Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1153523	Методы и средства защиты информации

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Безопасность компьютерных систем	**Код ОП** 1. 10.03.01/33.01
Направление подготовки 1. Информационная безопасность	**Код направления и уровня подготовки** 1. 10.03.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Методы и средства защиты информации

1.1. Аннотация содержания модуля

Модуль посвящен изучению видов, источников и носителей защищаемой информации, рассматриваются демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники; структура, классификация и основные характеристики технических каналов утечки информации. Изучаются возможности видов технической разведки; концепция и методы инженерно-технической защиты информации и излагаются методы расчета и инструментального контроля показателей защиты информации.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Технические средства охраны	4
2	Программно-аппаратные средства защиты информации	5
	ИТОГО по модулю:	9

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Высшая математика для профессиональной деятельности
Постреквизиты и кореквизиты модуля	1. Организационно-правовые основы информационной безопасности 2. Защита информации от утечки по техническим каналам

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Программно-аппаратные средства защиты	ПК-1 - Способен оценивать роль информации,	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном

информации	информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Определять оптимальные методы обеспечения информационной безопасности П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
	ПК-3 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	З-1 - Изложить состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации З-2 - Изложить методологию управления информационной безопасностью, основанную на нормативных и методических документах У-1 - Применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации П-1 - Осуществлять обоснованный выбор методов поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации П-2 - Разрабатывать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации

	ПК-6 - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	З-1 - Описать основные перспективы развития науки и техники в области профессиональной деятельности, в том числе системы поддержки принятия решений, системы искусственного интеллекта У-1 - Применять методы и системы искусственного интеллекта при реализации практических разработок в области защиты информации в телекоммуникационных системах У-2 - Формулировать задачи исследования, выбирать методы и средства их решения П-1 - Иметь опыт решения научно-технических задач в области своей профессиональной деятельности
	ПК-9 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты информации телекоммуникационных систем З-2 - Описать основные методы инструментального мониторинга и аудита защищенности телекоммуникационных систем У-1 - Администрировать средства и системы защиты информации телекоммуникационных систем П-1 - Иметь практический опыт выбора средств контроля функционирования средств и систем управления информационной безопасностью телекоммуникационных систем
Технические средства охраны	ПК-3 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	З-1 - Изложить состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации З-2 - Изложить методологию управления информационной безопасностью, основанную на нормативных и методических документах

		У-1 - Применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации П-1 - Осуществлять обоснованный выбор методов поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации П-2 - Разрабатывать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации
	ПК-9 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты информации телекоммуникационных систем З-2 - Описать основные методы инструментального мониторинга и аудита защищенности телекоммуникационных систем У-1 - Администрировать средства и системы защиты информации телекоммуникационных систем П-1 - Иметь практический опыт выбора средств контроля функционирования средств и систем управления информационной безопасностью телекоммуникационных систем

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной и очно-заочной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Технические средства охраны

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Духан Евгений Изович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”
2	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”
3	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
4	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _6_ от _26.05.2023_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Духан Евгений Изович, Профессор,**
- **Куц Дмитрий Владимирович, Старший преподаватель,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Концепция технической защиты информации	Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
2	Теоретические основы технической защиты информации	Информации как предмет защиты. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как

		источники опасных сигналов. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения. Организованные каналы утечки (съема) информации –закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала
3	Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства. Физические процессы при подавлении опасных сигналов. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Средства предотвращения утечки

		информации по техническим каналам. Средства 7маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.
4	Организационные основы технической защиты информации	Государственная система защиты информации.Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженернотехнической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-9 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты информации телекоммуникационных систем

			соответствующих проектных решений	

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Технические средства охраны

Электронные ресурсы (издания)

1. , Шелупанов, А. А., Киреенко, А. П.; Экономическая безопасность: финансовые, правовые и IT-аспекты: материалы второй Всероссийской научно-практической онлайн-конференции, 29 марта 2018 г. : материалы конференций.; Директ-Медиа, Москва, Берлин; 2018; https://biblioclub.ru/index.php?page=book&id=562277 (Электронное издание)

Печатные издания

1. Бузов, Г. А., Калинин, С. В., Кондратьев, А. В.; Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России.; Горячая линия - Телеком, Москва; 2005 (17 экз.)

2. Домарев, В. В.; Безопасность информационных технологий. Методология создания систем защиты; DiaSoft, Москва; СПб.; Киев; 2002 (5 экз.)

3. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Технические средства охраны

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Подключение к сети Интернет	
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES

		Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _6_ от _26.05.2023_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Куц Дмитрий Владимирович, Старший преподаватель,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Применение средств криптографической защиты информации	Система защиты корпоративной информации «Secret Disk». Основные характеристики Создание защищенных логических дисков. Работа с защищенными дисками. Настройка параметров СКЗИ. Управление секретными дисками. Хранение конфиденциальной информации на съемных носителях. Система криптографической защиты «КриптоАРМ». Система криптографической защиты «КриптоПро». Компоненты удостоверяющего центра. Развёртывание удостоверяющего центра на баз «КриптоПро». Свободно распространяемое средство криптографической защиты «VeraCrypt».
2	Применение СЗИ от НСД для организации защищенных компьютерных систем.	Использование специализированных аппаратно-программных средств защиты информации (СЗИ) Назначение и возможности СЗИ от НСД, требования, предъявляемые к ним. Реализация в СЗИ ограничения на вход в систему и политики разграничения доступа. Контроль технологического мусора. Обзор современных отечественных средств защиты информации. Применение СЗИ от НСД «Страж-NT». Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Организация учета сменных носителей информации. Регистрация событий. Гарантированное удаление данных. Применение СЗИ от НСД

		«Dallas Lock». Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Печать штампа. Регистрация событий. Гарантированное удаление данных. Реализация запрета загрузки ПЭВМ в обход СЗИ. Применение СЗИ от НСД «Secret NET». Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Регистрация событий. Гарантированное удаление данных. Настройка механизма шифрования.
3	Применение средств организации виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Развертывание защищенной сети VipNet. Межсетевое взаимодействие в сетях VipNet. Организация VPN средствами СЗИ Континент. Развертывание центра управления сетью Континент. Организация VPN между защищаемыми сетями и между удаленным пользователем и защищаемой сетью на базе СЗИ Континент.
4	Проектирование средств криптографической защиты информации	Применение библиотек CryptoAPI для работы с СКЗИ «КриптоПро CSP». Создание, загрузка и удаление криптографического контейнера. Генерация, проверка наличия и экспорт открытых ключей. Формирование и проверка электронной подписи файлов. Зашифрование и расшифрование данных файла. Гарантированное уничтожение файла.
5	Проектирование средств защиты информации от несанкционированного распространения	Общие принципы построения подсистем защиты от несанкционированного распространения программного обеспечения на основе электронных ключей Guardant Использование электронных ключей Guardant для защиты приложений

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональн	ПК-9 - Способен проводить подготовку исходных данных для проектирования подсистем, средств	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты

		ой деятельности	обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	информации телекоммуникационных систем

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Электронные ресурсы (издания)

1. , Синадский, , Н. И.; Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие.; Уральский федеральный университет, ЭБС АСВ, Екатеринбург; 2014; http://www.iprbookshop.ru/65983.html (Электронное издание)

Печатные издания

1. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

2. Хорев, П. Б.; Программно-аппаратная защита информации : [учеб. пособие] для студентов вузов, обучающихся по направлению "Информ. безопасность" и "Информатика и вычисл. техника".; ФОРУМ, Москва; 2009 (2 экз.)

Профессиональные базы данных, информационно-справочные системы

Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Банк данных угроз безопасности информации - Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
3	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	