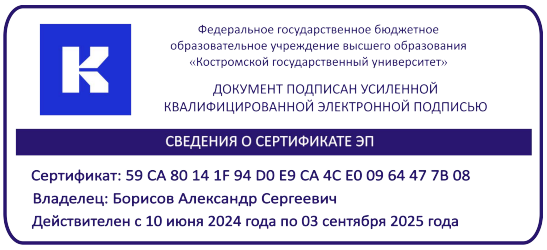
МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

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 «Программно-аппаратные средства защиты информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»;
- формирование у бакалавров профессиональных навыков по эксплуатации и обслуживанию аппаратуры, оборудования и программного обеспечения, связанных с:
-обеспечением безопасности данных;
- шифрованием и защитой от несанкционированного доступа;
- профессиональных навыков выявления и уничтожения компьютерных вирусов;
- противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- навыков работы со специальной технической литературой;
- создание представления о принципах, методах и средствах выявления угроз безопасности информационных систем;
- развитие способностей к логическому и алгоритмическому мышлению и осуществлению проверки защищенности объектов на соответствие требованиям нормативных документов.

Задачи дисциплины:

- Изучение программно-аппаратной защиты информации;
- Изучение принципов построения программно-аппаратных средств разведки;
- Изучение принципов организации работ по программно-аппаратной защите информации;

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:
знать:
- методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;
− современные средства разработки и анализа программного обеспечения на языках высокого уровня.
уметь:
- организовывать работу по программно-аппаратной защите информации;
- устанавливать, настраивать и обслуживать программно-аппаратные средства защиты информации;
- контролировать эффективность мер программно-аппаратной защиты информации.
владеть:
- формальной постановки и решения задач по программно-аппаратной защиты информации;
- оформления рабочей технической документации с учетом действующих нормативных и методических
- документов в области информационной безопасности;
- организации проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.

В результате изучения учебной дисциплины «Программно-аппаратные средства защиты информации» 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 выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

способностью проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-2.1);

способностью формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2.2);

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 четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «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:	68
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа в часах	76
Форма промежуточной аттестации	экзамен

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	34
Практические занятия	-
Лабораторные занятий	34
Консультации	3,7
Зачет/зачеты	-
Экзамен/экзамены	0,35
Курсовые работы	-
Курсовые проекты	–
Всего	38,05

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	Лаб	
1.	Введение (предмет и задачи программно-аппаратной защиты информации; методы и средства защиты информации и предотвращения несанкционированного доступа)	12	2	2	4
2.	Идентификация и аутентификация (идентификация пользователей (субъектов доступа к данным); процедура идентификации и аутентификации; однофакторная и двухфакторная идентификации; биометрические методы идентификации и аутентификации; технологии автоматической идентификации; протоколы идентификации/аутентификации	12	2	2	5
3.	Обобщенный алгоритм аутентификации, на основе алгоритма RSA, схемы Фейге-Фиата-Шамира. Эль-Гамаля, Шнорра, протоколы идентификации с нулевой передачей знаний; протоколы Kerberos, S/Key (RFC 1760), PAP и CHAP. OpenID, Windows Live ID, LDAP, OpenLDAP)	12	2	2	5
4.	Система разграничения доступа к информации (архитектура системы; концепция построения систем разграничения доступа)	12	2	2	5
5.	Модели разграничения доступа	12	2	2	5
6.	Методы и средства защиты программ от компьютерных вирусов. Характеристика и классификация компьютерных вирусов.	12	2	2	5
7.	Требования к антивирусной защите ФСТЭК России. Классификация методов защиты от компьютерных вирусов	10	2	2	5
8.	Классификация средств защиты. Государственный реестр сертифицированных средств защиты информации.	10	2	2	5
9.	Краткая характеристика средств защиты Secret	10	2	2	5

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лаб	
	Net, Пак Криптон, Secret Disk и другие.				
10.	Общая характеристика электронных идентификаторов (eToken, JKarta, Maxim (iButton), Sentinel, Guardant, Rutoken, CmDongle, WibuKey, SenseLock, LOCK и т.д.)	10	2	2	5
11.	Защита программ от программных закладок. Способы внедрения закладок. Классификация не декларированных возможностей программного обеспечения. Методы вскрытия не декларированных возможностей. Подходы выявления дефектов в программном обеспечении. Возможны методы защиты.	20	4	4	10
12.	Методы и способы защиты программ от исследования	10	2	2	5
13.	Подходы к защите программ от несанкционированного копирования	10	2	2	5
14.	Архитектура программно-аппаратных средств защиты информации. Конфигурация средств программно-аппаратных средств защиты информации. Методы реализации, функционал и особенности использования программно-аппаратных средств защиты информации	20	4	4	10
Экзамен		36			
Всего:		**180**	**34**	**34**	**86**

5.2. Содержание:

1. **Введение (предмет и задачи программно-аппаратной защиты информации;)**

Предмет и задачи программно-аппаратной защиты информации основные понятия, уязвимость компьютерных систем, политика безопасности в компьютерных системах. Оценка защищенности. Методы и средства защиты информации и предотвращения несанкционированного доступа.

2. **Идентификация и аутентификация**

Идентификация пользователей (субъектов доступа к данным); процедура идентификации и аутентификации; однофакторная и двухфакторная идентификации; биометрические методы идентификации и аутентификации; технологии автоматической идентификации; протоколы идентификации/аутентификации

3. **Протоколы идентификации.**

Обобщенный алгоритм, на основе алгоритма RSA, схемы Фейге-Фиата-Шамира. Эль-Гамаля, Шнорра, протоколы идентификации с нулевой передачей знаний; протоколы Kerberos, S/Key (RFC 1760), PAP и CHAP. OpenID, Windows Live ID, LDAP, OpenLDAP)

4. **Система разграничения доступа к информации (архитектура системы; концепция построения систем разграничения доступа)**

Основными функциями системы разграничения доступа (СРД) являются: реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным; реализация ПРД субъектов и их процессов к устройствам создания твердых копий; изоляция программ

процесса, выполняемого в интересах субъекта, от других субъектов; управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа; реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.
Функционирование СРД опирается на выбранный способ разграничения доступа. Наиболее прямой способ гарантировать защиту данных - это предоставить каждому пользователю вычислительную систему как его собственную. В многопользовательской системе похожих результатов можно добиться использованием модели виртуальной ЭВМ.

5. Модели разграничения доступа; надежность систем разграничения доступа

Рассмотрены основные модели разграничения доступа к объектам компьютерных систем со стороны их субъектов.
Дискреционное разграничение доступа к объектам (Discretionary Access Control — DAC)
Мандатное разграничение доступа (Mandatory Access Control — MAC)
Ролевое разграничение доступа (Role-Based Access Control — RBAC)
Особенности организации, достоинства и недостатки каждой модели

6. **Методы и средства защиты программ от компьютерных вирусов.**

Компьютерные вирусы как особый класс разрушающего программного воздействия; защита от разрушающего программного воздействия; антивирусные программы. Характеристика и классификация компьютерных вирусов. Характеристика средств нейтрализации компьютерных вирусов.

7. Требования к антивирусной защите ФСТЭК России.

Классы и требования средств антивирусной защиты. Классификация методов защиты от компьютерных вирусов

8. Общая характеристика программно-аппаратных средств защиты информации

Основными средствами программно-технической защиты информации в современных автоматизированных системах являются: - идентификация и аутентификация; - управление доступом; - протоколирование и аудит; - криптография; - экранирование; - антивирусная защита.

9. Классификация средств защиты. Государственный реестр сертифицированных средств защиты информации.

Правовые основы ведения государственного реестра сертифицированных средств защиты информации. Требования сертифицирующего органа и порядок сертификации.

10. Краткая характеристика средств защиты Secret Net, Пак Криптон, Secret Disk и другие.

Основные характеристики, функциональные возможности, достоинства, недостатки, сферы применения и ограничения.

11. Общая характеристика электронных идентификаторов

Особенности реализации идентификаторов eToken, JKarta, Maxim (iButton), Sentinel, Guardant, Rutoken, CmDongle, WibuKey, SenseLock, LOCK. Достоинства, недостатки, сферы применения

12. Защита программ от программных закладок.

Способы внедрения закладок. Классификация не декларированных возможностей программного обеспечения. Методы вскрытия не декларированных возможностей. Подходы выявления дефектов в программном обеспечении. Возможны методы защиты.
Сигнатурное и эвристическое сканирование. Аппаратные средства противодействия вредоносному коду. Контроль целостности программного обеспечения. Мониторинг инфор-

мационных потоков. Изолированная программная среда. Цифровая подпись исполняемого кода. Шифрование исполняемого кода. Средства анализа уязвимостей.

13. Методы и способы защиты программ от исследования

Принципы создания и использования систем защиты от исследования. Требования к системам защиты от исследования. Основные компоненты системы защиты от исследования. Активные и пассивные методы, затрудняющие исследование программ. Обфускация кода.

14. Подходы к защите программ от несанкционированного копирования

Принципы создания и использования систем защиты от копирования. Требования к системам защиты от копирования. Основные компоненты системы защиты от копирования. Методы, затрудняющие считывание скопированной информации, криптографические методы, методы с использованием идентификатора

15. Архитектура программно-аппаратных средств защиты информации.

Конфигурация средств программно-аппаратных средств защиты информации
Методы реализации, функционал и особенности использования программно-аппаратных средств при защите операционных систем, баз данных, сетевых соединений.

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) дисциплин	Задание	Методические рекомендации по выполнению задания	Форма контроля
1	2	3	4	5

1.	Тема № 1	Усвоить	1. Изучить Предмет и задачи программно-аппаратной защиты информации Литература основная[1,2]	Контрольный опрос
2.	Тема № 2	Усвоить,	1. Изучить основные понятия идентификации и аутентификации. 2. Факторы и методы аутентификации. Литература основная[1,2]	Контрольный опрос
3.	Тема № 3	Усвоить	1. Изучить алгоритмы идентификации и аутентификации Литература основная[1,2], дополнительная [4]	Проверка выполнения лабораторной работы
4.	Тема № 4	Усвоить	1. Изучить структуру и функции системы разграничения доступа Литература основная[1,2], дополнительная [1-8]	Контрольный опрос
5.	Тема № 5	Усвоить	1. Изучить модели разграничения доступа Литература основная[1-6], дополнительная [1-9]	Контрольный опрос
6.	Тема № 6	Усвоить	1. Изучить классификацию компьютерных вирусов, отличительные признаки. Методы защиты. Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
7.	Тема № 7	Приобрес-ти навык	1. Изучить классификацию и требования к антивирусной защиты ФСТЭК Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы
8.	Тема № 8	Усвоить	1. Изучить общую характеристику программно-аппаратных средств защиты информации. Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
9.	Тема № 9	Усвоить, Приобрес-ти навык	1. Изучить государственных реестр сертифицированных средств защиты информации. 2. Найти все антивирусы из реестра ФСТЭК, определить их класс. Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы
10.	Тема № 10	Приобрес-ти навык	1. Изучить характеристики электронных идентификаторов 2. Выполнить работы по установке и настройке системы ключевой идентификации (по уточненному списку) Литература основная[1-4], дополнительная [1-9]	Проверка выполнения лабораторной работы
11.	Тема № 11	Приобрес-ти навык	1. Изучить характеристики средств защиты 2. Выполнить работы по установке и	Контрольный опрос

			настройке СЗИ Secret Net (или другой из имеющихся) Литература основная[1-4], дополнительная [1-9]	
12.	Тема № 12	Усвоить	1.Изучить классификацию не декларированных возможностей программного обеспечения и методы их обнаружения. Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
13.	Тема № 13	Усвоить	Познакомиться с основными компонентами системы защиты от исследования. Реализовать обфускацию кода средствами среды разработки Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
14.	Тема № 14	Приобрести навык	Изучить методы, затрудняющие копирование программного обеспечения. Литература основная[1-6], дополнительная [1-8]	Проверка выполнения лабораторной работы
15.	Тема № 15	Приобрести навык	1. Выполнить работы по установке и настройке СЗИ VipNet (или другой из имеющихся) Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы

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. Использование специализированных аппаратно-программных средств защиты информации от несанкционированного доступа. Создание защищенных виртуальных дисков средствами программно-аппаратных комплексов и «SecretDisk»
2. Использование СЗИ «Соболь» для построения системы ключевой аутентификации
3. Использование аппаратного модуля доверенной загрузки «Аккорд ФМДЗ для построения системы ключевой аутентификации
4. Защита информации от несанкционированного доступа средствами программно-аппаратного комплекса «Dallas Lock»
5. Реализация многоуровневой политики разграничения доступа средствами программно-аппаратного комплекса «Страж NT»
6. Комплексная защита информации средствами программно-аппаратного комплекса «Secret NET».
7. Организация VPN средствами протокола PPTP .
8. Защита сетевого трафика средствами протокола IPSec в ОС Windows NT 5 .
9. Организация VPN средствами протокола SSL в ОС Windows Server 2003
10. Применение специализированных средств организации VPN на примере «VipNet».
11. Организация защищенного документооборота с использованием криптографических средств, предоставляемых СКЗИ «КриптоПро».
12. Исследование возможностей антивирусов. Выбор антивируса в соответствии с требованиями защиты по определенному классу.

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.

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.

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