МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

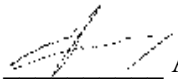
Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Год начала подготовки 2017

Разработал:  Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедры защиты информации

Рецензент:  Алексеев Дмитрий Станиславович, доцент кафедры защиты информации, к.т.н.

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи освоения дисциплины

Целями дисциплины «Защита информационных процессов в компьютерных системах» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»;

научить студентов основным принципам и методам, применяемым при защите компьютерных систем.

Задачи дисциплины:

- ознакомить с основными понятиями, используемыми при защите информации в компьютерных системах; - дать представление об основных проблемах защиты информации в компьютерных системах;
- обучить студентов методам защиты информации в компьютерных системах для построения защищенных информационных технологий;
- получить навыки практической работы по использованию средств защиты информационных процессов в компьютерных системах.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать:

принципы и методы организационной, технической, программно-аппаратной защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации; программные средства системного, прикладного и специального назначения.

уметь:

- определять информационные ресурсы, подлежащие защите (ОПК-7),
- выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
- администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

владеть:

− методами и средствами выявления угроз безопасности автоматизированным системам (ОПК-7),

− средствами администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

В результате изучения учебной дисциплины «Защита информационных процессов в компьютерных системах» у обучаемых должны сформироваться **профессиональные компетенции**:

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

3. Место дисциплины в структуре ОП ВО

Данная дисциплина относится к базовой части Блока Б1. В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ. Дисциплина изучается на третьем курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасно-

сти», «Техническая защита информации» по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Информатика».

Курс тесно взаимосвязан с другими дисциплинами. Он является полезным для изучения таких дисциплин как «Комплексные система зашиты информации на предприятии», «Защита информации в корпоративных ИС», «Организация и управление службой защиты информации на предприятии».

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	5
Общая трудоемкость в часах	180
Аудиторные занятия в часах, в том числе:	50
Лекции	16
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа в часах	130
Форма промежуточной аттестации	экзамен

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	16
Практические занятия	-
Лабораторные занятий	34
Консультации	
Зачет/зачеты	0,25
Экзамен/экзамены	
Курсовые работы	-
Курсовые проекты	–
Всего	50,25

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
1.	Основные угрозы информации в компьютерных системах. Классификация информационных процессов.	22	2	4	16
2.	Защита информационных процессов хранения информации. Классификация носителей информации.	22	2	4	16
3.	Анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера	22	2	4	16

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
4.	Специфика возникновения угроз в открытых сетях	24	2	6	16
5.	Особенности защиты информации на узлах компьютерной сети	22	2	4	16
6.	Методы и инструменты используемые злоумышленниками для атак и способы их парирования	24	2	4	16
7.	Системные вопросы защиты программ и данных	22	2	6	16
8.	Основные категории требований к программной и программно-аппаратной реализации средств защиты информации	18	2		16
Экзамен					
Всего:		**180**	**16**	**34**	**130**

5.2. Содержание:

1. Основные угрозы информации в компьютерных системах. Классификация информационных процессов.
   Характеристика информационных процессов хранения, передачи, обработки информации. Технические средства реализации информационных процессов. Физические особенности систем хранения информации. Задача тайной передачи. Особенности каналов передачи информации. Угрозы целостности, доступности, конфиденциальности. Случайные и преднамеренные угрозы. традиционный или универсальный шпионаж и диверсии; несанкционированный доступ к информации (НСД); утечка по техническим каналам; модификация структур КС; вредоносные программы.
2. Защита информационных процессов хранения и обработки информации. Классификация носителей информации.
   Носители информации. Виды памяти. Хранилища информации. Физические особенности систем хранения информации. Общая схема процесса обработки информации. Постановка задачи обработки. Исполнитель обработки. Алгоритм обработки. Типовые задачи обработки информации.
3. Защита информационного процесса передачи информации. Анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
   Источник и приемник информации. Информационные каналы. Роль органов чувств в процессе восприятия информации человеком. Структура технических систем связи. Что такое кодирование и декодирование. Понятие шума; приемы защиты от шума. Скорость передачи информации и пропускная способность канала.
4. Специфика возникновения угроз в открытых сетях
   Классификация атак по уровню сетевой модели OSI и их методы предотвращения.
   Классификация атак по типу и их методы предотвращения.
   Классификация атак по местоположению злоумышленника и атакуемого объекта и их методы предотвращения.
   Атаки на отказ в обслуживании. Цели. Структура атаки. Способы защиты.

5. Особенности защиты информации на узлах компьютерной сети

Средства защиты информации на узлах компьютерной сети. Требования защиты информации в локальной вычислительной сети. Классификация автоматизированных системы и классы защищенности.

6. Методы и инструменты используемые злоумышленниками для атак и способы их парирования.

Эволюция вымогателей: Цель – данные, а не системы.
Типы атак: Вредоносное ПО, Фишинг, Атаки на инфраструктуру, Атаки нулевого дня. Уязвимости: Нарушение политик безопасности сотрудниками, Недостаток осведомлённости и некомпетентность сотрудников, Недостаток знаний и навыков у ответственных за ИБ и ИТ, Уязвимости аппаратного и программного обеспечения.
Инструменты хакеров: Анализ сетевого трафика. Сканирование сети. Выявление пароля. IP-spoofing или подмена доверенного объекта сети. Отказ в обслуживании или Denial of Service (DoS). Атаки на уровне приложений.

7. Системные вопросы защиты программ и данных

Порядок защиты информационной системы. Порядок контроля ЛВС и рабочих станций. Объекты контроля. Анализ контролируемых событий.

8. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации

Пользовательские требования; Системные требования и ограничения; Функциональные требования; Нефункциональные требования.

6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения методов формирования, организации и поддержки комплекса мер по обеспечению информационной безопасности объекта защиты;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема) дисциплины	Задание	Методические рекомендации по выполнению задания	Форма контроля
1	2	3	4	5
1.	Тема № 1	Усвоить Приобрести навык	1. Изучить Характеристики информационных процессов 2. При выполнении лабораторной работы обратить внимание на информационные потоки, протекающие в ИС, исходя из них определить угрозы безопасности Литература основная[1,2]	Контрольный опрос Проверка выполнения лабораторной работы
2.	Тема № 2	Усвоить, Приобрести навык	1. Изучить характеристики носителей информации 2. Освоить методы восстановления информации и методы гарантированного удаления информации Литература основная[1,2]	Контрольный опрос Проверка выполнения лабораторной работы
3.	Тема № 3	Усвоить Приобрести навык	1. Проанализировать особенности прохождения информационных потоков при работе на изолированном компьютере 2. Освоить настройку встроенных средств безопасности в операционных системах семейства Windows Литература основная[1,2], дополнительная [4]	Проверка выполнения лабораторной работы
4.	Тема № 4	Усвоить Приобрести навык	1. Повторить протоколы сетевой модели 2. Изучить особенности работы протоколов с позиции из уязвимости 3. Освоить программного обеспечение для сканирования сети и методы блокировки сканирования Литература основная[1,2], дополнительная [1-8]	Контрольный опрос Проверка выполнения лабораторной работы
5.	Тема № 5	Усвоить Приобрести навык	1. Изучить виды средств защиты информации на узле компьютерной сети 2. Освоить настройку встроенных средств защиты ОС Windows от внешних сетевых атак Литература основная[1-6], дополнительная [1-9]	Контрольный опрос Проверка выполнения лабораторной работы
6.	Тема № 6	Усвоить Приобрести навык	1. Изучить типы атак и механизмы их реализации 2. Изучить классификацию и требования к антивирусной защиты ФСТЭК 3. Освоить установку и настройку	Контрольный опрос Проверка выполнения лабораторной работы

			антивируса в соответствии с особенностями функционирования рабочего места Литература основная[1-4], дополнительная [1-8]	
7.	Тема № 7	Усвоить Приобрес-ти навык	1. Изучить порядок применения средств защиты информации. 2. Изучить методы анализа контролируемых событий 3. Освоить метод анализа программного кода и методы противодействия анализу программного кода Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы
8.	Тема № 8	Усвоить	1. Изучить общую характеристику программно-аппаратных средств защиты информации с точки зрения защиты конкретных информационных поток Литература основная[1-4], дополнительная [1-8]	Контрольный опрос

Формой отчетности по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- Наличие полного конспекта лекций
- Сдача всех контрольных работ (3 шт) с положительным результатом

6.2. Тематика и задания для практических занятий (*при наличии*)

Не предусмотрены

6.3. Тематика и задания для лабораторных занятий

1. Определение основных угроз информационной безопасности в компьютерных системах
   Цель работы: Определить и сформулировать основные угрозы в компьютерной системе в зависимости от специфики ее работы. Определить потоки информации, циркулирующие в компьютерной системе.
2. Изучение физических особенностей носителей информации и файловых систем. Программные методы гарантированного удаления информации.
   Цель работы: сформировать умение восстанавливать информацию после удаления стандартными методами и гарантированно удалять информацию специализированными программными средствами
3. Настройка компонентов безопасности операционной системы изолированного компьютера
   Цель работы: сформировать умение настраивать механизмы защиты, встроенные в операционную систему, на примере, ОС Windows
4. Методы и инструменты используемые злоумышленниками для атак в локальной сети. Сканирование сети. Прослушивание трафика. Обнаружение открытых портов.
   Цель работы: познакомить с методами злоумышленников по несанкционированному получению информации о функционировании компьютерной сети, сформировать умение применять методы блокирования исследования сети и проведения сетевых атак.
5. Настройка операционной системы для блокировки сетевых атак.

Цель работы: сформировать умение настраивать механизмы сетевой защиты, встроенные в операционную систему, на примере, ОС Windows

6. Выбор и настройка антивирусного программного обеспечения в соответствии с выдвигаемыми требованиями
   Цель работы: сформировать умение выбирать, устанавливать и настраивать антивирусное программного обеспечение в соответствии с требованиями регулятора и условиями функционирования локальной сети.
7. Исследование программного кода и воздействия на него, на примере поиска константы и изменение кода.
   Цель работы: формирование знаний студентов о принципах представления целочисленных констант исходного кода программы в исполнительном модуле, понимание какую информацию стоит скрывать и как это делать наиболее простым методом.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

а) основная

1. **Долозов, Н.Л**. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. - 63 с. : схем., ил. - Библиогр. в кн. - ISBN 978-5-7782-2753-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438307
2. **Технологии защиты** информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820
3. **Аппаратные и программные средства защиты информации**: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6 **http://znanium.com/catalog.php?bookinfo=923168**
4. **Программно-аппаратная защита информации**: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-004-7, 500 экз. **http://znanium.com/catalog.php?bookinfo=489084**
5. **Хорев, Павел Борисович.** Программно-аппаратная защита информации : учеб. пособие для студ. вузов напр "Информац. безопасность" и "Информатика и выч. техника" / Хорев, Павел Борисович. - Москва : ФОРУМ, 2013; 2011. - 352 с.: ил. - (Высш. образование). - ОПД. - обязат. - ISBN 978-5-91134-353-8 : 346.00; 250.00.
6. **Пушкарев, В.П**. Защита информационных процессов в компьютерных системах: (Безопасность жизнедеятельности 2) : учебное пособие / В.П. Пушкарев, В.В. Пушкарев ; Министерство образования и науки Российской Федерации, Федеральное бюджетное государственное образовательное учреждение высшего профессионального образования, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). Кафедра средств радиосвязи (СРС). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2005. - 131 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208718
7. Душин, В. К. **Теоретические основы информационных процессов и систем** [Электронный ресурс] : Учебник / В. К. Душин. - 5-е изд. - М.: Издательско-торговая корпорация «Дашков и К°», 2014. - ISBN 978-5-394-01748-3. **http://znanium.com/catalog.php?bookinfo=450784**

б) дополнительная

1. **Системы защиты** информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351
2. **Шандриков, А.С**. Информационные технологии : учебное пособие / А.С. Шандриков. - Минск : РИПО, 2015. - 444 с. : ил. - Библиогр.: с. 426-430. - ISBN 978-985-503-530-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=463339
3. **Нестеров, С.А.** Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
4. **Креопалов, В.В.** Технические средства и методы защиты информации : учебно-практическое пособие / В.В. Креопалов. - Москва : Евразийский открытый институт, 2011. - 278 с. - ISBN 978-5-374-00507-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90753
5. **Обеспечение информационной безопасности машиностроительных предприятий** : В 2-х ч.: учебник для вузов. Ч. 2 / С. А. Клейменов [и др.]. - Старый Оскол : ТНТ, 2011. - 432 с.: рис. - УМО. - СД. - обязат. - ISBN 978-5-94178-282-6 : 617.78.
6. **Мельников, В. П.** Информационная безопасность : Учеб. пособие для студ. образоват. учреждений сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : Академия, 2005. - 336 с. - (Среднее профессиональное образование) (Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 5-7695-1816-2 : 237.33.
   Допущено МО РФ
7. **Мельников, Владимир Павлович.** Информационная безопасность и защита информации : учеб. пособие для вузов спец. 230201 "Информац. системы и технологии" / Мельников Владимир Павлович, С. А. Клейменов, А. М. Петраков ; под ред. Клейменова С.А. - 3-е изд., стер. - Москва : Академия, 2008. - 336 с. - (Высш. проф. образов. Информат. и выч. техн.). - УМО. - ЕН, ОПД, СД. - ISBN 978-5-7695-4884-0 : 165.66.
8. **Щекочихин, Олег Владимирович.** Администрирование информационных систем и защита информации : учеб. пособие / Щекочихин Олег Владимирович. - Кострома : КГТУ, 2014. - 110 с. - б.
9. Информационные технологии: разработка информационных моделей и систем: Учеб. пос. / А.В.Затонский - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014 - 344с.: 60x88 1/16 + (Доп. мат. znanium.com) - (Высшее образование: Бакалавриат)(о) ISBN 978-5-369-01183-6, 500 экз. http://znanium.com/catalog.php?bookinfo=400563
10. Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - 2-е изд. - М.: Форум: НИЦ ИНФРА-М, 2014. - 448 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-833-5, 1000 экз. http://znanium.com/catalog.php?bookinfo=435900
11. Информационные технологии и системы: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0376-6 http://znanium.com/catalog.php?bookinfo=429113
12. **Соловьев, Игорь Владимирович.** Проектирование информационных систем. Фундаментальный курс : учеб. пособие для вузов напр. "Информац. системы" / Со-

ловьев Игорь Владимирович, Майоров Андрей Александрович ; под ред. В. П. Савиных. - Москва : Академ. проект, 2009. - 398 с. - (Фундамент. учебник). - УМО. - СД. - обязат. - ISBN 978-5-8291-1156-4 : 343.00.
13. **Советов, Борис Яковлевич.** Информационные технологии : учебник для вузов по напр. "Информ. системы" / Советов Борис Яковлевич, Цехановский Владислав Владимирович. - 4-е изд., стереотип. - Москва : Высш. шк., 2008. - 263 с.: ил. - МО РФ напр. - Информатика и вычислительная техника; Информационные системы. - ОПД. - ISBN 978-5-06-004275-7 : 160.00.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Информационно-образовательные ресурсы:
1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:
1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6.Электронно-библиотечная система (ЭБС) «Инфра-М».

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

Лекционная аудитория, оснащенная проектором, компьютером.
Лаборатория программно-аппаратных средств обеспечения информационной безопасности - компьютерный класс 9 персональных компьютеров
Перечень специального оборудования и программного обеспечения

1. Комплект СЗИ НСД Scarlet Net v 7.0 + Secret Net Card
2. Программный комплекс защиты от НСД «Zecurion Lock»
3. Программный комплекс защиты от НСД «Dallas Lock 8.0-K»
4. Программно-аппаратный комплекс защиты от НСД «Соболь»
5. Аппаратный модуль доверенной загрузки «Аккорд ФМДЗ»
6. Комплекс СЗИ НСД «Страж NT»
7. Модуль защиты от НСД и контроля устройств средства защиты информации Secret Net Studio 8.
8. Модуль защиты диска и шифрования контейнеров средства защиты информации Secret Net Studio 8.
9. Модуль персонального межсетевого экрана средства защиты информации Secret Net Studio 8.
10. Комплект "Дополнительная защита" средства защиты информации Secret Net Studio 8.
11. Средство защиты информации Secret Net LSP.
12. Модуль Континент АП.
13. Средства защиты информации vGate R2 Enterprise Plus.
14. Модуль Secret MDM Secure Pack