МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Обнинский институт атомной энергетики –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(ИАТЭ НИЯУ МИФИ)

Одобрено УМС ИАТЭ НИЯУ МИФИ,
Протокол №2-8/2021 От 30.08.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ
(ЗИ)
(Наименование дисциплины)

09.03.01 - Информатика и вычислительная техника
(Код (шифр), наименованиенаправления подготовки (специальности) ФГОС)

Профиль **«Вычислительные машины, комплексы, системы и сети»**
(Профиль направления)

Название программы бакалавриата

бакалавр
(Квалификация (степень) выпускника)

очная
Форма обучения (очная, очно-заочная (вечерняя), заочная)

г. Обнинск 2021 г.

Программа составлена в соответствии с требованиями образовательного стандарта высшего образования национального исследовательского ядерного университета «МИФИ» по направлению подготовки 09.03.01 – Информационные системы и технологии (уровень бакалавриата),

Автор(ы)

_____ Е.С. Волобуев, к.т.н., доцент

Рецензент(ы)

Программа рассмотрена на заседании отделения интеллектуальных кибернетических систем (О)
(протокол № 5/7 от «30» июля 2021 г.)

Руководитель образовательной программы
09.03.01 Информатика и вычислительная техника
_____ С.О. Старков
«30» июля 2021 г.

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

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенций	Результаты освоения ООП *Содержание компетенций*	Перечень планируемых результатов обучения по дисциплине
ОПК -3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**знать:** правовые основы защиты компьютерной информации, организационные, технические и программные методы и средства защиты информации в АСОИУ и ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; иметь представление о направлениях развития и перспективах защиты информации; **уметь:** применять методы защиты компьютерной информации при проектировании и эксплуатации АСОИУ и ИС в различных предметных областях;; **иметь навыки:** установки и настройки программного обеспечения, применяемого для защиты АСОИУ и ИС от несанкционированного доступа, как из сетей общего пользования, так и внутренних сетей предприятия..
ОПК-6	Способен разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием;	

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина реализуется в рамках базовой части.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Операционные системы, Системное программное обеспечение, ЭВМ и ПУ, Теория принятия решений, Сети ЭВМ и телекоммуникации, Базы данных, Сетевые технологии

Дисциплина изучается на 3 курсе в 6 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единиц (з.е.), 144 академических часов.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	80
Аудиторная работа (всего):	46

Лекции	32
семинары, практические занятия	
лабораторные работы	32
Внеаудиторная работа (всего):	
индивидуальная работа обучающихся с преподавателем:	38
курсовое проектирование	
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем*)*	3*8*
творческая работа (эссе)	
Самостоятельная работа обучающихся(всего)	80
Вид промежуточной аттестации обучающегося (зачет/экзамен(часы))	З*ачет*

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела /темы дисциплины	Общая трудоёмкость всего *(в часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость *(в часах)*				Формы текущего контроля успеваемости
			Аудиторные учебные занятия*			СРО	
			Лек	Сем/Пр	Лаб		
1.1.	**Введение в информационную безопасность**	2	2				
1.2.	**Законодательный уровень защиты информации.**	2	4				
1.3.	**Административный уровень информационной безопасности.**	2	4				
1.4.	**Криптографические методы защиты информации**	9	4		4	1	
1.5.	**Идентификация, аутентификация, управление доступом.**	8	6		10	2	
1.2.	**Безопасность вычислительных сетей**	10	6		6	2	
1.6	**Безопасность баз данных.**	8	4		6	2	

1.7	**Безопасность операционных систем**	11	2		4	2	

*Прим.: Лек – лекции, Сем/Пр – семинары, практические занятия, Лаб – лабораторные занятия, СРО – самостоятельная работа обучающихся

4.2. Содержание дисциплины, структурированное по разделам (темам)

4.2.1. Лекционный курс

№	Наименование раздела /темы дисциплины	Содержание
1.1.	**Введение в информационную безопасность**	Основные понятия и определения. Понятие информационной безопасности. Свойства информации как объекта защиты: доступность, целостность, конфиденциальность. Угроза информационной безопасности, виды угроз, классификация угроз. Мероприятия по обеспечению информационной безопасности.
1.2.	**Законодательный уровень защиты информации.**	Основные законодательные акты РФ по защите информации. Законы «О государственной тайне», «Об информатике, информатизации и защите информации», «О лицензировании отдельных видов деятельности», «О персональных данных». Стандарты информационной безопасности. Руководящие документы Гостехкомиссии РФ.
1.3.	**Административный уровень информационной безопасности.**	Политика безопасности. Оценка и управление рискам в области ИБ. Физическая защита. Управление персоналом. Поддержание работоспособности. Планирование восстановительных работ.
1.4.	**Криптографические методы защиты информации**	Введение в криптографию. Основные понятия криптографии. Виды систем шифрования и области применения криптографических алгоритмов. Свойства шифров, примеры простых систем шифрования. Симметричные алгоритмы шифрования, сети Фейстеля, алгоритмы Blowfish, IDEA, ГОСТ 28147-89. Система AES. Ассиметричное шифрование. Система Диффи-Хеллмана, шифр Эль Гамаля, шифр RSA. Криптографические хеш-функции. Цифровая подпись. Стандарты цифровой подписи. Открытое распределение колючей.
1.5.	**Идентификация, аутентификация, управление доступом.**	Основные понятия. Методы аутентификации. Многоразовые пароли, атаки на пароли, требования к паролям и парольным системам. Одноразовые пароли, алгоритмы формирования одноразовых паролей. Строгая аутентификация. Система аутентификации Cerberos. Аутентификация с использованием технических средств: магнитные карты, смарт-карты, USB-ключи. Биометрическая

		аутентификация. Задача управления доступом. Дискреционное управление доступом. Изолированная программная среда. Полномочное управление доступом. Управление доступом в Java среде..
1.2.	**Безопасность вычислительных сетей**	Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Интеграция локальных вычислительных сетей в глобальные. Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Протоколы аутентификации Kerberos, SSL, TLS. Технология PKI (Public Key Infrastructure) – интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих шифрование с открытым ключом, а также для управления ими. Многоуровневая защита корпоративных сетей. Виртуальные частные сети, варианты построения и продукты реализации. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Системы адаптивного анализа защищенности. Задачи и программно-аппаратные средства администратора безопасности сети..
1.6	**Безопасность баз данных.**	Особенности БД как объектов защиты информации. Обеспечение конфиденциальности. Избирательная защита. Пользователи, привилегии, роли. Мандатная защита. Метки безопасности. Избирательные механизмы защиты в СУБД Oracle. Обеспечение доступности. Резервное копирование и восстановление. Аудит. SQL инъекции
1.7	**Безопасность операционных систем**	Общая характеристика операционных систем. Назначение, возможности, модели безопасности операционных систем группы Windows, UNIX. Организация управления доступом и защиты ресурсов ОС. Основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

4.2.3. Лабораторные занятия

№	**Наименование раздела /темы дисциплины**	**Название лабораторной работы**

1.1.	**Введение в информационную безопасность**	**Обеспечение доступности информации средствами ОС Windows**
1.4.	**Криптографические методы защиты информации**	**Шифрующие файловые системы**
1.4.	**Криптографические методы защиты информации**	**Использование пакета PGP**
1.5.	**Идентификация, аутентификация, управление доступом.**	**Развертывание инфраструктуры Windows.**
1.5.	**Идентификация, аутентификация, управление доступом.**	**Управление доступом в ОС Windows**
1.7	**Безопасность операционных систем**	
1.2.	**Безопасность вычислительных сетей**	**Использование межсетевых экранов**

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студентами самостоятельно в рамках подготовки к лабораторным работам изучаются следующие вопросы:

- обеспечение конфиденциальности, целостности и доступности информации в соответствии с требованиями международных и отечественных стандартов информационной безопасности;

- задачи и принципы сопровождения системного программного обеспечения, управление безопасностью ОС;

- средства языка SQL для организации разграничения доступа, концепция и реализация механизма ролей, использование представлений, организация аудита системных событий и действий пользователя в системах баз данных;

- реализация симметричных и асимметричных криптоалгоритмов в программно-аппаратных разработках российских производителей;

Контроль освоения материала осуществляется в ходе приема лабораторных работ. Используемая литература, приведенная в разделе 8. По умолчанию предполагается литература из п.п. 8.2 (дополнительная). В отдельных необходимых случаях после номера источника в круглых скобках указывается п.п. 8.1 (основная литература).

Содержание самостоятельной работы	Литера-тура	Форма контроля
Обеспечение конфиденциальности, целостности и доступности информации в соответствии с требованиями международных и отечественных стандартов информационной безопасности	[1, 9]	Собеседование перед сдачей соответствующей лабораторной работы
Задачи и принципы сопровождения системного программного обеспечения, управление безопасностью ОС	[5, 6]	
Средства языка SQL для организации разграничения доступа, концепция и реализация механизма ролей, использование представлений, организация аудита системных событий и действий пользователя в системах баз данных	[10]	
Реализация симметричных и асимметричных криптоалгоритмов в программно-аппаратных разработках российских производителей	[8]	
Этапы проектирования комплексной системы информационной безопасности и требования к ним	[12], (4.1)	

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

6.1. Паспорт фонда оценочных средств по дисциплине

Вид контроля	Этап рейтинговой системы Оценочное средство	Балл	
		Минимум	Максимум
Текущий	**Контрольная точка № 1**		
	Контрольная № 1	5	15
	Контрольная точка № 2		
	Контрольная № 2	5	15
	Лабораторные работы	30	30
Промежуточный	**Экзамен**		
	Вопросы на экзамене	20	40
ИТОГО по дисциплине		60	100

6.2. Типовые контрольные задания или иные материалы

6.2.1. Экзамен или зачет

Оценка "отлично" выставляется за полный ответ на все поставленные вопросы. Ответы должны иллюстрироваться примерами в виде схем и фрагментов программ на ассемблере или языке высокого уровня.:

Оценка "хорошо" выставляется за неполный или частичный ответ на большинство поставленных вопросов.

Оценка "удовлетворительно" ставится за владение понятиями и определениями в объеме курса.

Типовые вопросы на экзамене

1. Дайте характеристику симметричных криптосистем. На каких принципах они основаны?
2. Перечислите основные уязвимости IP сетей.
3. Что дает злоумышленнику сборка мусора?
4. Каким образом можно использовать триггеры для обеспечения аудита БД?
5. Чем характеризуется избирательное управление доступом к информации.
6. Что такое «хеш-функция»? Зачем необходимо ее использовать? Приведите примеры хэш-функций.
7. Каким образом можно использовать представления для ограничения доступности информации в БД?
8. На каких принципах основано действие программ-архиваторов? Приведите пример.
9. Чем характеризуется полномочная (мандатная) политика безопасности.
10. Какие свойства сообщений используются в криптоанализе?
11. Для чего нужна и что представляет собой матрица доступа?
12. Поясните понятия «привилегия», «роль» в БД.
13. Что такое «объектная привилегия». Как они предоставляются?
14. Сформулируйте основные требования к паролям.
15. Что такое «системная привилегия». Для чего необходимы системные привилегии?
16. Для чего нужен и как организуется аудит?
17. Перечислите основные методы подбора паролей.
18. Перечислите и охарактеризуйте основные функции подсистемы защиты ОС.
19. Дайте характеристику асимметричных криптосистем. На каких принципах они основаны?
20. В чем различие фрагментарного и комплексного подхода к созданию защищенных систем?
21. Опишите свойства информации как объекта защиты.
22. Опишите алгоритм шифрования DES.
23. Перечислите основные причины возникновения угроз в сетях.
24. Сформулируйте основные функции ОС.
25. Основные свойства информации: целостность, конфиденциальность, доступность.
26. Перечислите типичные атаки на операционные системы.
27. Сформулируйте основные требования к шифрам. Какой шифр называется устойчивым?
28. Какими средствами реализуется целостность информации в базе данных?
29. Опишите основные группы методов защиты информации.
30. Что такое режим работы криптографического алгоритма? Перечислите основные режимы.
31. Перечислите угрозы, характерные для СУБД.
32. Понятие о политике безопасности. Как реализуется политика безопасности? Что предусматривает адекватная политика безопасности?
33. Что такое «потоковое шифрование»? Можно ли блочный шифр использовать как потоковый, если да, то в каком режиме?
34. Опишите следующие понятия: «идентификация», «авторизация», «аутентификация».
35. Что такое доступность базы данных?
36. Что такое цифровая подпись? Принципы построения цифровой подписи.

6.2.2. Вопросы к контрольной работе по защите ОС и БД

Вариант 1

1. Для чего применяются и как организованы идентификация, аутентификация и авторизация СД?

2. Что такое триггер? Каким образом можно использовать триггеры для обеспечения аудита БД?
3. Что такое «системная привилегия». Для чего необходимы системные привилегии?
4. Какие виды атак можно реализовать с помощью SQL-инъекций?

Вариант 2

1. Для чего нужна и что представляет собой матрица доступа?
2. Поясните понятие «привилегия» в БД. Предоставление и отзыв привилегий.
3. Для чего нужен и как организуется аудит?
4. Способы противодействия SQL- инъекциям.

Вариант 3

1. Сформулируйте основные требования к паролям.
2. Перечислите недостатки средств защиты информации в SQL.
3. Какими средствами реализуется целостность информации в базе данных?
4. Каким образом осуществляется идентификация пользователей в СУБД Interbase?

Вариант 4

1. Перечислите основные методы подбора паролей.
2. Перечислите особенности БД и СУБД, как объекта защиты информации.
3. Поясните понятие «роль» в БД. В чем состоит гибкость ролей? Создание ролей.
4. Что такое доступность базы данных? Каким образом можно обеспечить доступность БД?

Вариант 5

1. Для чего применяются и как организованы идентификация, аутентификация и авторизация СД?
2. Перечислите угрозы, характерные для СУБД.
3. Что такое «объектная привилегия». Как они предоставляются?
4. В чем, по-вашему, недостатки систем, обеспечивающих защиту БД на уровне приложений?

Вариант 6

1. Для чего нужна и что представляет собой матрица доступа?
2. Что такое представление? Как их использовать для ограничения доступности информации в БД?
3. Основные группы пользователей БД.
4. Что такое SQL-инъекции, каковы условия для их реализации?

Вариант 7

1. В чем, по-вашему может состоять атака «сборка мусора?» в ИС. Что дает злоумышленнику такая атака?
2. Что такое триггер? Каким образом можно использовать триггеры для обеспечения аудита БД?
3. Что такое «системная привилегия». Для чего необходимы системные привилегии?
4. Какие виды атак можно реализовать с помощью SQL-инъекций?

Вариант 8

1. Охарактеризуйте избирательное и полномочное разграничение доступа.
2. Для чего нужен и как организуется аудит?
3. Поясните понятие «привилегия» в БД. Предоставление и отзыв привилегий.

4. Способы противодействия SQL- инъекциям.

Вариант 9
1. Для чего применяются и как организованы идентификация, аутентификация и авторизация СД?
2. Перечислите недостатки средств защиты информации в SQL.
3. Какими средствами реализуется целостность информации в базе данных?
4. Каким образом осуществляется идентификация пользователей в СУБД Interbase?

Вариант 10
1. Для чего нужна и что представляет собой матрица доступа?
2. Перечислите особенности БД и СУБД, как объекта защиты информации.
3. Поясните понятие «роль» в БД. В чем состоит гибкость ролей? Создание ролей.
4. Что такое доступность базы данных? Каким образом можно обеспечить доступность БД?

Вариант 11
1. Сформулируйте основные требования к паролям.
2. Для чего и какими способами осуществляется разграничение доступа к объектам ОС?
3. Перечислите угрозы, характерные для СУБД.
4. Что такое «объектная привилегия». Как они предоставляются?

Вариант 12
1. Приведите пример классификации угроз безопасности информационным системам системам.
2. Для чего и какими способами осуществляется разграничение доступа к объектам ОС?
3. Что дает злоумышленнику сборка мусора?
4. В чем, по-вашему, недостатки систем, обеспечивающих защиту БД на уровне приложений?

Вариант 13
1. Какие факторы могут повлиять на доступность БД. Перечислите основные подходы к обеспечению доступности.
2. Каким образом реализуется хранение матрицы доступа в базах данных.
3. Приведите описание возможной схемы двухсторонней строгой аутентификации с участием третьей, доверенной стороны.
4. Какие возможны подходы к идентификации и аутентификации пользователей БД. В чем, по-вашему, состоят преимущества и недостатки этих подходов.

6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Экзамен (100 баллов)	Лабораторные работы	30
	Контрольная работа № 1	15
	Контрольная работа № 2	15
	Ответы на экзаменационный билет	40

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная учебная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. М: ИД «Форум» 2011 – 591 с.

2. Галатенко В.А.

3. Введение в информационную безопасность. Уч. пособие для высших учебных заведений. Под редакцией Горбатого В.С. М: «горячая линия Телеком» 2011 – 298с..

4. Информационная безопасность и защита информации. Учебное пособие для ВУЗов. Под редакцией Клейменов С.А. М: Изд центр «Академия» 2011 – 336с

б) дополнительная учебная литература

. Фисун А.П. Информационное право и информационная безопасность информационной сферы: учебное пособие. – Орел: ОГУ, 2004.– 303 с.

2. Малюк А.А. Информационная безопасность: концептуальные методологические основы защиты информации. – М.: Горячая линия – Телеком, 2004. – 280 с.

3. Волобуев С.В. Защита в операционных системах: учебное пособие по курсу «Методы и средства защиты компьютерной информации». – Обнинск: ИАТЭ, 2003. – 80 с.

4. Зихерт К., Ботт Э. Безопасность Windows. – СПб.: «Питер», 2003. – 688 с.

5. Волобуев С.В., Волобуев Е.С. Применение системы защиты информации ViPNet в электронном документообороте: учебно-методическое пособие. – Обнинск: ГОУ «ГЦИПК», 2004. — 181 с.

6. Волобуев С.В., Бологов Е.П. Информационная безопасность баз данных: учебное пособие по курсу «Методы и средства защиты компьютерной информации». – Обнинск: ИАТЭ, 2005. – 76 с.

7. Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М.: ЗАО «АЭИ «Прайм-ТАСС». – 2006.

8. Волобуев С.В., Волобуев Е.С. Программно-аппаратные средства защиты компьютерной информации: учебное пособие по курсу «Методы и средства защиты компьютерной информации». – Обнинск: ИАТЭ, 2006. – 80 с.

9. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2007. – 320 с.

10. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия – Телеком, 2004. – 248 с.

11. Волобуев С.В., Волобуев Е.С. Комплексное обеспечение информационной безопасности автоматизированных систем: учебное пособие. – Обнинск: ФГОУ «ГЦИПК», 2006. – 137 с.

12. Волобуев С.В. Безопасность социотехнических систем. – Обнинск, «Викинг», 2000. – 340 с.

13. Волобуев С.В. Введение в информационную безопасность: учебное пособие. – Обнинск: ИАТЭ, 2001. – 80 с.

14. Волобуев С.В. Информационная безопасность автоматизированных систем: учебное пособие – Обнинск: ИАТЭ, 2001. – 80 с.

15. Волобуев С.В. Философия безопасности социотехнических систем. – М.: Вузовская книга, 2002. – 360с.

16. Белкин П.Ю., Михальский О.О., Першаков А.С. и др. Защита программ и данных: учебное пособие. – М.: Радио и связь, 2000. – 168 с.

17. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах: учебное пособие. – М.: Радио и связь, 2000. – 168 с.

18. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: учебное пособие. – М.: Юнити, 2000. – 528 с.

19. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. Шаньгина В.Ф. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

20. Зегжда П.Д., Ивашко А.М. Основы безопасности информационных систем: учебное пособие. – М.: Горячая линия – Телеком, 2000. – 452с.

21. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных. Учебник для вузов. – СПб.: Корона-принт, 2002. – 672 с.

22. Меньшаков Ю.К. Защита информации от технических разведок. – М.: РГГУ, 2002. – 400 с.

23. Петраков А.В. Основы практической защиты информации. 2-е изд.: учебное пособие. – М.: Радио и связь, 2000. – 368 с.

24. Конституция Российской Федерации (принята 12 декабря 1993 года).

25. Гражданский кодекс РФ от 18.12.2006 № 230-ФЗ. Часть четвертая. Раздел VII Права на результаты интеллектуальной деятельности и средства индивидуализации.

26. Кодекс РФ от 30.12.2001 № 195-ФЗ «Об административных правонарушениях» (в части вопросов защиты информации) (с изм. и доп. от 30.06.2003 №86-ФЗ).

27. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000).

28. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» (с изм. и доп. от 6.10.1997 № 131-ФЗ; от 30.06.2003 № 86-ФЗ; от 11.11. 2003. № 153-ФЗ; от 29.06. № 58-ФЗ; от 22.08. 2004 № 122-ФЗ).

29. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

30. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

31. Федеральный закон РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

32. Федеральный закон РФ от 7.07.2003 № 126-ФЗ «О связи».

33. Федеральный закон РФ от 10.01.2002 г. № 1-ФЗ. «Об электронной цифровой подписи».

34. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

35. Постановление Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

36. Постановление Правительства РФ от 31.08.2006 № 532 «Об утверждении положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

37. Постановление Правительства РФ от 23.09.2002 № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

38. Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

39. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

40. ГОСТ Р.34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

41. ГОСТ Р.34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

42. ГОСТ Р.34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

43. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

44. ГОСТ Р ИСО/МЭК 17799. Информационные технологии. Методы безопасности. Руководство по управлению безопасностью информации.

45. ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования.

46. Гостехкомиссия России. Сборник руководящих документов по защите информации от несанкционированного доступа. – М., 1998.

47. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – М., 1999.

48. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. – М., 2002.

9. Методические указания для обучающихся по освоению дисциплины

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии и лабораторной работе. Уделить внимание следующим понятиям: данные, представление, атака, целостность, конфиденциальность, доступность
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Работа с конспектом лекций, просмотр рекомендуемой литературы.
Контрольная работа	Ознакомиться с основной и дополнительной литературой, включая справочные издания, зарубежные источники, основополагающие термины. Попрактиковаться в решении задач

Лабораторная работа	При выполнении лабораторных работ необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программные продукты: операционные системы Windows XP, Windows 2003, СУБД Oracle 9, система защиты информации от несанкционированного доступа «Secret Net», программный пакет PGP, почтовая программа The Bat!, межсетевой экран Outpost Firewall, сетевые сканеры: NMap, XSpider, GFI LANGuard Network Security Scanner, Microsoft Baseline Security Analyzer, сетевой монитор системы обнаружения атак Snort, антивирусный пакет Dr. Web – сканер для Windows.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Сетевой компьютерный класс. Для проведения лабораторных занятий используется система виртуальных машин Virtual PC компании Oracle. Использование виртуальных машин позволяет моделировать в рамках одного физического компьютера несколько лабораторных установок, оснащенных различными ОС и связанных в различные сетевые конфигурации**12. Иные сведения и (или) материалы**

12. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

Студенты самостоятельно изучают литературу и техническую документацию, для получения знаний, необходимых для выполнения лабораторных работ. Самостоятельно осваивают принципы использования применяемых программных средств. Самостоятельно выполняют тестирование и отладку программ. Самостоятельно осваивают ряд вопросов из раздела "Современные микропроцессоры"

12.3. Краткий терминологический словарь