и защиты информации;
- раскрытие базовых содержательных положений в области информационной безопасности и защиты информации;
- раскрытие современной доктрины информационной безопасности;
- определение целей, значения и принципов защиты информации;
- раскрытие методов определения состава защищаемой информации, классификация ее по видам тайны, материальным носителям, собственникам и владельцам;
- установление и раскрытие структуры угроз защищаемой информации;
- раскрытие направлений, видов, методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации;
- установление и раскрытие сущности компонентов защиты информации;
- раскрытие назначения, сущности и структуры систем защиты информации.

2. Место дисциплины в структуре ОП специалитета

Дисциплина «Информационная безопасность» относится к числу учебных дисциплин обязательной части цикла Б.1.1 образовательной программы специалитета (Б1.1.8)

Дисциплина «Информационная безопасность» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП:
«Безопасность жизнедеятельности», «Основы деловой коммуникации», «Правовое регулирование в сфере науки и технологий».

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	**уметь:** корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетные единицы, т.е. **54** академических часа (лекции - 18 часов, лабораторные работы - 36 часов, самостоятельная работа – 90 часов, форма контроля - экзамен) в 1 семестре.

Структура и содержание дисциплины «Информационная безопасность» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

1 семестр

Тема 1. Методология защиты информации

Классификационная схема понятий в области информационной безопасности. Доктрина информационной безопасности Российской Федерации. Стратегия развития информационной безопасности Российской Федерации на 2017-2030 годы. Нормативно-правовая база РФ в области ИБ. Зарубежный опыт правового обеспечения защиты информации. Стандарты и рекомендации по безопасности ISO. Руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК). Свойства информации, подлежащие защите: конфиденциальность, целостность и доступность. Концепция комплексной системы защиты информации. Служебная тайна. Коммерческая тайна. Персональные данные. Государственная тайна. Интеллектуальная собственность и авторское право. Виды объектов информатизации как объектов защиты информации. Классификация угроз информационной безопасности. Модель угроз информационной безопасности. Модель нарушителя. Уровни защиты информации. Политика безопасности. Главные направления работ по защите информации. Организационно-технические мероприятия по защите информации, регламентирующие производственную деятельность предприятия и его работников.

Тема 2. Защита информации в информационных системах от утечки по техническим каналам.

Общая классификация угроз и уязвимостей информационных систем. Методика определения актуальных угроз безопасности. Структура типового технического канала утечки информации (ТКУИ). Классификация ТКУИ. Методы и средства технической защиты информации Классификация технических каналов утечки информации (ТКУИ). Угрозы утечки информации по техническим каналам. Виды аппаратуры для регистрации

побочных электромагнитных излучений и наводок (ПЭМИН). Методика оценки защищенности от утечки информации по техническим каналам.

Тема 3. Защита информации в информационных системах от несанкционированного доступа (НСД)

Угрозы несанкционированного доступа (НСД) к информации. Разновидности угроз НСД и их источники. Уязвимости информационных систем, связанные с НСД. Уязвимости системного и прикладного программного обеспечения. Методы и средства защиты информации от НСД. Матричные и многоуровневые (мандатные) модели разграничения доступа. Основные принципы контроля доступа к ресурсам системы. Диспетчеризация доступа. Идентификация и аутентификация пользователей. Авторизация. Ключи защиты. Современные системы защиты компьютерных систем (КС) от несанкционированного доступа к информации. Характеристика угроз программно-математических воздействий (ПМВ). Виды вредоносных программ. Сетевые угрозы и уязвимости. Возможные последствия от реализации угроз при межсетевом взаимодействии. Выявление угроз НСД за счет межсетевого взаимодействия. Определение класса защищенности информационной системы.

Тема 4. Защита информации с использованием шифровальных (криптографических) средств

Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования. Ключи и алгоритмы шифрования. Методы шифрования с симметричным ключом. Криптографическая система RSA. Электронная цифровая подпись на основе криптографического преобразования. Особенности стандартизации и сертификации криптографических средств.

Тема 5. Система менеджмента информационной безопасностью (СМИБ) на предприятии

Семейство стандартов СМИБ. Управление рисками информационной безопасности. Общее содержание процесса оценки рисков. Анализ уровня рисков. Факторы, влияющие на вероятность реализации угрозы. Методологии оценки рисков по двум и по трем факторам. Субъективная шкала тяжести возможных последствий. Инструментальные средства анализа рисков. Принятие решений по обработке и управлению рисками. Практические правила управления информационной безопасностью. Пример содержания политики информационной безопасности. Основные вопросы управления доступом к информации. Расследование инцидентов в сфере информационной безопасности.

Тема 6.. Комплексная система защиты информации (КСЗИ)

.

Определение КСЗИ. Три основные компоненты создания КСЗИ напредприятии. Моделирование КСЗИ. Этапы создания КСЗИ (Технико-экономическое обоснование,

Техническое задание, эскизный, технический и рабочий проекты. Внедрение и сдача в опытную эксплуатацию. Доработка (при необходимости) и приемка заказчиком системы).

Тема 7. Организация конфиденциального делопроизводства на предприятии.

Организационно-распорядительные документы, регламентирующие порядок конфиденциального делопроизводства. Общероссийский классификатор управленческой документации (ОКУД). Порядок подготовки, оформления документов и учета материальных носителей конфиденциальной информации. Задачи, функции и должностные обязанности сотрудников конфиденциального делопроизводства. Автоматизированные системы электронного конфиденциального делопроизводства (СЭД). Правила делопроизводства в федеральных органах исполнительной власти. Организация контроля за соблюдением исполнителями должностных инструкций.

5. Образовательные технологии

Методика преподавания дисциплины «Информационная безопасность» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение интерактивных лекционных и лабораторных занятий в форме видео уроков;
- подготовка к выполнению лабораторных работ с использованием видео уроков;
– подготовка, представление и обсуждение презентаций на лабораторных занятиях;
- подготовка к экзамену.

Удельный вес занятий, проводимых в интерактивных формах, определен образовательной программой, особенностью контингента обучающихся и содержанием дисциплины «Информационная безопасность» и в целом по дисциплине составляет 50% (27 часов) аудиторных занятий. Занятия лекционного типа составляют 33% (18 часов) от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

-подготовка на лабораторном занятии отчета с презентацией на тему: «Методы и средства защиты информации» (индивидуально для каждого обучающегося) и с ее обсуждением;

Образцы контрольных вопросов и заданий для проведения текущего контроля, экзамена приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК - 7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин, практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ОПК - 7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности				
уметь: корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;	Обучающийся не умеет или в недостаточной степени умеет корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.	Обучающийся демонстрирует неполное соответствие следующих умений: корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих умений: корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие следующих умений: корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися

планируемых результатов обучения дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков, приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков, приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — URL: https://urait.ru/bcode/477968
2. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с.— URL: https://urait.ru/bcode/467370

б) дополнительная литература:

учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — URL: https://urait.ru/bcode/450371

в) программное обеспечение и Интернет-ресурсы:

1. http://knowledgemanagement.report.ru/
2. www.km.improvement.ru2.
3. www.kmclub.ru (Клуб Практиков Управления Знаниями)
4. http://bibliotekar.ru/biznes-29/index.htm
5. http://www.elitarium.ru/psychology/prinjatie_reshenijj/
6. http://www.risk-manage.ru/
7. http://www.genrih-lemke.narod.ru
8. http://all-ib.ru/
9. http://citforum.ru/security/
10. http://securityvulns.ru/
11. http://www.itsec.ru/main.php
12. http://www.securrity.ru/
13. Локальный электронный учебник по направлению «Информационная безопасность» для бакалавров и специалистов. Федоров Н.В. Свидетельство о государственной регистрации программы для ЭВМ № 2013610300.
14. Операционная система Windows 7(или ниже) – Microsoft Open License Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215
15. Офисные приложения, Microsoft Office 2013(или ниже) – Microsoft Open License Лицензия № 61984042

8. Материально-техническое обеспечение дисциплины

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, компьютер, экран) – 1 комплект.

Для проведения лабораторных работ необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Текущий контроль осуществляется на лабораторных занятиях, промежуточный контроль осуществляется на экзамене в письменной и устной форме.

10. Методические рекомендации для преподавателя

Взаимодействие преподавателя со студентами можно разделить на несколько составляющих – лекционные, практические и лабораторные занятия и консультирование. Преподаватель должен последовательно вычитать студентам ряд лекций, в ходе которых следует сосредоточить внимание на ключевых моментах конкретного теоретического материала, а также организовать проведение практических занятий таким образом, чтобы активизировать мышление студентов, стимулировать самостоятельное извлечение ими необходимой информации из различных источников, сравнительный анализ методов

решений, сопоставление полученных результатов, формулировку и аргументацию собственных взглядов на многие спорные проблемы.

Перед началом преподавания преподавателю необходимо:

- изучить рабочую программу, цели и задачи дисциплины;
- четко представлять себе, какие знания, умения и навыки должен приобрести студент;
- познакомится с видами учебной работы;
- изучить содержание разделов дисциплины.

В ходе лекционного занятия преподаватель должен назвать тему, учебные вопросы, ознакомить студентов с перечнем основной и дополнительной литературы по теме занятия.

Во вступительной части лекции обосновать место и роль изучаемой темы в учебной дисциплине, раскрыть ее практическое значение. Если читается не первая лекция, то необходимо увязать ее тему с предыдущей, не нарушая логики изложения учебного материала. Лекцию следует начинать, только чётко обозначив её характер, тему и круг тех вопросов, которые в её ходе будут рассмотрены.

В основной части лекции следует раскрывать содержание учебных вопросов, акцентировать внимание студентов на основных категориях, явлениях и процессах, особенностях их протекания. Раскрывать сущность и содержание различных точек зрения и научных подходов к объяснению тех или иных явлений и процессов. Следует аргументировано обосновать собственную позицию по спорным теоретическим вопросам. Приводить примеры. Задавать по ходу изложения лекционного материала риторические вопросы и самому давать на них ответ. Это способствует активизации мыслительной деятельности студентов, повышению их внимания и интереса к материалу лекции, ее содержанию. Преподаватель должен руководить работой студентов по конспектированию лекционного материала, подчеркивать необходимость отражения в конспектах основных положений изучаемой темы, особо выделяя категорийный аппарат.

В заключительной части лекции необходимо сформулировать общие выводы по теме, раскрывающие содержание всех вопросов, поставленных в лекции. Объявить план очередного семинарского или лабораторного занятия, дать краткие рекомендации по подготовке студентов к семинару или лабораторной работе. Определить место и время консультации студентам, пожелавшим выступить на семинаре с докладами и рефератами по актуальным вопросам обсуждаемой темы.

Цель практических и лабораторных занятий - обеспечить контроль усвоения учебного материала студентами, расширение и углубление знаний, полученных ими на лекциях и в ходе самостоятельной работы. Повышение эффективности практических занятий достигается посредством создания творческой обстановки, располагающей студентов к высказыванию собственных взглядов и суждений по обсуждаемым вопросам, желанию у студентов поработать у доски при решении задач.

После каждого лекционного, лабораторного и практического занятия сделать соответствующую запись в журналах учета посещаемости занятий студентами, выяснить у старост учебных групп причины отсутствия студентов на занятиях. Проводить групповые и индивидуальные консультации студентов по вопросам, возникающим у студентов в ходе их подготовки к текущей и промежуточной аттестации по учебной дисциплине, рекомендовать в помощь учебные и другие материалы, а также справочную литературу.

Экзамен или зачет по дисциплине проводится в форме письменного экзамена с последующей индивидуальной беседой со студентом на основе вопросов, сформулированных в зачетных или экзаменационных билетах. В билет вносится два теоретических и один практический вопрос из различных разделов дисциплины для более полной проверки знаний студентов. Оценка выставляется преподавателем и объявляется после ответа. Преподаватель принимающий зачет или экзамен лично несет ответственность за правильность выставления оценки.

Приложение

Структура и содержание дисциплины «Информационная безопасность»
по направлению подготовки 23.05.01 "Наземные транспортно-технологические средства"

Образовательная программа (профиль)
«Компьютерное моделирование транспортных средств»
Форма обучения
Очная
Год приема - 2021
(специалист)

/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб.	СРС	КСР	К.Р.	К.П.	РГР	Реферат	К/р	Э	З
	Пятый семестр														
	Тема 1. Методология защиты информации	1	1	2		2	6								
	Тема 1. Методология защиты информации	1	2			4	6					+			
	Тема 2. Защита информации в информационных системах от утечки по техническим каналам.	1	3	2		2	8								
	Тема 2. Защита информации в информационных системах от утечки по техническим каналам.	1	4			4	6					+			
	Тема 3. Защита информации в информационных системах от несанкционированного доступа (НСД)	1	5	2		2	8								
	Тема 3. Защита информации в информационных системах от несанкционированного доступа (НСД)	1	6			4	6					+			
	Тема 4. Защита информации с использованием шифровальных (криптографических) средств	1	7	2		2	8								
	Тема 4. Защита информации с использованием шифровальных (криптографических) средств	1	8			4	6					+			
	Тема 5. Система менеджмента информационной безопасностью (СМИБ) на предприятии	1	9	4			8								
	Тема 5. Система менеджмента информационной	1	10			4	6					+			

	безопасностью (СМИБ) на предприятии														
	Тема 6.. Комплексная система защиты информации (КСЗИ)	1	11	4			8								
	Тема 6.. Комплексная система защиты информации (КСЗИ)	1	12			4	6					+			
	Тема 7. Организация конфиденциального делопроизводства на предприятии.	1	13	2		**4**	8					+			
	Форма аттестации													Э	
	Всего часов по дисциплине в первом семестре		144	18		36	90							3	
	Всего часов по дисциплине		144	18		36	90							3	

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 23.05.01 "Наземные транспортно-технологические средства"

ОП (профиль): «Компьютерное моделирование транспортных средств»

Форма обучения: очная

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Информационная безопасность»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Тематика докладов и сообщений

Темы рефератов

Вопросы для текущего контроля

Вопросы для самостоятельного изучения

Экзамен

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Информационная безопасность					
ФГОС ВО					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие общекультурные и общепрофессиональные компетенции:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средства**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ОПК - 7	способностью понимать сущность и значение информации в развитии современного информационного общества, способностью сознавать опасности и угрозы, возникающие в этом процессе, способностью соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	**уметь:** корректно выбрать и применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;	лекция, самостоятельная работа, практические занятия	Реферат, экзамен	**Базовый уровень:** -уметь корректно выбрать при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики **Повышенный уровень:** -уметь корректно применять при решении профессиональных задач методы и средства информационной безопасности и защиты интересов личности, общества и государства,

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы

Примерная тематика рефератов по курсу
«Информационная безопасность»

1. Новые информационные технологии – новые возможности, новые угрозы
2. Перспективы развития средств ЗИ
3. Новые информационно-коммункационные технологии
4. Мобильные телекоммуникационные устройства
5. Робототехника и мехатроника и перспективы их развития
6. Нанотехнологии и перспективы их применения в ЗИ
7. Сетевые технологии и средства ЗИ
8. Информационное оружие и информационные войны
9. Квантовые компьютеры и криптография
10. Связь ИБ и гудвилла компании
11. Правовое обеспечение защиты интеллектуальной собственности компании

Вопросы для текущего контроля:

Тема 1. Методология защиты информации

1. Доктрина информационной безопасности Российской Федерации. Стратегия развития информационной безопасности Российской Федерации на 2017-2030 годы.
2. Нормативно-правовая база РФ в области ИБ. Источники знаний в компании.
3. Зарубежный опыт правового обеспечения защиты информации. Стандарты и рекомендации по безопасности ISO.
4. Руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК).
5. Свойства информации, подлежащие защите: конфиденциальность, целостность и доступность.
6. Концепция комплексной системы защиты информации. Служебная тайна. Коммерческая тайна. Персональные данные. Государственная тайна.
7. Интеллектуальная собственность и авторское право.
8. Виды объектов информатизации как объектов защиты информации.
9. Классификация угроз информационной безопасности. Модель угроз информационной безопасности. Модель нарушителя.
10. Уровни защиты информации.
11. Политика безопасности. Главные направления работ по защите информации.
12. Организационно-технические мероприятия по защите информации, регламентирующие производственную деятельность предприятия и его работников.

Тема 2. Защита информации в информационных системах от утечки по техническим каналам.

1. Общая классификация угроз и уязвимостей информационных систем.
2. Методика определения актуальных угроз безопасности.

3. Структура типового технического канала утечки информации (ТКУИ). Классификация ТКУИ.
4. Методы и средства технической защиты информации
5. Классификация технических каналов утечки информации (ТКУИ).
6. Угрозы утечки информации по техническим каналам.
7. Виды аппаратуры для регистрации побочных электромагнитных излучений и наводок (ПЭМИН).
8. Методика оценки защищенности от утечки информации по техническим каналам.

Тема 3. Защита информации в информационных системах от несанкционированного доступа (НСД)

1. Угрозы несанкционированного доступа (НСД) к информации. Разновидности угроз НСД и их источники.
2. Уязвимости информационных систем, связанные с НСД.
3. Уязвимости системного и прикладного программного обеспечения. Методы и средства защиты информации от НСД.
4. Матричные и многоуровневые (мандатные) модели разграничения доступа.
5. Основные принципы контроля доступа к ресурсам системы. Диспетчеризация доступа. Идентификация и аутентификация пользователей. Авторизация. Ключи защиты.
6. Современные системы защиты компьютерных систем (КС) от несанкционированного доступа к информации.
7. Характеристика угроз программно-математических воздействий (ПМВ).
8. Виды вредоносных программ.
9. Сетевые угрозы и уязвимости. Возможные последствия от реализации угроз при межсетевом взаимодействии.
10. Выявление угроз НСД за счет межсетевого взаимодействия.
11. Определение класса защищенности информационной системы.

Тема 4. Защита информации с использованием шифровальных (криптографических) средств

1. Введение в криптологию. Исторический обзор.
2. Криптография и криптоанализ.
3. Понятие криптостойкости системы защиты информации.
4. Шифрование как метод криптографического преобразования.
5. Ключи и алгоритмы шифрования.
6. Методы шифрования с симметричным ключом.
7. Криптографическая система RSA.
8. Электронная цифровая подпись на основе криптографического преобразования.
9. Особенности стандартизации и сертификации криптографических средств.

Тема 5. Система менеджмента информационной безопасностью (СМИБ) на предприятии

1. Семейство стандартов СМИБ. Управление рисками информационной безопасности.
2. Общее содержание процесса оценки рисков. Анализ уровня рисков.
3. Факторы, влияющие на вероятность реализации угрозы.
4. Методологии оценки рисков по двум и по трем факторам.
5. Субъективная шкала тяжести возможных последствий.

6. Инструментальные средства анализа рисков. Принятие решений по обработке и управлению рисками.
7. Практические правила управления информационной безопасностью.
8. Пример содержания политики информационной безопасности.
9. Основные вопросы управления доступом к информации.
10. Расследование инцидентов в сфере информационной безопасности.

Тема 6.. Комплексная система защиты информации (КСЗИ)

.

1. Определение КСЗИ.
2. Три основные компоненты создания КСЗИ на предприятии.
3. Моделирование КСЗИ.
4. Этапы создания КСЗИ (технико-экономическое обоснование, Техническое задание, эскизный, технический и рабочий проекты. Внедрение и сдача в опытную эксплуатацию, доработка (при необходимости) и приемка заказчиком системы).

Тема 7. Организация конфиденциального делопроизводства на предприятии.

1. Организационно-распорядительные документы, регламентирующие порядок конфиденциального делопроизводства.
2. Общероссийский классификатор управленческой документации (ОКУД).
3. Порядок подготовки, оформления документов и учета материальных носителей конфиденциальной информации.
4. Задачи, функции и должностные обязанности сотрудников конфиденциального делопроизводства.
5. Автоматизированные системы электронного конфиденциального делопроизводства (СЭД).
6. Правила делопроизводства в федеральных органах исполнительной власти.
7. Организация контроля за соблюдением исполнителями должностных инструкций.

Вопросы для самостоятельного изучения

1. Информационная безопасность (ИБ) как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
2. Нормативно-правовая база РФ в области ИБ.
3. Зарубежный опыт правового обеспечения защиты информации. Стандарты и рекомендации по безопасности ISO.
5. Руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК).
6. Свойства информации, подлежащие защите: конфиденциальность, целостность и доступность.
7. Концепция комплексной системы защиты информации. Служебная тайна. Коммерческая тайна. Персональные данные. Государственная тайна.
8. Интеллектуальная собственность и авторское право.
9. Виды объектов информатизации как объектов защиты информации.
10. Классификация угроз информационной безопасности. Модель угроз информационной безопасности. Модель нарушителя.
11. Уровни защиты информации.

12. Политика безопасности предприятия.. Главные направления работ по защите информации.
13. Организационно-технические мероприятия по защите информации, регламентирующие производственную деятельность предприятия и его работников.
14. Общая классификация угроз и уязвимостей информационных систем.
15. Методика определения актуальных угроз безопасности.
16. Структура типового технического канала утечки информации (ТКУИ). Классификация ТКУИ.
17. Методы и средства технической защиты информации
18. Классификация технических каналов утечки информации (ТКУИ).
19. Угрозы утечки информации по техническим каналам.
20. Виды аппаратуры для регистрации побочных электромагнитных излучений и наводок (ПЭМИН).
21. Методика оценки защищенности от утечки информации по техническим каналам. Угрозы несанкционированного доступа (НСД) к информации.
22. Разновидности угроз НСД и их источники.
23. Уязвимости информационных систем, связанные с НСД.
24. Уязвимости системного и прикладного программного обеспечения. Методы и средства защиты информации от НСД.
25. Матричные и многоуровневые (мандатные) модели разграничения доступа.
26. Основные принципы контроля доступа к ресурсам системы. Диспетчеризация доступа. Идентификация и аутентификация пользователей. Авторизация. Ключи защиты.
27. Современные системы защиты компьютерных систем (КС) от несанкционированного доступа к информации.
28. Характеристика угроз программно-математических воздействий (ПМВ).
29. Виды вредоносных программ.
30. Сетевые угрозы и уязвимости. Возможные последствия от реализации угроз при межсетевом взаимодействии.
31. Выявление угроз НСД за счет межсетевого взаимодействия.
32. Определение класса защищенности информационной системы.
33. Общие понятия, история развития и классификация криптографических средств.
34. Криптография и криптоанализ. Общая характеристика различных методов шифрования.
35. Понятие криптостойкости системы защиты информации.
36. Шифрование как метод криптографического преобразования.
37. Ключи и алгоритмы шифрования.
38. Методы шифрования с симметричным ключом.
39. Криптографическая система RSA.
40. Электронная цифровая подпись на основе криптографического преобразования.
41. Особенности стандартизации и сертификации криптографических средств. Отечественные и зарубежные стандарты шифрования.
42. Общая характеристика и классификация компьютерных вирусов.
43. Семейство стандартов СМИБ. Управление рисками информационной безопасности.
44. Общее содержание процесса оценки рисков. Анализ уровня рисков.
45. Факторы, влияющие на вероятность реализации угрозы.
46. Методологии оценки рисков по двум и по трем факторам.
47. Субъективная шкала тяжести возможных последствий.
48. Инструментальные средства анализа рисков. Принятие решений по обработке и управлению рисками.
49. Практические правила управления информационной безопасностью.
50. Управление доступом к информации.
51. Расследование инцидентов в сфере информационной безопасности.
52. Три основные компоненты создания КСЗИ на предприятии.

53. Моделирование КСЗИ.
54. Этапы создания КСЗИ (технико-экономическое обоснование, Техническое задание, эскизный, технический и рабочий проекты. Внедрение и сдача в опытную эксплуатацию, доработка (при необходимости) и приемка заказчиком системы).

55. Организационно-распорядительные документы, регламентирующие порядок конфиденциального делопроизводства.
56. Общероссийский классификатор управленческой документации (ОКУД).
57. Порядок подготовки, оформления документов и учета материальных носителей конфиденциальной информации.
58. Задачи, функции и должностные обязанности сотрудников конфиденциального делопроизводства.
59. Автоматизированные системы электронного конфиденциального делопроизводства (СЭД).
60. Правила делопроизводства в федеральных органах исполнительной власти.
61. Организация контроля за соблюдением исполнителями должностных инструкций.
62. Составляющие и источники рисков в управлении.
63. Подходы к организации защиты коммерческой тайны на предприятии
64. Служба безопасности на предприятии. Функции службы безопасности на предприятии
65. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
66. Идентификация и аутентификация субъектов доступа к ресурсам информационной системы. Парольные методы и оценка их эффективности. Биометрические методы.

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Информационная безопасность (ИБ) как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
2. Нормативно-правовая база РФ в области ИБ.
3. Зарубежный опыт правового обеспечения защиты информации. Стандарты и рекомендации по безопасности ISO.
4. Руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК).
5. Свойства информации, подлежащие защите: конфиденциальность, целостность и доступность.
6. Концепция комплексной системы защиты информации. Служебная тайна. Коммерческая тайна. Персональные данные. Государственная тайна.
7. Интеллектуальная собственность и авторское право.
8. Виды объектов информатизации как объектов защиты информации.
9. Классификация угроз информационной безопасности. Модель угроз информационной безопасности. Модель нарушителя.
10. Уровни защиты информации.
11. Политика безопасности предприятия.. Главные направления работ по защите информации.

12. Организационно-технические мероприятия по защите информации, регламентирующие производственную деятельность предприятия и его работников.
13. Общая классификация угроз и уязвимостей информационных систем.
14. Методика определения актуальных угроз безопасности.
15. Структура типового технического канала утечки информации (ТКУИ). Классификация ТКУИ.
16. Методы и средства технической защиты информации
17. Классификация технических каналов утечки информации (ТКУИ).
18. Угрозы утечки информации по техническим каналам.
19. Виды аппаратуры для регистрации побочных электромагнитных излучений и наводок (ПЭМИН).
20. Методика оценки защищенности от утечки информации по техническим каналам. Угрозы несанкционированного доступа (НСД) к информации.
21. Разновидности угроз НСД и их источники.
22. Уязвимости информационных систем, связанные с НСД.
23. Уязвимости системного и прикладного программного обеспечения. Методы и средства защиты информации от НСД.
24. Матричные и многоуровневые (мандатные) модели разграничения доступа.
25. Основные принципы контроля доступа к ресурсам системы. Диспетчеризация доступа. Идентификация и аутентификация пользователей. Авторизация. Ключи защиты.
26. Современные системы защиты компьютерных систем (КС) от несанкционированного доступа к информации.
27. Характеристика угроз программно-математических воздействий (ПМВ).
28. Виды вредоносных программ.
29. Сетевые угрозы и уязвимости. Возможные последствия от реализации угроз при межсетевом взаимодействии.
30. Выявление угроз НСД за счет межсетевого взаимодействия.
31. Определение класса защищенности информационной системы.
32. Общие понятия, история развития и классификация криптографических средств.
33. Криптография и криптоанализ. Общая характеристика различных методов шифрования.
34. Понятие криптостойкости системы защиты информации.
35. Шифрование как метод криптографического преобразования.
36. Ключи и алгоритмы шифрования.
37. Методы шифрования с симметричным ключом.
38. Криптографическая система RSA.
39. Электронная цифровая подпись на основе криптографического преобразования.
40. Особенности стандартизации и сертификации криптографических средств. Отечественные и зарубежные стандарты шифрования.
41. Общая характеристика и классификация компьютерных вирусов.
42. Семейство стандартов СМИБ. Управление рисками информационной безопасности.
43. Общее содержание процесса оценки рисков. Анализ уровня рисков.
44. Факторы, влияющие на вероятность реализации угрозы.
45. Методологии оценки рисков по двум и по трем факторам.
46. Субъективная шкала тяжести возможных последствий.
47. Инструментальные средства анализа рисков. Принятие решений по обработке и управлению рисками.
48. Практические правила управления информационной безопасностью.
49. Управление доступом к информации.
50. Расследование инцидентов в сфере информационной безопасности.
51. Три основные компоненты создания КСЗИ на предприятии.
52. Моделирование КСЗИ.

53. Этапы создания КСЗИ (технико-экономическое обоснование, Техническое задание, эскизный, технический и рабочий проекты. Внедрение и сдача в опытную эксплуатацию, доработка (при необходимости) и приемка заказчиком системы).
54.
55. Организационно-распорядительные документы, регламентирующие порядок конфиденциального делопроизводства.
56. Общероссийский классификатор управленческой документации (ОКУД).
57. Порядок подготовки, оформления документов и учета материальных носителей конфиденциальной информации.
58. Задачи, функции и должностные обязанности сотрудников конфиденциального делопроизводства.
59. Автоматизированные системы электронного конфиденциального делопроизводства (СЭД).
60. Правила делопроизводства в федеральных органах исполнительной власти.
61. Организация контроля за соблюдением исполнителями должностных инструкций.
62. Составляющие и источники рисков в управлении.
63. Подходы к организации защиты коммерческой тайны на предприятии
64. Служба безопасности на предприятии. Функции службы безопасности на предприятии
65. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
66. Идентификация и аутентификация субъектов доступа к ресурсам информационной системы. Парольные методы и оценка их эффективности. Биометрические методы.