

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
1156041	Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры	Код ОП 1. 10.04.01/22.01
Направление подготовки 1. Информационная безопасность	Код направления и уровня подготовки 1. 10.04.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Согласовано:

Управление образовательных программ

Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)

1.1. Аннотация содержания модуля

Целью модуля является приобретение новых и/или совершенствование существующих компетенций учащихся в сфере информационной безопасности. Изучаются требования к мерам защиты информации от несанкционированного доступа и принцип их выбора; установка, настройка и администрирование средств защиты информации от несанкционированного доступа; оценивание и инструментальные средства анализа защищенности компьютерных систем, экспертное оценивание трудно формализуемых свойств (параметров); методы и стандарты оценки защищенности, правовые аспекты ИСПДн, ГИС и значимых объектов КИИ. В модуль входят: - Меры и средства защиты информации от несанкционированного доступа (НСД) в ИСПДн, ГИС и значимых объектах КИИ; - Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ; - Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ.

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	Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ	3
2	Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ	3
3	Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ	3
ИТОГО по модулю:		9

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	<ol style="list-style-type: none">1. Математические методы информационной безопасности2. Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

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
<p>Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ</p>	<p>ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание</p>	<p>З-1 - Понимать основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности</p> <p>З-2 - Различать направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем</p> <p>У-1 - Проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности</p> <p>У-2 - Формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ</p> <p>П-2 - Разрабатывать концептуальные стратегии решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ</p>
	<p>ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности</p>	<p>З-1 - Понимать методы концептуального проектирования технологий обеспечения информационной безопасности</p> <p>З-2 - Использовать современные методы и средства тестирования</p> <p>У-1 - Выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью</p> <p>П-1 - Обладать навыками практической реализации типовых задач разработки и исследования систем защиты информации</p>

		компьютерных систем и сетей и систем обеспечения информационной безопасностью
	ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	<p>З-1 - Различать отечественные и зарубежные стандарты в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов</p> <p>З-2 - Понимать правила создания технического задания на создание подсистем безопасности информационных систем</p> <p>З-3 - Перечислять основные угрозы безопасности информации и модели нарушителя в информационных системах</p> <p>З-4 - Формулировать основные нормативные правовые акты в области обеспечения информационной безопасности</p> <p>З-5 - Понимать нормативные методические документы ФСБ России в области защиты информации</p> <p>З-6 - Использовать нормативные методические документы ФСТЭК России в области информационной безопасности</p> <p>У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности</p> <p>У-2 - Разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации</p> <p>У-3 - Разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации</p> <p>У-4 - Разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности</p> <p>У-5 - Работать с технической и эксплуатационной документацией</p>

		<p>П-1 - Разрабатывать политики безопасности различных уровней</p> <p>П-2 - Производить расчеты и управлять рисками в информационной безопасности, в соответствии с требованиями уровня безопасности, стоимости и сроков реализации</p> <p>П-3 - Иметь опыт работы с нормативными правовыми актами в области информационной безопасности</p>
	<p>ОПК-4 - Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок</p>	<p>З-3 - Характеризовать современные достижения науки в области информационной безопасности</p> <p>П-4 - Осуществлять поиск информации в глобальной информационной сети Интернет</p>
<p>Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ</p>	<p>ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности</p>	<p>З-3 - Описывать принципы построения и функционирования современных информационных систем</p> <p>З-4 - Объяснять назначение комплексной системы защиты информации, принципы ее организации и этапы разработки</p> <p>У-3 - Разрабатывать модели угроз и нарушителей информационной безопасности информационных систем</p> <p>П-2 - Участвовать в организации комплексной системы защиты объекта</p>
<p>Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ</p>	<p>ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание</p>	<p>З-3 - Понимать методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности</p> <p>У-3 - Разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ. Оценивать эффективность решений и анализировать показатели деятельности</p> <p>П-1 - Участвовать в разработке системы обеспечения информационной безопасности объекта</p>

		П-3 - Планировать и оценивать трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений
	ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	З-2 - Использовать современные методы и средства тестирования У-2 - Проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Меры и средства защиты информации от
несанкционированного доступа в ИСПДн,
ГИС и значимых объектах КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Каннер Татьяна Михайловна		старший преподавате ль	МФТИ

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

Протокол № 10 от 04.03.2022 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Исключительно электронного обучения с использованием онлайн-курса университета-партнера в рамках сетевого договора
- 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	онлайн-курс университета-партнера в рамках сетевого договора дисциплина "Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ"	https://openedu.ru/course/mipt/ISMMAUA/?session=spring_2022

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ

Электронные ресурсы (издания)

Профессиональные базы данных, информационно-справочные системы

Меры и средства защиты информации от несанкционированного доступа

https://openedu.ru/course/mipt/ISMMAUA/?session=spring_2022

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

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ

Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащённость 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 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Student EES
2	Текущий контроль и промежуточная аттестация	Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM

3	Самостоятельная работа студентов	Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM
4	Лабораторные занятия	Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы контроля защищенности
информации ИСПДн, ГИС и значимых
объектов КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподавате ль	

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

Протокол № 10 от 04.03.2022 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

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	Анализ способов оценки защищенности компьютерных систем	Формальная постановка задачи измерения/оценивания объектов; Особенности и разновидности методов оценивания защищенности компьютерных систем; Объект и предмет оценивания защищенности компьютерных систем; Угрозно-вероятностное оценивание защищенности компьютерных систем; Оценивание защищенности компьютерных систем в идеологии «рисков»; Оценивание защищенности компьютерных систем по анализу реализованности установленных требований; Оценивание защищенности компьютерных систем путем испытаний.
2	Инструментальные средства анализа защищенности компьютерных систем	Инструментальные средства анализа защищенности компьютерных систем; Классификация и общая характеристика с средствами ментального анализа. защищенности компьютерных систем; Демонстрация функциональных возможностей сетевого сканера безопасности XSpider; Программные средства поддержки комплексной оценки уровня информационной безопасности организационных структур; Программно-инструментальная система метрического анализа уязвимостей компьютерных систем CVSS; Алгоритм расчета риска нарушения безопасности ИТСиС КВО по результатам испытаний исследований .
3	Определение весовых коэффициентов компетентности специалистов-экспертов	Определение весовых коэффициентов компетентности специалистов-экспертов; Градации показателя компетентности; Учет компетентности по взаимооценкам специалистов-экспертов; Парное сравнение как метод

		экспертного оценивания порядка предпочтения на некоторой совокупности анализируемых объектов; Оценка компетентности экспертов на основе оценивания эталонного объекта
--	--	---

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ

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. , Андрончик, А. Н., Богданов, В. В., Домуховский, Н. А., Коллеров, А. С., Синадский, Н. И., Хорьков, Д. А., Щербаков, М. Ю.; Защита информации в компьютерных сетях. Практический курс : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем".; УГТУ-УПИ, Екатеринбург; 2008 (1 экз.)

2. 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

Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ

Сведения об оснащении 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 EDUA5 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	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		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 Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Не требуется
4	Самостоятельная работа студентов	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Стандарты и методы оценки защищенности
ИСПДн, ГИС и значимых объектов КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподавате ль	
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

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

Протокол № 10 от 04.03.2022 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

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	Общие сведения о стандартах оценки защищенности и «Общие критерии»	Общие сведения об отечественных и зарубежных стандартах оценки защищенности компьютерных систем ”Общие критерии“ и национальные стандарты на их основе
2	Профили и стандарты защиты	Профили защиты ФСТЭК России Стандарты ISO/IEC серии 27000 Менеджмент риска ИБ. Защита информации в финансовых организациях

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ

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. Гайдамакин, Н. А.; Разграничение доступа к информации в компьютерных системах; Издательство Уральского университета, Екатеринбург; 2003 (3 экз.)

2. , Гайдамакин, Н. А.; Сборник нормативных правовых актов по компьютерной и информационной безопасности Т. 2. Ведомственные нормативные правовые акты и руководящие документы; Гриф, Екатеринбург; 2006 (1 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.)

4. Афонцев, Э. В.; Разработка методики выявления аномалий трафика в магистральных Интернет-каналах : дис. на соиск. учен. степ. канд. техн. наук : 05.13.01. ; Екатеринбург; 2007 (1 экз.)

5. Синадский, Н. И., Бакланов, В. В.; Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие.; [ГОУ ВПО УГТУ-УПИ], Екатеринбург; 2007 (70 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

Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ

Сведения об оснащении 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 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Student 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 Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Student EES

3	Текущий контроль и промежуточная аттестация	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Доска аудиторная</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p>	Не требуется
4	Самостоятельная работа студентов	<p>Периферийное устройство</p> <p>Персональные компьютеры по количеству обучающихся</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p> <p>Подключение к сети Интернет</p>	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES