

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФИЛИАЛ ФГБОУ ВО «ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА» В Г. НАХОДКЕ
КАФЕДРА МЕНЕДЖМЕНТА И ЭКОНОМИКИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Рабочая программа учебной дисциплины

по направлению подготовки

38.03.05 Бизнес-информатика

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.05 «Бизнес-информатика» и «Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» (утв. приказом Минобрнауки России от 5 апреля 2017 г. № 301)

Составители:

Боршевников А.Е., ассистент кафедры информационных технологий и систем,

Витязев Г.Г., ассистент кафедры менеджмента и экономики.

Рассмотрена и утверждена на заседании кафедры менеджмента и экономики от «28» апреля 2018 года, протокол № 9

Заведующий кафедрой (разработчика)


«28» апреля 2018г.


_____ *подпись*

Просалова В.С.
фамилия, инициалы

Заведующий кафедрой (выпускающей)

«28» апреля 2018г.


_____ *подпись*

Просалова В.С.
фамилия, инициалы

1 Цель и задачи освоения дисциплины

Целью освоения дисциплины "Информационная безопасность и защита информации" является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи освоения дисциплины: формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли; формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов; формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемыми результатами обучения по дисциплине, являются знания, умения, навыки и/или опыт деятельности, характеризующие этапы/уровни формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы в целом. Перечень компетенций, формируемых в результате изучения дисциплины, приведен в таблице 1.

Таблица 1 – Формируемые компетенции

Название ОПОП ВО (сокращенное название)	Компетенции	Название компетенции	Составляющие компетенции	
38.03.05 Бизнес-информатика (Б-БИ)	ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	Знания:	Знание действующего законодательства в области информационной безопасности
			Умения:	Умение использовать действующее законодательство в области информационной безопасности для организации бизнес-процессов
	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления	Знания:	Знание современных технологий и методик защиты информации

		информационной безопасностью ИТ-инфраструктуры предприятия	Умения:	Умение управлять информационной безопасностью организации
			Навыки:	Владение методами оценки рисков информационной безопасности; владение современными технологиями защиты информации

3 Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность и защита информации» входит в базовую общепрофессиональную часть ОПОП. Для изучения данной части необходимы базовые знания в области информационных технологий, юриспруденции и экономики.

4 Объем дисциплины

Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу по всем формам обучения, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП	Форма обучения	Цикл	Курс	Трудоемкость (З.Е.)	Объем контактной работы (час)						СРС	Форма аттестации
					Всего	Аудиторная			Внеаудиторная			
						лек	прак	лаб	ПА	КСР		
Б-БИ	ОЗФО	Б.1.В.15	4	4	24	10	-	5	9	-	120	Экзамен

5 Структура и содержание дисциплины

5.1 Структура дисциплины

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.

Таблица 3 – Структура дисциплины

№	Название темы	Вид занятия
1	Введение в информационную безопасность	Лекция

2	Правовое обеспечение информационной безопасности	Лекция
3	Организационное обеспечение информационной безопасности	Лекция
4	Технические средства и методы защиты информации	Лекция
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	Лекция
6	Криптографические методы защиты информации	Лекция
7	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Лабораторная работа
8	Использование криптографических средств защиты информации	Лабораторная работа
9	Реализация работы инфраструктуры открытых ключей	Лабораторная работа
10	Средства стеганографии для защиты информации	Лабораторная работа
11	Настройка безопасного сетевого соединения	Лабораторная работа
12	Антивирусные средства защиты информации	Лабораторная работа

5.2 Содержание дисциплины

Лекционные занятия:

Тема 1. Введение в информационную безопасность

Содержание темы:

Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.

Литература по теме:

Для подготовки можно использовать источник 1, указанный в разделе 9.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лекционное занятие. Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.

Тема 2. Правовое обеспечение информационной безопасности

Содержание темы:

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Литература по теме:

Для подготовки можно использовать источник 1, указанный в разделе 9.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лекционное занятие. Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.

Тема 3. Организационное обеспечение информационной безопасности

Содержание темы:

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Литература по теме:

Для подготовки можно использовать источник 1, указанный в разделе 9.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лекционное занятие. Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.

Тема 4. Технические средства и методы защиты информации

Содержание темы:

Инженерная защита объектов. Защита информации от утечки по техническим каналам.

Литература по теме:

Для подготовки можно использовать источники 1,4, указанные в разделе 9.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лекционное занятие. Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности

Содержание темы:

Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Литература по теме:

Для подготовки можно использовать источники 1,6,7,8,9, указанные в разделе 9.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лекционное занятие. Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.

Тема 6. Криптографические методы защиты информации

Содержание темы:

Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

Литература по теме:

Для подготовки можно использовать источник 1,2,3,5,10, указанный в разделе 9.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лекционное занятие. Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.

Лабораторные работы:

Тема 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности

Содержание темы:

Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лабораторное задание. Может быть сдано удаленно в электронной форме.

Тема 2. Использование криптографических средств защиты информации

Содержание темы:

Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лабораторное задание. Используется кейс технология. Может быть сдано удаленно в электронной форме.

Тема 3. Реализация работы инфраструктуры открытых ключей

Содержание темы:

Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лабораторное задание. Используется кейс технология. Может быть сдано удаленно в электронной форме.

Тема 4. Средства стеганографии для защиты информации

Содержание темы:

Использование средств стеганографии для защиты файлов.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лабораторное задание. Используется кейс технология. Может быть сдано удаленно в электронной форме.

Тема 5. Настройка безопасного сетевого соединения

Содержание темы:

Создание защищенного канала связи средствами виртуальной частной сети.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лабораторное задание. Используется кейс технология. Может быть сдано удаленно в электронной форме.

Тема 6. Антивирусные средства защиты информации

Содержание темы:

Изучение настроек средств антивирусной защиты информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии:

Лабораторное задание. Используется кейс технология. Может быть сдано удаленно в электронной форме.

6 Методические указания для обучающихся по освоению дисциплины

Текущая самостоятельная работа по курсу «Информационная безопасность и защита информации» направлена на углубление и закрепление знаний, на развитие практических умений и включает такие виды работ, как:

- работа с лекционным материалом;
- работа с рекомендованной литературой при подготовке к практическим занятиям;

- подготовка к зачёту.

При изучении дисциплины "Информационная безопасность и защита информации" рекомендуется рейтинговая технология обучения, которая позволяет реализовать непрерывную и комплексную систему оценивания учебных достижений студентов. Непрерывность означает, что текущие оценки не усредняются (как в традиционной технологии), а непрерывно складываются на протяжении семестра при изучении первого или второго модуля. Комплексность означает учет всех форм учебной и творческой работы студента в течение семестра.

Рейтинг направлен на повышение ритмичности и эффективности самостоятельной работы студентов. Он основывается на широком использовании тестов и заинтересованности каждого студента в получении более высокой оценки знаний по дисциплине.

Принципы рейтинга: непрерывный контроль (в идеале на каждом из аудиторных занятий) и получение более высокой оценки за работу, выполненную в срок. При проведении практических занятий необходимо предусматривать широкое использование активных и интерактивных форм (компьютерных симуляций, деловых и ролевых игр).

Рейтинг включает в себя два вида контроля: текущий, промежуточный и итоговый по дисциплине.

Текущий контроль (ТК) - основная часть рейтинговой системы, основанная на беглом опросе раз в неделю или в две недели. Формы: оценка за сдачу теоретических минизачетов, выполнение индивидуальных заданий и лабораторных работ. Важнейшей формой ТК, позволяющей опросить всех студентов на одном занятии являются теоретические модули, на которых студенты самостоятельно отвечают на вопросы для самостоятельной оценки.

Контрольные вопросы для самостоятельной оценки качества освоения учебной дисциплины

Тема 1. Введение в информационную безопасность

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности

1. Какие основные законы в области защиты информации в РФ?
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
3. Что такое концепция информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?
9. Что такое коммерческая тайна?
10. Что такое режим коммерческой тайны?
11. Что такое государственная тайна?

12. Опишите правовой режим государственной тайны.
13. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

Тема 3. Организационное обеспечение информационной безопасности

1. Какие основные международные стандарты в области информационной безопасности существуют?
2. Что такое "Единые критерии"?
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безопасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Тема 4. Технические средства и методы защиты информации

1. Что такое инженерная защита объектов?
2. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
3. Что такое технические каналы утечки информации?
4. Перечислите основные виды технических каналов утечки информации?
5. Перечислите методы защиты информации от утечки по визуальному каналу.
6. Перечислите методы защиты информации от утечки по воздушному каналу.
7. Перечислите методы защиты информации от утечки по вибрационному каналу.
8. Перечислите методы защиты информации от утечки по индукционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности

1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?

Тема 6. Криптографические методы защиты информации

1. Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?
4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?

9. Какие основные криптографические протоколы используются в сетях?

Основная цель ТК: своевременная оценка успеваемости студентов, побуждающая их работать равномерно, исключая малые загрузки или перегрузки в течение семестра.

Лекционные занятия желательно проводить в режиме презентаций с демонстрацией применения основного материала, излагаемого в теме. Это существенно улучшает динамику лекций.

Целесообразно обеспечивать студентов на 1-2 лекции вперед раздаточным материалом в электронном виде (сложные схемы, графики, аналитические исследования и опорный конспект). Основное время лекции лучше тратить на подробные аналитические комментарии и особенности применения рассматриваемого материала в профессиональной деятельности студента.

Лабораторные работы следует проводить в компьютерном классе либо в аудитории с мультимедийным оборудованием, используя оригинальную методику и профессиональные программы. Можно рекомендовать установку оригинальных программ на ПК студентов и выполнять ряд задач дома. В этом случае в классе основное внимание концентрируется на методике использования названных программ и анализе полученных результатов.

Промежуточный контроль (ПК) - это проверка знаний студентов по разделу программы. Формы: Опрос по теории согласно списку вопросов для самостоятельной оценки усвоения материала.

Цель ПК: побудить студентов отчитаться за усвоение раздела дисциплины накопительным образом, т.е. сначала за первый, затем за второй, затем за третий разделы и т.д. В конечном итоге многие студенты могут получить итоговые оценки по дисциплине "автоматом".

Итоговый контроль по дисциплине (ИКД) - это проверка уровня учебных достижений студентов по всей дисциплине за семестр. Формы контроля: экзамен. Цель итогового контроля: проверка базовых знаний дисциплины, полученных при изучении модуля, достаточных для последующего обучения.

Вопросы к экзамену для оценки качества освоения учебной дисциплины

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.

20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Распределение объемов различного вида контролей можно проиллюстрировать следующими цифрами на примере семестра: текущий контроль – 40 условных баллов; промежуточный контроль - 30 условных баллов; итоговый контроль - 30 условных баллов. Вся дисциплина оценивается в 100 условных баллов, если вся дисциплина оценивается цифрой, отличной от 100 баллов, то под условным баллом следует понимать процент от максимального числа баллов.

При этом действует следующая система перевода рейтинговых (условных) баллов в обычную шкалу качественных оценок: “Отлично” (5) - 91–100 условных баллов; “Хорошо” (4) - 75–90 условных баллов; “Удовлетворительно” (3) - 61–74 условных баллов; “Неудовлетворительно” (2) - < 61 условных баллов.

Приведенные цифры говорят о том, что на любой стадии обучение студента можно считать удовлетворительным, если он набирает не менее 61 условных баллов. Так, например, набрав в ходе ТК и ПК 61 баллов, студент гарантирует себе оценку “удовлетворительно”.

Рекомендации по работе с литературой.

Знания анализа информационной безопасности являются необходимыми, поскольку очевидна тесная связь профессиональной деятельности специалиста в области информационных технологий.

В процессе изучения дисциплины «Информационная безопасность и защита информации», для того, чтобы применять современные программные средства в области защиты информации необходимо получить основные понятия в этой области (тема 1). Данный вопрос рассмотрен в учебнике: Расторгуев С. П. Основы информационной безопасности: учеб. пособие. М.: Академия, 2009. – 187 с. В учебнике подробно представлена информация, как универсального характера, так и конкретные знания. Дается полное представление об информационной безопасности.

На современном этапе работа с информацией невозможна без использования средств и методов криптографической защиты информации. Получить сведения об информационных системах (тема 6) поможет учебник: Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р.А. Хади – М.: СОЛОН-Пресс, 2009. - 256 с. В нём рассматривается современное состояние дел в области практической криптографии, а также перспективы ее развития.

7 Перечень учебно-методического обеспечения для самостоятельной работы

При подготовке реферата (доклада) студенты всех форм обучения могут воспользоваться литературой, приведённой в учебной программе.

8 Фонд оценочных средств для проведения промежуточной аттестации

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине созданы фонды оценочных средств (Приложение 1).

9 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

- а) основная литература

1. Баранова Е.К. Моделирование системы защиты информации. Практикум: учеб. пособие для студентов вузов / Е. К. Баранова, А. В. Бабаш. - М.: РИОР: ИНФРА-М, 2015. - 120 с. - (Высшее образование: Бакалавриат)
2. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студентов вузов, обуч. по направл. подгот. "Информ. безопасность" / В. В. Платонов. - 2-е изд., стер. - М.: Академия, 2014. - 336 с.
3. Защита информации: учеб. пособие для студентов вузов (бакалавриат и магистратура) / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - М.: РИОР: ИНФРА-М, 2013. - 392 с. - (Высшее образование: Бакалавриат; Магистратура).
- б) дополнительная литература
4. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.: ил.
5. Расторгуев С. П. Основы информационной безопасности: учеб. пособие. М.: Академия, 2009. – 187 с.
6. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
7. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р.А. Хади – М.: СОЛОН-Пресс, 2009. - 256 с.
8. Мао В. Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом "Вильямс", 2005. –768 с.
9. Ховард М., Лебланк Д., Виега Д. 19 смертных грехов, угрожающих безопасности программ. – М.: Издательский Дом ДМК-пресс, 2006. – 288 с.: ил.
10. Смит Р.Э. Аутентификация: от паролей до открытых ключей.: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. –432 с.: ил.
11. Касперски К. Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 527 с.: ил.
12. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. – СПб.: БХВ-Петербург, 2005. – 432 с.: ил.
13. Алферов А.П., Зубов А.Ю, Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. – М.:Гелиос АРВ, 2002. – 380 с.: ил.
14. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие для студентов образоват. учреждений сред. проф. образования, обуч. по спец. "Информатика и вычислит. техника" / В. Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2016. - 416 с.

10 Перечень ресурсов информационно - телекоммуникационной сети «Интернет»

а) полнотекстовые базы данных:

1. Научная электронная библиотека eLIBRARY.RU: <http://www.eLIBRARY.RU>
2. Ресурс Цифровые учебные материалы <http://abc.vvsu.ru/>
3. ЭБС «Руконт»: <http://www.rucont.ru/>
4. ЭБС «Юрайт»: <http://www.biblio-online.ru/>

11 Материально-техническое обеспечение дисциплины

а) программное обеспечение: БД Консультант плюс, OpenSSL, TrueCrypt, ImageSpy, OpenVPN, MS Office, демоверсии VipNet client, SecretNet

б) техническое и лабораторное обеспечение – компьютерный класс, аудитория с презентационным оборудованием.