Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»
Ивановский филиал

Утверждено
на заседании совета Ивановского филиала
протокол № 1 от «11» 04 20 16
Председатель совета Арефьева Н.Т.

Кафедра Коммерции, технологии и прикладной информатики

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.02.01 *Основы информационной безопасности*

Направление подготовки	**09 . 03 . 03 Прикладная информатика**
Направленность (профиль) программы	***Прикладная информатика в экономике***
Уровень высшего образования	***Бакалавриат***
Программа подготовки	***Академинчский бакалавриат***

Иваново – 2016 г.

1. Цели освоения дисциплины

Целью дисциплины является сформировать у студентов четкое представление и понимание теоретических и прикладных знаний о современных методах обеспечения информационной безопасности в информационных инфраструктурах государственных и частнопредпринимательских предприятий и организаций.

В результате изучения дисциплины студенты должны овладеть методологическим инструментарием обеспечения информационной безопасности, методами и средствами правового, организационно-административного, физического, технического, технологического, программного, программно-аппаратного и криптографического обеспечения информационной безопасности. Изучить международные стандарты информационного обмена, определить понятия информационных угроз и особенности обеспечения информационной безопасности в условиях функционирования в России глобальных, региональных, корпоративных и локальных компьютерных сетей. Важным условием в изучении дисциплины «Основы информационной безопасности» является изучение методов формирования электронных документов и электронного документооборота, идентификации и аутентификации пользователей и документов в информационных инфраструктурах на основе электронной цифровой подписи, а также методов управления контролем доступа, необходимых для построения защищенных информационных систем локального, регионального, корпоративного и глобального назначений. Предметом дисциплины является изложение основ правовой, организационно-административной, физической, технической, программной и программно-аппаратной защиты информации в современных информационных технологиях, средств и методов управления контролем доступа в компьютерных системах, методов идентификации и верификации пользователей и документов в открытых и специализированных современных информационных систем. Место дисциплины в области науки, техники и практики охватывает совокупность проблем, связанных с технологией и защитой информации в информационной инфраструктуре предприятий и организаций.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Основы информационной безопасности» изучается на третьем курсе.

Дисциплина «Основы информационной безопасности» базируется на знаниях полученных студентами в процессе освоения программы по предметам: «Информатика и программирование» ОК-13,

«Правовые основы прикладной информатики»ОК-13(теоретические основы в области правовых основ информатики, информационных прав и свобод человека и гражданина, защиты интеллектуальных прав в информационной сфере; основы законодательства Российской Федерации в области информатики).

«Сетевые решения в современных телекоммуникациях» ПК-8, (Владеть: – проектированием компьютерной сети предприятия.)
«Системное программирование» ПК-18.(Знать: принципы программного управления учётными записями пользователя; Владеть: – созданием программ, позволяющих автоматизировать системное администрирование.

Для входного контроля осуществляется поведение тестового контроля, тесты размещены в фонде оценочных средств по данной дисциплине.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

1. Способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-13)
2. Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе, участвовать в реинжиниринге прикладных и информационных процессов (ПК-8)
3. Способен анализировать и выбирать методы и средства обеспечения информационной безопасности (ПК-18);

В результате изучения дисциплины студент должен: иметь целостное представление об актуальных проблемах информационной безопасности компьютерных систем, методах и средствах криптографической защиты информации, методах управления контролем доступа в компьютерных системах, методах аутентификации и идентификации пользователей и документов в информационных технологиях.

Знать:

- законодательную и нормативно-правовую базу обеспечения информационной безопасности;
- технологию построения защищенных компьютерных систем.
- средства и методы управления контролем доступа в компьютерных технологиях;
- средства и методы аутентификации и идентификации пользователей и документов в компьютерных технологиях
- методы и методики оценки рисков информационной безопасности.
- **уметь:**
- применять полученные знания в решении прикладных задач защиты информации в компьютерных технологиях .
- разрабатывать программу информационной безопасности предприятия.

приобрести навыки:

- пользования библиотеками прикладных программ компьютерных систем для решения задач по защите информации в информационных технологиях
- применения стандартов Государственной Технической Комиссии при Президенте Российской Федерации (Федеральная служба по техническому и экспортному контролю Российской Федерации) по проблемам информационной безопасности в своей профессиональной деятельности;

Владеть, иметь опыт:

- определения требований и состава средств, методов и мероприятий по организации комплекса средств защиты информации в компьютерных технологиях;
- использование методов организации, планирования и контроля функционирования комплекса средств защиты информации;
- практического применения технических, программных и программно-аппаратных средств и методов защиты информации в компьютерных технологиях;
- организации системы управления контролем доступа в сетевых компьютерных технологиях и оценку их информационной безопасности

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 144 часа, 4 зачетных единиц. Вид аттестации – экзамен .

Таблица

Индент. №	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы				Формы текущ. контр.
				лекции	семинар, практич.	лаборат.	самост. работа	
1.	Введение. Понятие информационной безопасности	5	5	2			4	тест
2.	Объектно-ориентированный подход информационной безопасности	5		2			4	тест
3	Основные определения и критерии классификации угроз	5		2	2		2	тест
4	Законодательный уровень информационной безопасности	5		2	2		4	тест
5	Административный уровень информационной безопасности	5		2	2		6	тест
6	Управление рисками	5		2			6	тест
7	Процедурный уровень информационной безопасности	5		2	2		4	тест
8	Основные программно-технические меры	5			6	10	14	тест
9	Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности	5				4	12	тест
10	Оценочные стандарты и технические спецификации.	5			2		8	тест
11	Активный аудит	5		2	2		6	тест
12	Экранирование, анализ защищенности	5				4	6	тест
13	Туннелирование и управление	5				2	6	тест
			итого	16	18	20	54	

4.1 Практические и семинарские занятия, их наименование, содержание

Таблица2

№ п/п	№ раздела дисциплины	Наименование лабораторных работ
1	Законодательный уровень информационной безопасности	1.Нормативные документы в области информационной безопасности. 2.Изучение системы отечественных стандартов информационной безопасности.
2	Административный уровень информационной безопасности	3.Процедурный уровень информационной безопасности.
3	Основные программно-технические меры	4.Защита информации в браузерах,MS Office. 5.Защита информации с помощью пароля. 6.Архивированию и восстановлению системы с использованием программы Handy Backup.
4	Управление рисками	7.Анализ рисков информационной безопасности
5	Активный аудит	8.Аудит информационной безопасности
7	Экранирование, анализ защищенности	9.Настройка параметров безопасности домена. 10.Построение концепции информационной безопасности предприятия.

Содержание дисциплины

Разделы и темы .

Раздел 1. Введение. Понятие информационной безопасности

Информационная безопасность рассматривается в разных контекстах(в доктрине информационной безопасности Российской Федерации , в Законе РФ "Об участии в международном информационном обмене".). Рассматриваются подходы к проблемам информационной безопасности. Спектр интересов субъектов, связанных с использованием информационных систем. Информационная безопасность на национальном, отраслевом, корпоративном или персональном уровне.

Раздел 2. О необходимости объектно-ориентированного подхода к информационной безопасности.

Вводится понятие класса, объекта, инкапсуляции, наследовании и полиморфизма. Компонентные объектные среды и их достоинства. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

Раздел 3.Основные определения и критерии классификации угроз.

Даются понятия: атаки , злоумышленника, источника угроз. Классификация угроз. Угрозы доступности и их классификация. Основные угрозы целостности и их классификация. Угрозы конфиденциальности. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.

Раздел 4 Законодательный уровень информационной безопасности

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Значение информационной безопасности и ее место в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Международные стандарты информационного обмена, правовые основы защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера. Федеральные Законы Российской Федерации по обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности,

Руководящие документы и инструкции Федеральной службы по техническому и экспортному контролю (ФСТЭК) (бывшая Государственная техническая комиссия при Президенте Российской Федерации (ГТК)), Приказы и распоряжения ФСБ РФ, Ведомственные приказы и распоряжения.

Раздел 5. Административный уровень информационной безопасности

Сформулирована главная цель мер административного уровня. Дается понятие термина "политика безопасности". Элементы политики безопасности. Политика верхнего уровня, среднего уровня. Программа безопасности организации. Управление рисками. Основные понятия. Мероприятия по управлению рисками. Подготовительные этапы управления рисками. Основные этапы управления рисками.

Раздел 6. Процедурный уровень информационной безопасности.

Основные классы мер процедурного уровня. Классы мер на процедурном уровне. Управление персоналом. Физическая защита. Методы и средства защиты информации от несанкционированного доступа. Аутенфикация пользователей по биометрическим характеристикам, клавиатурному подчерку и росписи мыши, на основе паролей и модели «рукопожатия». Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Раздел 7 Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности Архитектурная безопасность -три принципа, содержащиеся в приведенном утверждении. Международные стандарты информационного обмена. Модели безопасности и их применение. Безопасность в сетях Internet и Intranet. Технология безопасности. Модели анализа безопасности программного обеспечения**.**

Раздел 8. Оценочные стандарты и технические спецификации

"Оранжевая книга" как оценочный стандарт. Шесть классов безопасности - C1, C2, B1, B2, B3, A1 и их основные характеристики. Информационная безопасность распределенных систем. Рекомендации X.800.Сетевые сервисы безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".Функциональные требования. Требования доверия безопасности. Руководящие документы Гостехкомиссии России.

Раздел 9 Активный аудит.

Основные понятия. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты. Экранирование. Основные понятия. Анализ защищенности. Классификация межсетевых экранов. Анализ защищенности. Доступность. Основы мер обеспечения высокой доступности.

Раздел 10. Туннелирование и управление

Туннелирование. Управление. Основные понятия. Возможности типичных систем. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности

5. Образовательные технологии

В качестве образовательных технологий используются предметно-ориентированные и личностно-ориентированные:

- для каждого раздела дисциплины определены целевые установки, критерии их достижения;
- сформулированы контрольные вопросы, подготовлены тесты обучающего и контролирующего типов;
- сделан акцент на развитие инициативы и самостоятельности студентов при изучении информационных технологий;
- подготовка доклада с презентацией на теоретические темы, связанные с информационными технологиями;

Для организации самостоятельной работы студентов на сервере университета размещены электронные материалы папка МАТЕРИАЛЫ(Бреславская) (Информационная безопасность) на рабочем столе рабочих станций.

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

Оценка результатов освоения учебной дисциплины включает в себя: текущий контроль знаний и промежуточную аттестацию студентов, конкретные сроки и процедура проведения которых доводятся до сведения студентов в течение первых двух месяцев от начала обучения.

Текущий контроль знаний проводится в форме проведения лабораторных и практических занятий, устного итестовых заданий, выполнению контрольных работ.

Промежуточная аттестация по итогам освоения программы учебной дисциплины проводится в форме экзамена.

Условием допуска студента к экзамену является выполнение всех практических заданий лабораторных работ, и сдача отчётов по самостоятельной работе. Для оценки знаний студентов на экзамене используются тесты. Каждому студенту за отведённое время предлагается выполнить 25 тестовых заданий.

Условием положительной аттестации («отлично») является получение от 90-100 баллов правильно выполненных тестовых заданий

Студент, получает оценку «хорошо», является получение от 80-90- баллов правильно выполненных тестовых заданий

Студент, получает оценку «удовлетворительно», за работу, выполненную в не полном объеме не менее 60 правильно выполненных заданий .

Студент, получает оценку «неудовлетворительно» является получение от 59 и ниже баллов правильно выполненных тестовых заданий

В течение семестра студент обязан самостоятельно выполнять практическую работу, отчитываться на практических занятиях поэтапно о выполняемой работе.

Дисциплина разделена на ряд логически завершенных блоков (модулей), по которым проводится промежуточный контроль Для обеспечения текущего контроля прохождения дисциплины применяется тестирующая система «Аист», которая основана на бальной оценке выполненного теста. Тестовые задания представлены в ФОС по данной дисциплине.

По окончании пятого семестра проводится экзамен. Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями, установленными в вузе. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в освоения дисциплины.

Оценочные средства. Примерный промежуточный тест

1.Что такое защита информации:

1.защита от несанкционированного доступа к информации
2 выпуск бронированных коробочек для дискет
3 комплекс мероприятий, направленных на обеспечение информационной безопасности

2.Что из перечисленного не относится к числу основных аспектов информационной безопасности:

1 доступность
2 целостность
3 защита от копирования
4 конфиденциальность

3.Компьютерная преступность в мире:

1.остается на одном уровне
2.снижается
3.растет

4.Что из перечисленного относится к числу основных аспектов информационной безопасности:

1. подлинность - аутентичность субъектов и объектов

2. целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения

3.стерильность - отсутствие недекларированных возможностей

5.Сложность обеспечения информационной безопасности является следствием:

1.невнимания широкой общественности к данной проблематике

2.все большей зависимости общества от информационных систем

3.быстрого прогресса информационных технологий, ведущего к постоянному

изменению информационных систем и требований к ним

6.Структурный подход опирается на:

1. семантическую декомпозицию

2.алгоритмическую декомпозицию

3.декомпозицию структур данных

7.Объектно-ориентированный подход использует:

1.семантическую декомпозицию
2. объектную декомпозицию
3. алгоритмическую декомпозицию

8.Метод объекта реализует волю:

1.вызвавшего его пользователя
2.владельца информационной системы
3.разработчика объекта

9.Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на просмотрщик файлов определенного формата могут быть наложены следующие ограничения:

1.запрет на чтение файлов, кроме просматриваемых и конфигурационных

2.запрет на изменение файлов, кроме просматриваемых и конфигурационных

3.запрет на изменение каких-либо файлов

10. Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что:

1.существует обширная литература по объектно-ориентированному подходу

2.объектно-ориентированный подход применим как на стадии проектирования информационных систем, так и при их реализации

3.объектно-ориентированный подход позволяет успешно справляться с модификацией сложных информационных систем

Примерный итоговый тест(полный текст представлен в ФОС)

1.Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю называется

1.дипломом
2.Лицензией
3.Патентом

2.Вредоносный код, который выглядит как функционально полезная программа, называется

1.апплетом
2.троянской
3.математической

3.Целиком посвящена вопросам защиты информации. В статье Закона фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации.

1.Статья 27
2.Статья 15
3.Статья 16
закона "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ (принят Государственной
Думой 8 июля 2006 года).

4.Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и

1.аппаратные средства
2.программы
3.сети

5.Агрессивное потребление ресурсов является угрозой:

1.доступности
2.конфиденциальности
3.целостности

6.Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

1.просчеты при администрировании информационных систем
2.необходимость постоянной модификации информационных систем
3.сложность современных информационных систем

7.Самыми опасными источниками внутренних угроз являются:

1.некомпетентные руководители
2.обиженные сотрудники
3.любопытные администраторы

8.Melissa подвергает атаке на доступность:

1.системы электронной коммерции
2.геоинформационные системы
3.системы электронной почты

9.Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории:
обеспечение доступности, целостности, конфиденциальности информационных ресурсов и._____

1. информационных услуг
2. поддерживающей инфраструктуры
3. сведения о технических каналах утечки информации

10.Под определение средств защиты информации, данное в Законе "О государственной тайне"", подпадают:

1.средства выявления злоумышленной активности
2.средства обеспечения отказоустойчивости
3.средства контроля эффективности защиты информации

11. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

1.выработка и проведение в жизнь единой политики безопасности
2.унификация аппаратно-программных платформ
3.минимизация числа используемых приложений

12. Назначение принципа минимизации привилегий :

1. уменьшить ущерб от случайных или умышленных некорректных действий;
2. идентификация ресурсов, необходимых для выполнения критически
важных функций;
3. подготовиться к авариям.

13. Меры физического управления доступом позволяют контролировать и при необходимости ограничивать:

1. конфигурационное управление персонала;
2. вход и выход сотрудников и посетителей;
3. выявление критически важных функций организации
и установление приоритетов.

14. На процедурном уровне можно выделить следующие классы мер:

1.управление персоналом;
2.физическая защита;
3.поддержание работоспособности;
4.реагирование на нарушения режима безопасности;
5 применение административных мер к персоналу
6.планирование восстановительных работ.

15. Процесс планирования восстановительных работ можно разделить на следующие этапы:

1.выявление критически важных функций организации,
установление приоритетов;
2.идентификация ресурсов, необходимых для
выполнения критически важных функций;
3.определение перечня возможных аварий;
4.разработка стратегии восстановительных работ;
5.сертификация важных функций
6.подготовка к реализации выбранной стратегии;
7.проверка стратегии.

Что не относится к этому процессу?

16. Уровень безопасности B, согласно "Оранжевой книге", характеризуется:
    1. произвольным управлением доступом
    2. принудительным управлением доступом
    3. верифицируемой безопасностью

Вопросы к экзамену

1. Понятие информационной безопасности.
2. Доктрина информационной безопасности Российской Федерации, важные составляющих национальных интересов РФ в информационной сфере.
3. О необходимости объектно-ориентированного подхода к информационной безопасности.
4. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
5. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.
6. Основные определения и критерии классификации угроз.
7. Наиболее распространенные угрозы доступности.
8. Некоторые примеры угроз доступности.
9. Вредоносное программное обеспечение.
10. Основные угрозы целостности.
11. Основные угрозы конфиденциальности.
12. Что такое законодательный уровень информационной безопасности и почему он важен?
13. Обзор российского законодательства в области информационной безопасности.
14. Закон "Об информации, информационных технологиях и о защите информации"). В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области
15. Законом "О лицензировании отдельных видов деятельности".
16. Закон "Об электронной цифровой подписи" и правовые условия использования электронной цифровой подписи в электронных документах.
17. Федеральный закон "О Персональных данных" и обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, основные понятия, используемые в Федеральном законе.
18. Обзор зарубежного законодательства в области информационной безопасности
19. О текущем состоянии российского законодательства в области информационной безопасности.
20. Административный уровень информационной безопасности. Основные понятия
21. Политика безопасности.

22. Программа безопасности.
23. Управление рисками.
24. Подготовительные этапы управления рисками.
25. Основные этапы управления рисками.
26. Процедурный уровень информационной безопасности.
27. Основные классы мер процедурного уровня.
28. Управление персоналом.
29. Поддержание работоспособности.
30. Реагирование на нарушения режима безопасности.
31. Планирование восстановительных работ.
32. Основные понятия программно-технического уровня информационной безопасности.
33. Архитектурная безопасность.
34. Основные составляющие информационной безопасности.
35. Законодательный, административный и процедурный уровни.
36. Программно-технические меры.
37. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт.
38. Информационная безопасность распределенных систем. Рекомендации X.800.
39. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"
40. Гармонизированные критерии Европейских стран.
41. Интерпретация "Оранжевой книги" для сетевых конфигураций.
42. Руководящие документы Гостехкомиссии России.
43. Активный аудит.
44. Шифрование компьютерной криптографии и ее месте в общей архитектуре информационных систем.
45. Контроль целостности и криптографические методы позволяющие надежно контролировать целостность.
46. Цифровые сертификаты (понятия цифрового сертификата и удостоверяющего центра).
47. Экранирование. Экран как средство разграничения доступа. Экран как последовательность фильтров.
48. Экранирование, анализ защищенности.
49. Классификация межсетевых экранов. Анализ защищенности.
50. Доступность. Основные понятия. Основы мер обеспечения высокой доступности
51. Туннелирование и управление.
52. Туннелирование – как элемент в списке сервисов безопасности.

а) Основная литература:

1.Доктрина информационной безопасности Российской Федерации.
2. Федеральный закон Российской Федерации «Об информации, информационным технологиям и защите информации» №149-ФЗ от 27 июля 2006 года.
3. Федеральный закон от 4 июля 1996 г. «Об участие в международном информационном обмене».
4. Федеральный закон от 06 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
5. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. N1300. (В редакции Указа Президента Российской Федерации от 10 января 2000 г. N24.
6. Приказ ФСБ РФ №66 от 9 февраля 2005 года «Об утверждении Положения о разработке, производстве, реализации т эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
7. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» №351 от 17 марта 2002 года.
8.ФСТК России. Руководящие документы. М., ФСТК, 2006 г..

9.Кондаков В. В., Краснобородько А. А. Информационная безопасность систем физической защиты, учета и контроля ядерных материалов: учебное пособие. Изд-во: МИФИ, 2008. http://biblioclub.ru/index.php?page=book&id=231133&sr=1
10 Попов В. Б.Основы информационных и телекоммуникационных технологий: учебное пособие, Ч. 2. Основы информационной безопасности Изд-во: Финансы и статистика, 2005. http://biblioclub.ru/index.php?page=book&id=221465&sr=1
11. Оглтри Т. В.Firewalls. Практическое применение межсетевых экранов Издатель: ДМК Пресс, 2008. http://biblioclub.ru/index.php?page=book&id=132131&sr=1
12.Астахов А. М.Искусство управления информационными рисками Издатель: ДМК Пресс, 2010.http://biblioclub.ru/index.php?page=book&id=86481&sr=1
13.Петренко С. А., Курбатов В. А. Политики безопасности компании при работе в Интернет Издатель: ДМК Пресс, 2011. http://biblioclub.ru/index.php?page=book&id=85101&sr=1
14. Креопалов В. В.Технические средства и методы защиты информации: учебно-практическое пособие Издатель: Евразийский открытый институт, 2011.http://biblioclub.ru/index.php?page=book&id=90753&sr=1

Дополнительная литература:

1. Поляков А. М. Безопасность Oracle глазами аудитора. Нападение и защита Издатель: ДМК Пресс, 2010. http://biblioclub.ru/index.php?page=book&id=86474&sr=1
2. Агапов А. В., Алексеева Т. В., Васильев А. В.Обработка и обеспечение безопасности электронных данных: учебное пособие Издатель: Московский финансово-промышленный университет «Синергия», 2012.http://biblioclub.ru/index.php?page=book&id=252894&sr=1
3. Семенов Ю. А Алгоритмы телекоммуникационных сетей, Ч. 3. Процедуры, диагностика, безопасность Издатель: Интернет-Университет Информационных Технологий, 2007 http://biblioclub.ru/index.php?page=book&id=233324&sr=1.
4. Ложников П. С., Михайлов Е. М.Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft. Издатель: Интернет-Университет Информационных Технологий, 2008http://biblioclub.ru/index.php?page=book&id=233194&sr=1
5. Шаньгин В. Ф Защита компьютерной информации. Эффективные методы и средства .Издатель: ДМК Пресс, 2010. http://biblioclub.ru/index.php?page=book&id=86475&sr=1

8. Материально-техническое обеспечение дисциплины.

На кафедре имеется три компьютерных класса на 45 рабочих места, оборудованный видиопроектором, интерактивной доской и другой организационной техникой, позволяющей успешно проводить практические и лабораторные занятия по данной дисциплине. Структура и состав компьютерных классов приведены в ООП на кафедре ИТЭ и ОП.

Автор к.т.н., доцент,
Ст.преподаватель кафедры ИТЭ ОП_____Бреславская И.Б.

Программа рассмотрена на заседании кафедры ИТЭ и ОП
от «27» 06__2014 г., протокол № _8_

Программа одобрена на заседании Ученого совета экономического факультета
от «_16__» _09_2014 г., протокол № _1_