МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

"28" 04 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки
09.03.03 Прикладная информатика
Образовательная программа (профиль подготовки)
«Большие и открытые данные»

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Москва 2022

Программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению **09.03.03 «Прикладная информатика»** и профилю подготовки **«Большие и открытые данные».**

Программу составил

_____/В.Г. Евтихов/

Программа дисциплины утверждена на заседании кафедры «Прикладная информатика»
«____» августа 2022 г. протокол № _____

Заведующий кафедрой
доцент, к.э.н.  /С.В.Суворов/

Программа согласована с руководителем образовательной программы по направлению подготовки **09.03.03 «Прикладная информатика»** по профилю подготовки **«Большие и открытые данные».**

_____ С.В.Суворов/
«____» августа 2022 г.

Программа утверждена на заседании учебно-методической комиссии факультета Информационных технологий

Председатель комиссии  /Д. Г. Демидов/

«____»_____2022 г. Протокол:

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 бакалавриата

Дисциплина «Информационная безопасность» относится к числу профессиональных учебных дисциплин базовой части цикла Б.1.1 образовательной программы бакалавриата (Б1.1.14).

Дисциплина «Информационная безопасность» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП: «Вычислительные системы, сети, телекоммуникации», «Операционные системы», «Базы данных», «Электронный бизнес и рынки ИКТ» , «Информационные системы и технологии», «Современные интернет-технологии», « Проектирование информационных систем».

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
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности	**знать:** значение информации в развитии современного общества; **уметь:** использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства;

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетные единицы, т.е. 216 академических часов (лекции - 54 часов, лабораторные занятия – 54 часов, самостоятельная работа – 108 часов, форма контроля - экзамен) в 4 и 5 семестре.

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

Содержание разделов дисциплины

4 семестр

Тема 1.Управление знаниями и рисками предприятия

Управление знаниями, как новая функция управления Структура системы знаний. Процесс управления знаниями. Основные компоненты в управлении знаниями. Знания как информационное оружие. Источники знаний в компании. Операционно-тактические и стратегические преимущества от применения управления знаниями в бизнесе. Методы и проблемы в управлении знаниями. Подготовка и планирование внедрения знаний. Перспективы применения управления знаниями в бизнесе. Внедрение системы управления знаниями и ее развитие. Общение и обучение. Анализ хода реализации проекта. Приоритеты управления и полный вектор управления. Модели для выявления и анализа возможностей, рисков и угроз. Методы прогнозирования рисков. Прогнозное планирование: определение рисков и поиск возможностей.

Тема 2. Экономическая безопасность

Криминальная конкуренция. Предпринимательская деятельность как объект экономической и информационной безопасности. Структура управления экономической и информационной безопасностью. Состав и структура информации в системе экономической и информационной безопасности. Коммерческая тайна. Информационное обеспечение внутрифирменной службы безопасности. Информационное обеспечение государственного регулирования в сфере безопасности Обеспечение экономической и информационной безопасности предприятия как функция инфраструктуры рыночной экономики Приоритеты

фирменной службы безопасности. Служба безопасности на предприятии Типичные экономико-правовые ситуации в бизнесе. Способы защиты прав и разрешения конфликтов. Личная финансовая безопасность Национальная экономическая безопасность.

Тема 3. Защита информации как объективная закономерность эволюции постиндустриального общества

Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Императив устойчивого развития. Глобализация информационных отношений. Информация как предмет труда. Информационные технологии. Информационные ресурсы. Информационные продукты и услуги. Информационный рынок. Объективная необходимость и общественная потребность в защите информации. Информация как объект правовой защиты. Сущность, общее содержание и цели защиты информации. Правовое регулирование вопросов защиты информации.

Тема 4. Информационная безопасность личности, общества и государства: социально-правовые аспекты

Право на информацию в системе гражданских прав личности. Возможные ограничения данного права. Массовая информация и информация ограниченного доступа. Неприкосновенность частной жизни, персональные данные. Конфиденциальность и секретность. Институт тайн. Коммерческая тайна. Государственная тайна. Права и обязанности собственника, владельца и потребителя информационных продуктов. Интеллектуальная собственность и авторское право. Информационная безопасность в сфере национальной безопасности РФ. Информационные войны, информационное оружие и информационный терроризм. Составляющие национальных интересов РФ в информационной сфере. Доктрина информационной безопасности РФ. Гарантии и правовые механизмы соблюдения прав и свобод граждан РФ при обеспечении информационной безопасности. Международные и отечественные нормативные и руководящие документы в области информационной безопасности и защиты информации.

Тема 5. Системный анализ угроз безопасности в компьютерных системах

Структурная и функциональная организация информационных компьютерных систем (КС). КС как объект защиты. Содержательная сущность защиты КС. Структурные и функциональные компоненты КС, нуждающиеся в защите. Системная классификация (таксономия) и обобщенный анализ возможных угроз информационной безопасности. Уязвимость информации и ее оценка. Виды, происхождение, предпосылки появления и источники угроз информационной безопасности. Последствия таких угроз. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации, побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей. Модель нарушителя информационной безопасности. Несанкционированная модификация структур КС в процессе эксплуатации. Традиционные методы промышленного шпионажа. Утечка информации по техническим каналам. Несанкционированное получение информации. Саморепродуцирующиеся вредительские программы.

Тема 6. Общая характеристика средств и методов защиты информации

Основные принципы реализации систем защиты информации. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности. Архитектура безопасности информационных систем. Политика безопасности.

Классификация и общая характеристика основных методов и средств защиты информации в компьютерных системах. Правовые и организационные средства защиты информации. Технические и технологические средства и методы защиты. Программно-аппаратные средства защиты. Криптографические методы защиты информации. Концепция комплексной системы защиты информации.

Тема 7. Организационно-правовое обеспечение защиты информации

Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима. Регламентация доступа персонала к информационным и вычислительным ресурсам. Организация работы с конфиденциальными документами. Учет, хранение, использование и уничтожение документов (носителей) с конфиденциальной информацией. Организация контроля за соблюдением исполнителями должностных инструкций. Правовое регулирование в сфере информационных отношений. Законодательство РФ в этой области. Зарубежный опыт правового обеспечения защиты информации. Стандартизация в области обеспечения информационной безопасности. Международные и отечественные нормативные и руководящие документы, связанные с информационной безопасностью. Стандарты и рекомендации по безопасности ISO. Руководящие документы Гостехкомиссии РФ.

Тема 8. Защита информации в компьютерных системах от несанкционированного вмешательства

Защита информации в компьютерных системах от несанкционированного доступа. Матричные и многоуровневые (мандатные) модели разграничения доступа. Основные принципы контроля доступа к ресурсам системы. Диспетчеризация доступа. Идентификация и аутентификация субъектов доступа. Пароли. Ключи защиты. Современные системы защиты персональных ЭВМ от несанкционированного доступа к информации.

Тема 9. Криптографические методы защиты

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 10. Компьютерные вирусы и антивирусные программные средства

Компьютерные вирусы как специальный класс саморепродуцирующихся вредительских программ. Вирусные атаки. Модели распространения вирусных программ. Классификация компьютерных вирусов. Файловые, загрузочные, сетевые вирусы. Вирусы и операционные системы. Вирусные программы: черви, троянский конь , макровирусы, мутанты, невидимки, логические бомбы и другие. Методы и средства антивирусной защиты. Программные средства обнаружения вирусов. Программы-сканеры, сторожа, ревизоры, детекторы и другие. Эвристические анализаторы. Методы устранения последствий заражения вирусами. Программы-доктора, программы- вакцины. Действия

пользователя при обнаружении заражения вирусами. Профилактика заражения вирусами компьютерных систем.

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 практических занятий в форме видеоуроков;
- подготовка к выполнению практических работ с использованием видеоуроков;
– подготовка, представление и обсуждение презентаций на практических 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 25% аудиторных занятий. Занятия лекционного типа составляют 33% 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 и выступление на практическом занятии 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, зачета 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
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности

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.

ОК-4 способностью использовать основы правовых знаний в различных сферах деятельност коммуникационных технологий и с учетом основных требований информационной безопасности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: значение информации в развитии современного общества;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: значение информации в развитии современного общества.	Обучающийся демонстрирует неполное соответствие следующих знаний: значение информации в развитии современного общества. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих знаний: значение информации в развитии современного общества, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: значение информации в развитии современного общества, свободно оперирует приобретенными знаниями.
уметь: использовать основы правовых знаний в различных сферах деятельности коммуникационн ых технологий и с учетом основных требований информационной безопасности;	Обучающийся не умеет или в недостаточной степени умеет использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности.	Обучающийся демонстрирует неполное соответствие следующих умений: использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности. 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: использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие следующих умений: использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности.. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности

владеть: высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства;	Обучающийся не владеет или в недостаточной степени владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.	Обучающийся владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях	Обучающийся частично владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, свободно применяет полученные навыки 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 по 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 показателям, 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 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. — 416 с.: ил.; 60×90 1/16. — (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз. — Режим доступа: http://znanium.com/bookread.php?book=423927

б) дополнительная литература:

1 Теория информационной безопасности и методология защиты информации: учебное пособие/ Загинайлов Ю. Н.:- М. – Берлин, Изд-во Директ-Медиа 2015 г. 253 с. . http://www.knigafund.ru/books/181420—

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

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Направление подготовки: 09.03.03 "Прикладная информатика"

ОП (профиль): «Прикладная информатика»

Форма обучения: заочная

Вид профессиональной деятельности: проектная; производственно-технологическая; аналитическая.

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, 2022 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Информационная безопасность					
ФГОС ВО 09.03.03 «Прикладная информатика»					
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**				
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности	**знать:** значение информации в развитии современного общества; **уметь:** использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства;	лекция, самостоятельная работа, практические и лабораторные занятия	Доклад, реферат, экзамен	**Базовый уровень** знать значение информации в развитии современного общества; уметь использовать основы правовых знаний в различных сферах деятельности коммуникационных технологий и с учетом основных требований информационной безопасности. **Повышенный уровень** -владеть высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

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

Примерная тематика докладов и сообщений по курсу «Информационная безопасность»

1. Новые информационно-коммункационные технологии
2. Виртуальная реальность
3. Мобильные телекоммуникационные устройства
4. Робототехника и мехатроника и перспективы их развития
5. Нанотехнологии и перспективы их применения
6. Сетевые технологии и электронная коммерция
7. Информационное оружие и информационные войны
8. Квантовые компьютеры и криптография

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.Управление знаниями и рисками предприятия.

1. Управление знаниями, как новая функция управления
2. Структура и процесс управления знаниями.
3. Основные компоненты в управлении знаниями. Знания как информационное оружие.
4. Источники знаний в компании.
5. Операционно-тактические и стратегические преимущества от применения управления знаниями в бизнесе.
6. Методы и проблемы в управлении знаниями.
7. Приоритеты управления и полный вектор управления.
8. Модели для выявления и анализа возможностей, рисков и угроз.
9. Методы прогнозирования рисков.
10. Прогнозное планирование: определение рисков и поиск возможностей.

Тема 2. Экономическая безопасность.

1. Предпринимательская деятельность как объект экономической и информационной безопасности.
2. Структура управления экономической и информационной безопасностью.
3. Состав и структура информации в системе экономической и информационной безопасности.
4. Коммерческая тайна.
5. Информационное обеспечение внутрифирменной службы безопасности.
6. Информационное обеспечение государственного регулирования в сфере безопасности
7. Приоритеты фирменной службы безопасности.
8. Служба безопасности на предприятии
9. Типичные экономико-правовые ситуации в бизнесе. Способы защиты прав и разрешения конфликтов.
10. Национальная экономическая безопасность.

Тема 3. Защита информации как объективная закономерность эволюции постиндустриального общества.

1. Эволюция информационных процессов и информационных отношений.
2. Сущность и цели информатизации. Императив устойчивого развития.
3. Глобализация информационных отношений.
4. Информация как предмет труда.
5. Информационные технологии. Информационные ресурсы.

6. Информационные продукты и услуги, информационный рынок.
7. Объективная необходимость и общественная потребность в защите информации.
8. Информация как объект правовой защиты.
9. Сущность, общее содержание и цели защиты информации.
10. Правовое регулирование вопросов защиты информации.

Тема 4. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

1. Право на информацию в системе гражданских прав личности.
2. Массовая информация и информация ограниченного доступа.
3. Неприкосновенность частной жизни, персональные данные.
4. Конфиденциальность и секретность.
5. Институт тайн. Коммерческая тайна. Государственная тайна.
6. Интеллектуальная собственность и авторское право.
7. Информационная безопасность в сфере национальной безопасности РФ. Доктрина информационной безопасности РФ.
8. Информационные войны, информационное оружие и информационный терроризм.
9. Гарантии и правовые механизмы соблюдения прав и свобод граждан РФ при обеспечении информационной безопасности.
10. Международные и отечественные нормативные и руководящие документы в области информационной безопасности и защиты информации.

Тема 5. Системный анализ угроз безопасности в компьютерных системах.

1. Структурная и функциональная организация информационных компьютерных систем (КС). КС как объект защиты.
2. Содержательная сущность защиты КС. Уязвимость информации и ее оценка.
3. Структурные и функциональные компоненты КС, нуждающиеся в защите.
4. Системная классификация и обобщенный анализ возможных угроз информационной безопасности.
5. Виды, происхождение, предпосылки появления и источники угроз информационной безопасности и последствия таких угроз.
6. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации, побочные влияния внешней среды.
7. Преднамеренные угрозы, злоумышленные действия людей. Модель нарушителя информационной безопасности.
8. Несанкционированная модификация структур КС в процессе эксплуатации.
9. Традиционные методы промышленного шпионажа.
10. Несанкционированное получение информации.

Тема 6. Общая характеристика средств и методов защиты информации.

1. Основные принципы реализации систем защиты информации.
2. Модели безопасности.
3. Уровни иерархии в обеспечении информационной безопасности.
4. Архитектура безопасности информационных систем.
5. Политика безопасности.
6. Правовые и организационные средства защиты информации.
7. Технические и технологические средства и методы защиты.
8. Программно-аппаратные средства защиты.
9. Криптографические методы защиты информации.
10. Концепция комплексной системы защиты информации.

Тема 7. Организационно-правовое обеспечение защиты информации.

1. Организационные мероприятия по защите информации.
2. Назначение и задачи служб безопасности. Создание контрольно-пропускного режима.
3. Регламентация доступа персонала к информационным и вычислительным ресурсам. Организация работы с конфиденциальными документами.
4. Учет, хранение, использование и уничтожение документов (носителей) с конфиденциальной информацией.
5. Организация контроля за соблюдением исполнителями должностных инструкций.
6. Законодательство РФ в этой области.
7. Зарубежный опыт правового обеспечения защиты информации.
8. Международные и отечественные нормативные и руководящие документы, связанные с информационной безопасностью.
9. Стандарты и рекомендации по безопасности ISO.
10. Руководящие документы Гостехкомиссии РФ.

Тема 8. Защита информации в компьютерных системах от несанкционированного вмешательства.

1. Защита информации в компьютерных системах от несанкционированного доступа.
2. Матричные и многоуровневые (мандатные) модели разграничения доступа.
3. Основные принципы контроля доступа к ресурсам системы.
4. Пароли. Ключи защиты.
5. Современные системы защиты персональных ЭВМ от несанкционированного доступа к информации.

Тема 9. Криптографические методы защиты.

1. Введение в криптологию. Исторический обзор. Криптография и криптоанализ.
2. Понятие криптостойкости системы защиты информации.
3. Шифрование как метод криптографического преобразования.
4. Ключи и алгоритмы шифрования. Методы шифрования с симметричным ключом. Методы замены (подстановки) и перестановки. Гаммирование.
5. Шифрование, использующее генераторы (датчики) псевдослучайных последовательностей.
6. Системы блочного шифрования на основе отечественного ГОСТа и стандарта DES (США).
7. Системы несимметричного шифрования: с открытым ключом для шифрования и закрытым - для дешифрования. Односторонние функции.
8. Криптографическая система RSA.
9. Электронная цифровая подпись на основе криптографического преобразования.
10. Особенности стандартизации и сертификации криптографических средств.

Тема 10. Компьютерные вирусы и антивирусные программные средства.

1. Компьютерные вирусы как специальный класс саморепродуцирующихся вредительских программ. Вирусные атаки как форма радиоэлектронной борьбы.
2. Модели распространения вирусных программ. Классификация компьютерных вирусов.
3. Вирусы и операционные системы. Файловые, загрузочные, сетевые вирусы.
4. Вирусные программы: черви, троянский конь, макровирусы, мутанты, невидимки, логические бомбы и другие.
5. Методы и средства антивирусной защиты. Программные средства обнаружения вирусов.
6. Программы-сканеры, сторожа, ревизоры, детекторы и другие. Эвристические анализаторы.
7. Методы устранения последствий заражения вирусами.
8. Программы-доктора, программы-вакцины.
9. Действия пользователя при обнаружении заражения вирусами.
10. Профилактика заражения вирусами компьютерных систем.

Вопросы для самостоятельного изучения

1. Интеллектуальный капитал (интеллектуальные активы) компании
2. Данные, информация знания (в контексте управления знаниями)

3. Классификации знаний (явные/неявные, формализованные/неформализованные)
4. Модель трансформации знаний в организации («спираль знаний» Нонака, Такеучи)
5. Знание как конкурентный ресурс
6. Проблема сохранения и развития интеллектуального капитала организации
7. Пятифазная модель создания организационного знания (Нонака, Такеучи)
8. Тактические процессы: приобретение/поиск знаний, сохранение знаний, использование знаний, распространение знаний
9. Инструменты управления знаниями: организационный, HR и информационно-технологический подходы
10. Стимулирование разработки и внедрение инноваций в организации. Формализация знаний
11. Обучение персонала и обучающаяся организация
12. Приоритеты управления как виды оружия
13. Структура полного вектора управления
14. Методы и технологии идентификации используемые при оценке рисков
15. Организация разработки решений руководителем на основе системного анализа складывающейся обстановки
16. Факторы, определяющие эффективность решений
17. Концепции, принципы и парадигмы разработки решений
18. Модель проблемной ситуации
19. Процесс разработки решений в сложных ситуациях
20. Содержание процесса обоснования решений
21. Критерии принятия решений и их шкалы .
22. Содержание процесса принятия решений
23. Общая характеристика проблемы коммуникации в процессе разработки решений в сложных ситуациях
24. Содержание процесса контроля
25. Постановки и основные методы решения базовых задач обоснования решений
26. Задача формирования исходного множества альтернатив и их оценки
27. Постановка задачи обоснования решений в условиях определенности
28. Составляющие и источники рисков в управлении
29. Технологии принятия решений при стохастическом риске
30. Технологии принятия решений при поведенческом риске
31. Технология ведения деловых бесед
32. Понятие ЭИБ. Объект и субъект управления в сфере ЭИБ
33. Принципы и факторы, определяющие эффективность управления в сфере ЭИБ
34. Важнейшие признаки предпринимательства с позиций его безопасности
35. Виды бизнеса в России. Особенности управления ЭИБ в России

36. Система управления ЭИБ предприятия
37. Понятие и субъекты криминальной конкуренции
38. Основные функции и группы объектов безопасности в предпринимательской деятельности
39. Структура информации, необходимой для анализа условий предпринимательской деятельности с точки зрения ее безопасности
40. Понятие коммерческой тайны и структура информации, составляющей коммерческую тайну
41. Структура информации с позиций обеспечения безопасности предприятия
42. Структура информации о фактах криминальной конкуренции
43. Информационная база и процедуры, осуществляемые в целях внутрифирменного управления в сфере безопасности
44. Подходы к организации защиты коммерческой тайны на предприятии
45. Информационная база государственного регулирования в сфере безопасности предпринимательства
46. Обеспечение ЭИБ предприятия как функция инфраструктуры рыночной экономики
47. Организации сферы услуг, для которых функции обеспечения ЭИБ являются сопутствующими
48. Приоритеты в фирменной системе ЭИБ
49. СБ на предприятии. Классификация функций СБ на предприятии
50. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
51. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
52. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
53. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
54. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
55. Общая характеристика случайных угроз информационной безопасности в КС.
56. Общая характеристика преднамеренных угроз информационной безопасности в КС.
57. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
58. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.
59. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
60. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.

61. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, владельца и пользователя информационных ресурсов.
62. Отечественное законодательство в области информации и защиты информации.
63. Ответственность за правонарушения при работе с компьютерными системами.
64. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
65. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.
66. Средства и методы разграничения доступа к ресурсам КС.
67. Защита программных средств КС от несанкционированного копирования и исследования.
68. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.
69. Контроль целостности программ и данных в процессе эксплуатации КС.
70. Общие понятия, история развития и классификация криптографических средств.
71. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
72. Системы шифрования с открытым ключом. Односторонние функции. Электронная цифровая подпись. Алгоритм шифрования RSA.
73. Отечественные и зарубежные стандарты шифрования.
74. Общая характеристика и классификация компьютерных вирусов.
75. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
76. Средства, используемые для обнаружения компьютерных вирусов.
77. Профилактика заражения компьютерными вирусами.
78. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.
79. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.
80. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
81. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.
82. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.
83. Основные технологические этапы разработки КСЗИ.
84. Средства моделирования, применяемые для оптимизации КСЗИ.
85. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.
86. Задачи, решаемые подсистемой аудита в составе защищенных КС.

Список вопросов для экзамена
по дисциплине

1. Интеллектуальный капитал (интеллектуальные активы) компании
2. Данные, информация знания (в контексте управления знаниями)
3. Классификации знаний (явные/неявные, формализованные/неформализованные)
4. Модель трансформации знаний в организации («спираль знаний» Нонака, Такеучи)
5. Знание как конкурентный ресурс
6. Проблема сохранения и развития интеллектуального капитала организации
7. Пятифазная модель создания организационного знания (Нонака, Такеучи)
8. Тактические процессы: приобретение/поиск знаний, сохранение знаний, использование знаний, распространение знаний
9. Инструменты управления знаниями: организационный, HR и информационно-технологический подходы
10. Стимулирование разработки и внедрение инноваций в организации. Формализация знаний
11. Обучение персонала и обучающаяся организация
12. Приоритеты управления как виды оружия
13. Структура полного вектора управления
14. Методы и технологии идентификации используемые при оценке рисков
15. Организация разработки решений руководителем на основе системного анализа складывающейся обстановки
16. Факторы, определяющие эффективность решений
17. Концепции, принципы и парадигмы разработки решений
18. Модель проблемной ситуации
19. Процесс разработки решений в сложных ситуациях
20. Содержание процесса обоснования решений
21. Критерии принятия решений и их шкалы .
22. Содержание процесса принятия решений
23. Общая характеристика проблемы коммуникации в процессе разработки решений в сложных ситуациях
24. Содержание процесса контроля
25. Постановки и основные методы решения базовых задач обоснования решений
26. Задача формирования исходного множества альтернатив и их оценки
27. Постановка задачи обоснования решений в условиях определенности

28. Составляющие и источники рисков в управлении
29. Технологии принятия решений при стохастическом риске
30. Технологии принятия решений при поведенческом риске
31. Технология ведения деловых бесед
32. Понятие ЭИБ. Объект и субъект управления в сфере ЭИБ
33. Принципы и факторы, определяющие эффективность управления в сфере ЭИБ
34. Важнейшие признаки предпринимательства с позиций его безопасности
35. Виды бизнеса в России. Особенности управления ЭИБ в России
36. Система управления ЭИБ предприятия
37. Понятие и субъекты криминальной конкуренции
38. Основные функции и группы объектов безопасности в предпринимательской деятельности
39. Структура информации, необходимой для анализа условий предпринимательской деятельности с точки зрения ее безопасности
40. Понятие коммерческой тайны и структура информации, составляющей коммерческую тайну
41. Структура информации с позиций обеспечения безопасности предприятия
42. Структура информации о фактах криминальной конкуренции
43. Информационная база и процедуры, осуществляемые в целях внутрифирменного управления в сфере безопасности
44. Подходы к организации защиты коммерческой тайны на предприятии
45. Информационная база государственного регулирования в сфере безопасности предпринимательства
46. Обеспечение ЭИБ предприятия как функция инфраструктуры рыночной экономики
47. Организации сферы услуг, для которых функции обеспечения ЭИБ являются сопутствующими
48. Приоритеты в фирменной системе ЭИБ
49. СБ на предприятии. Классификация функций СБ на предприятии
50. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
51. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
52. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
53. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
54. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
55. Общая характеристика случайных угроз информационной безопасности в КС.
56. Общая характеристика преднамеренных угроз информационной безопасности в КС.

57. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
58. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.
59. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
60. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
61. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, владельца и пользователя информационных ресурсов.
62. Отечественное законодательство в области информации и защиты информации.
63. Ответственность за правонарушения при работе с компьютерными системами.
64. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
65. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.
66. Средства и методы разграничения доступа к ресурсам КС.
67. Защита программных средств КС от несанкционированного копирования и исследования.
68. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.
69. Контроль целостности программ и данных в процессе эксплуатации КС.
70. Общие понятия, история развития и классификация криптографических средств.
71. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
72. Отечественные и зарубежные стандарты шифрования.
73. Общая характеристика и классификация компьютерных вирусов.
74. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
75. Средства, используемые для обнаружения компьютерных вирусов.
76. Профилактика заражения компьютерными вирусами.
77. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.
78. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.

Пример билета

1. Отечественное законодательство в области информации и защиты информации.
2. Контроль целостности программ и данных в процессе эксплуатации КС.

Приложение

Структура и содержание дисциплины «Информационная безопасность»
по направлению подготовки 09.03.03 "Прикладная информатика"
Образовательная программа (профиль)
«Прикладная информатика»
Форма обучения
Заочная
Год приема - 2013
(бакалавр)

n/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														
1.	Тема 1. Управление знаниями и рисками предприятия.	4	1-2	2		2	7					+			
2.	Тема 1. Управление знаниями и рисками предприятия.	4	3-4	2		2	7								
3.	Тема 2. Экономическая безопасность.	4	5-6	2		2	7					+			
4.	Тема 2. Экономическая безопасность.	4	7-8	2		2	7								
5.	Тема 3. Защита информации как объективная закономерность эволюции постиндустриального общества.	4	9-10	2		2	7					+			
6.	Тема 3. Защита информации как объективная закономерность эволюции постиндустриального общества.	4	11-12	2		2	7								
7.	Тема 4. Информационная безопасность личности, общества и государства: социально-правовые аспекты.	4	13-14	2		2	6					+			
8.	Тема 4. Информационная безопасность личности, общества и государства: социально-правовые аспекты	4	15-16	2		2	6								
9.	Тема 5. Системный анализ угроз безопасности в компьютерных системах.	4	17-18	2		2	6					+			
10.	Тема 5. Системный анализ угроз безопасности в компьютерных системах.	4	19-20	2		2	6								

11.	Гема 6. Общая характеристика средств и методов защиты информации.	5	1-2	4		4	6					+			
12.	Гема 6. Общая характеристика средств и методов защиты информации.	5	3-4	5		5	6								
13.	Тема 7. Организационно-правовое обеспечение защиты информации.	5	5-6	5		5	6					+			
14.	Тема 7. Организационно-правовое обеспечение защиты информации.	5	7-8	5		5	6								
15.	Тема 8. Защита информации в компьютерных системах от несанкционированного вмешательства.	5	9-10	5		5	6					+			
16.	Тема 9. Криптографические методы защиты.	5	11-12	5		5	6								
17.	Тема 10. Компьютерные вирусы и антивирусные программные средства.	5	13-17	5		5	6					+			
	Форма аттестации	5	18-21											Э	
	Всего часов по дисциплине в пятом семестре		108	54		54	108							Э	
	Всего часов по дисциплине		108	54		54	108							Э	