МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Брянский государственный технический университет» (БГТУ)

Факультет информационных технологий

(наименование факультета/института)

Системы информационной безопасности

(наименование кафедры, ответственной за реализацию дисциплины)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 3E0E6C00DDAD69AC496A79E33A58FAAB
Владелец: Федонин Олег Николаевич
Действителен: с 11.11.2021 до 11.02.2023

УТВЕРЖДАЮ
Первый проректор
по учебной работе и цифровизации
_____ В.А. Шкаберин
«___» _____ 20 __ г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины

Теория построения комплексных систем защиты информации

(наименование дисциплины)

10.06.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Методы и системы защиты информации, информационная безопасность

(направленность (профиль)/ специализация образовательной программы)

высшее образование – подготовка кадров высшей квалификации

(уровень образования)

Исследователь. Преподаватель-исследователь

(квалификация, присваиваемая по специальности или направлению подготовки)

Очная

(форма обучения)

2020

(год набора)

Брянск 2022

Теория построения комплексных систем защиты информации

(наименование дисциплины)

10.06.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Методы и системы защиты информации, информационная безопасность

(направленность (профиль)/ специализация образовательной программы)

Разработал:

Заведующий кафедрой «СИБ», к.т.н., доцент		М.Ю. Рытов
(должность, ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Рассмотрена и одобрена на заседании кафедры
Системы информационной безопасности

(наименование кафедры, ответственной за реализацию дисциплины)

«25» марта 2022 г., протокол № 7

Заведующий кафедрой к.т.н., доцент		М.Ю. Рытов
(ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Предисловие

Дисциплина «Теория построения комплексных систем защиты информации» направлена на расширение профессионального научного кругозора обучающихся, в том числе частично на подготовку к сдаче кандидатского экзамена по научной специальности 2.3.6. «Методы и защиты информации, информационная безопасность».

1. Цель освоения дисциплины.

Целью освоения дисциплины является создание у обучающихся целостного представления о современных тенденциях в области исследования, модификации, разработки и проектирования комплексных систем защиты информации.

2. Место дисциплины в структуре ОПОП.

Дисциплина «Теория построения комплексных систем защиты информации» относится к дисциплинам по выбору вариативной части ОПОП по направлению подготовки 10.06.01 «Информационная безопасность», направленность (профиль) «Методы и системы защиты информации, информационная безопасность».

Дисциплина «Психология и педагогика высшей школы» изучается в 4 семестре.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Таблица 1

Компетенции и требования к освоению дисциплины

Коды компетенций по ФГОС ВО	**Наименование компетенции**	**Результат освоения**
1	**2**	**3**
Профессиональные компетенции		
ПК-1	Углубленное изучение теоретических и методологических основ проектирования, эксплуатации и развития систем защиты информации	**знать:** современные программные, технические средства и информационные технологии, обеспечивающие безопасность информации; **уметь**: применять современные программные, технические средства и информационные технологии, обеспечивающие безопасность информации; **владеть** методами применения современных программных, технических средств и информационных технологий, обеспечивающих безопасность информации.
ПК-2	Способность ставить и решать инновационные задачи, связанные с разработкой методов и технических средств, повышающих эффективность эксплуатации и проектирования средств защиты информации с использованием глубоких фундаментальных и специальных знаний, аналитиче-	**знать:** способы моделирования и оптимизации комплексных систем защиты информации; **уметь:** определять и рассчитывать критерии эффективности функционирования комплексных систем защиты информации; **владеть:** навыками разработки программных решений для моделирования и оптимизации комплексных систем защиты информации

	ских методов и сложных моделей в условиях неопределенности	
ПК-3	Умение проводить анализ, самостоятельно ставить задачу исследования наиболее актуальных проблем, имеющих значение для защиты информации, грамотно планировать эксперимент и осуществлять его на практике	**знать:** основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; **уметь:** разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; **владеть** методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.

4. Объем дисциплины и виды учебной работы.

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов).

Вид учебной работы	Всего часов	Семестр
		4
Аудиторные занятия (всего)	12	12
В том числе:	-	-
Лекции (Л)	6	6
Практические занятия (ПЗ)	6	6
Лабораторные работы (ЛР)	-	-
Самостоятельная работа (СРС) (без учета подготовки к экзамену)	51	51
В том числе:	-	-
Курсовой проект	-	-
Подготовка к занятиям	-	-
Самоподготовка	51	51
Экзамен	45	45
Общая трудоемкость: 108 часов; 3 зачетные единицы	108	108

5. Содержание дисциплины.

5.1. Содержание разделов дисциплины (табл. 2).

Таблица 2

Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела (дидактические единицы)
1	**2**	**3**
1	Принципы организации и этапы разработки КСЗИ	Особенности современных АС как объекта защиты, уязвимость основных структурно-функциональных элементов распределенных АС. Источники угроз безопасности информации, системная классификация и общий анализ угроз безопасности, методы оценки уязвимости информации. Классификация угроз безопасности, неформальная модель нарушителя в АС. Классификация каналов проникновения в систему и утечки информации, классификация видов нарушений работоспособности систем. Концепция создания КСЗИ, этапы создания КСЗИ, научно-исследовательская разработка КСЗИ

2	Технологическое и организационное построение КСЗИ	Объекты защиты, средства и методы защиты. Разработка модели КСЗИ, типы моделей управления доступом. Организационное направление работ по созданию КСЗИ, Технология построения КСЗИ, мероприятия по созданию и поддержанию функционирования комплексной системы защиты. Организационная структура, основные функции службы компьютерной безопасности. Методическое направление работ по созданию КСЗИ, концепция (Политика) безопасности, нормативное направление работ по созданию и функционированию КСЗИ.
3	Сущность и содержание контроля функционирования КСЗИ	Структура управления КСЗИ, проблемы управления КСЗИ, проблема использования средств единого управления безопасностью. Принципы функционирования КСЗИ, методы функционирования КСЗИ. Подсистема генерации отчетов, средства расследования инцидентов.

5.2. Разделы дисциплины и виды занятий (в часах) (табл.4).

Таблица 4

Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	С	СРС	ЭКЗ	Всего часов
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	Принципы организации и этапы разработки КСЗИ	2	2	-	-	17	15	36
2	Технологическое и организационное построение КСЗИ	2	2	-	-	17	15	36
3	Сущность и содержание контроля функционирования КСЗИ	2	2	-	-	17	15	36

6. Лекции, практические занятия, лабораторные работы.

6.1. Лекции (табл. 5).

Таблица 5

Тематика лекций и их трудоемкость

№ п/п	№ раздела дисциплины	Тематика лекций	Трудоемкость (час.)
1	**2**	**3**	**4**
1	1	Принципы организации и этапы разработки КСЗИ	2
2	2	Технологическое и организационное построение КСЗИ	2
3	3	Сущность и содержание контроля функционирования КСЗИ	2
Итого			6

6.2. Практические занятия (табл. 6).

Таблица 6

Тематика практических занятий и их трудоемкость

№ п/п	№ раздела дисциплины	Тематика практических занятий	Трудоемкость (час.)
1	**2**	**3**	**4**
1	1	Анализ объекта защиты	2
2	2	Построение математической модели общей оценки угроз безопасности.	2
3	3	Формирование сетевой модели комплексной системы защиты информации на основе типизации её элементов.	2
Итого			6

6.3. Образовательные технологии.

В рамках изучения дисциплины предусмотрены следующие образовательные технологии:

Лекции: проводятся в форме мастер-класса преподавателя; используются опорные конспекты (системы слайдов), доводимые до аудитории с помощью мультимедийного оборудования
Практические занятия: проводятся в форме мастер-класса преподавателя; используется контекстное обучение с привязкой разбираемых примеров к реальным конструкциям и условиям их работы
Самостоятельная работа студентов: при проведении самостоятельной работы обучающиеся имеют доступ в лабораторию вычислительной техники кафедры ПТМиО с выходом в сеть «Интернет», а также к электронно-библиотечной системе университета
Консультации: проводятся в форме дискуссии «учебная группа – преподаватель»
Экзамен: письменный, проводится по билетам;

7. Самостоятельная работа студентов (табл. 7).

Таблица 7

№ п/п	№ раздела дисциплины	Вид самостоятельной работы
1	**2**	**3**
1	1	Работа с литературой;
2	2	Работа с литературой;
3	3	Работа с литературой;
4	1-3	Подготовка к экзамену

8. Учебно-методическое и информационное обеспечение дисциплины:

8.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю):

1. Лагерев, В.В. Советы студентам по рациональной организации учебного труда: учеб. пособ. для вузов / В.В. Лагерев. – Брянск: БИТМ, 1992. – 92 с. [259 экз.].

2. Рабочая программа учебной дисциплины «Теория построения комплексных систем защиты информации» для направления подготовки кадров высшей квалификации 10.06.01 «Информационная безопасность», направленность программы «Методы и системы защиты информации, информационная безопасность». [Электронный ресурс каф. СИБ]

8.2. Перечень основной, дополнительной и справочной учебной литературы, необходимой для освоения дисциплины:

а) основная литература:

1) Аверченков, В.И. Аудит информационной безопасности: учеб. пособие/В.И. Аверченков. – Брянск: БГТУ, 2010 – 269 с.
2) Аверченков, В.И. Организационная защита информации: учеб. пособие/В.И. Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2010 – 184с.
3) Аверченков, В.И., Служба защиты информации: организация и управление: учеб. пособие / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2010 – 186с.
4) Аверченков, В.И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2010 – 225 с.
5) Аверченков В.И., Автоматизация проектирования комплексных систем защиты информации: монография / В.И. Аверченков, М.Ю. Рытов, О.М. Голоембиовская. – Брянск: БГТУ, 2012 – 143 с.
6) Аверченков, В.И. Разработка системы технической защиты информации/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – Брянск: БГТУ, 2009. – 187 с. – (Серия «Организация и технология защиты информации»)
7) Аверченков, В.И. Методы и средства инженерно-технической защиты информации / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – Брянск: БГТУ, 2009. – 187 с. – (Серия «Организация и технология защиты информации»)
8) Аверченков В.И. Защита персональных данных в организации: монография/ В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – Брянск: БГТУ, 2010. – 124 с. - (Серия «Организация и технология защиты информации»).
9) Аверченков В.И. Аудит информационной безопасности органов системы государственного и муниципального управления: монография / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2009. –126 с

б) дополнительная литература:

1) Аверченков В.И. Методы и средства инженерно-технической защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков [и др.]. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 187 с. — 5-89838-357-3. — Режим доступа: http://www.iprbookshop.ru/7000.html

2) Ли Р.И. Основы научных исследований [Электронный ресурс] : учебное пособие / Р.И. Ли. — Электрон. текстовые данные. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2013. — 190 с. — 978-5-88247-600-6. — Режим доступа: http://www.iprbookshop.ru/22903.html
3) Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс] : лабораторный практикум / В.П. Пашинцев, А.В. Ляхов. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 196 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63217.html
4) Петренко В.И. Теоретические основы защиты информации [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 222 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63138.html
5) Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

в) справочная литература:

1) ISO 15408 «Общие критерии оценки безопасности информационных технологий».
2) ISO/IEC 18028-1: 2006 «Информационные технологии. Методы обеспечения безопасности. Сетевая IT безопасность. Управление сетевой безопасностью».
3) ISO/IEC 18028-5: 2006«Информационные технологии. Методы обеспечения безопасности. Защита сетевых взаимодействий при помощи Виртуальных Частных Сетей».
4) ГОСТ 15408-02«Критерии оценки безопасности информационных технологий».
5) ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

8.3. Перечень ресурсов сети «Интернет», необходимых для изучения дисциплины:

- Электронная информационно-образовательная среда (ЭИОС) БГТУ:
- www.tu-bryansk.ru - официальный сайт БГТУ;
- edu.tu-bryansk.ru - система электронной поддержки учебных курсов на базе программного обеспечения Moodle со встроенной подсистемой тестирования;
- mark.lib.tu-bryansk.ru/marcweb2 - электронная библиотечная система БГТУ;
- lib.tu-bryansk.ru - сайт библиотеки БГТУ со ссылками на внешние ЭБС;

9. Материально-техническое обеспечение дисциплины.

Специальные помещения:

- помещение для проведения занятий лекционного типа, групповых и индивидуальных консультаций (ауд. Б.303);
- помещение для текущего контроля и промежуточной аттестации, в том числе итоговой аттестации (ауд. 210);
- помещение для самостоятельной работы, оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации (ауд. 224).

Перечисленные специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Перечень необходимого программного обеспечения:

Операционные системы и офисные пакеты (ОС WINDOWS, Linux, LibreOffice).

10. Методические рекомендации по организации изучения дисциплины.

10.1. Методические рекомендации для преподавателей.

При чтении лекций должна решаться задача доступного изложения всех материалов по данной дисциплине согласно рабочей программе.

Главной задачей каждой лекции и практического занятия является раскрытие тематики и увязка с практическим применением машин в производстве.

При чтении лекций и проведении практических занятий целесообразно использовать опорные конспекты (систему слайдов с наглядными изображениями и тезисами лекций).

10.2. Методические рекомендации для обучающихся.

Подготовку по дисциплине «Теория построения комплексных систем защиты информации» можно разбить на несколько этапов:

- работа с литературой;
- подготовка к экзамену.

При подготовке к экзамену необходимо возникающие вопросы задать преподавателю на консультациях.

11. Фонд оценочных средств

11.1. Этапы формирования компетенций

Этапы формирования компетенций (разделы дисциплины)	Показатель освоения (коды)								
	ПК-1			ПК-2			ПК-3		
	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3
Компоненты КСЗИ.	+	+	+				+	+	+
Модели, методы и методики Теория построения комплексных систем защиты информации	+	+	+	+	+	+	+	+	+
Концептуальный подход к разработке Теория построения комплексных систем защиты информации			+	+	+		+	+	+

11.2. Индексированные показатели и критерии оценивания результатов

Коды компетенций по ФГОС ВО	**Наименование компетенции**	**Показатель освоения**	**Оценочные средства текущего контроля**	**Оценочные средства промежуточного контроля**
Профессиональные компетенции				
ПК-1	Углубленное изучение теоретических и методологических основ проектирования, эксплуатации и развития систем защиты информации	**Р1 – знает**: современные программные, технические средства и информационные технологии, обеспечивающие безопасность информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: применять современные программные, технические средства и информационные технологии, обеспечивающие безопасность информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет: методами применения современных программных, технических средств и информационных технологий, обеспечивающих безопасность информации.	Устный опрос (вопросы к экзамену)	Вопросы к экзамену

ПК-2	Способность ставить и решать инновационные задачи, связанные с разработкой методов и технических средств, повышающих эффективность эксплуатации и проектирования средств защиты информации с использованием глубоких фундаментальных и специальных знаний, аналитических методов и сложных моделей в условиях неопределенности	**Р1 – знает**: методами применения современных программных, технических средств и информационных технологий, обеспечивающих безопасность информации.	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: определять и рассчитывать критерии эффективности функционирования комплексных систем защиты информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет: навыками разработки программных решений для моделирования и оптимизации комплексных систем защиты информации	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
ПК-3	Умение проводить анализ, самостоятельно ставить задачу исследования наиболее актуальных проблем, имеющих значение для защиты информации, грамотно планировать эксперимент и осуществлять его на практике	**Р1 – знает**: основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.	Устный опрос (вопросы к экзамену)	Вопросы к экзамену

11.3. Оценочные средства для промежуточной аттестации

Шкала оценивания

Уровень освоения обучающимся учебного материала определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Показатели и критерии оценивания сформированности компетенций

Оценку «отлично» заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, умение свободно выполнять задания, предусмотренные учебной программой, изучивший основную и знакомый с дополнительной литературой. Во время экзамена обучающийся должен подробно ответить на два теоретических вопроса билета.

Оценку «хорошо» заслуживает обучающийся, обнаруживший полное знание учебного материала, успешно выполнивший предусмотренные учебной программой задания, изучивший основную литературу. Во время экзамена обучающийся должен подробно ответить на один теоретический вопрос билета и частично на другой.

Оценку «удовлетворительно» заслуживает обучающийся, обнаруживший знание основного учебного материала в полном объеме, необходимом для дальнейшей учебы и работы по профессии, выполнивший предусмотренные учебной программой задания, знакомый с основной литературой. Во время экзамена обучающийся должен подробно ответить хотя бы на один теоретический вопрос билета или частично на оба вопроса.

Оценку «неудовлетворительно» заслуживает обучающийся, обнаруживший пробелы в знаниях основного учебного материала, допустивший принципиальные ошибки при выполнении предусмотренных программой заданий. Во время экзамена обучающийся частично отвечает на один вопрос билета.

Процедура промежуточной аттестации – письменный экзамен.

Контрольно-измерительные материалы промежуточной аттестации

Вопросы к экзамену по дисциплине

1. Понятие КЗСИ, понятие системы управления, виды систем управления;
2. Процесс управления, объекты управления.
3. Обобщённый алгоритм принятия решения, факторы, влияющие на организацию КЗСИ;
4. Взаимосвязь угроз и уязвимостей безопасности информации;
5. Моделирование КСЗИ, методы моделирования;
6. Специальные методы неформального моделирования, концептуальная модель защиты информации;
7. Прямая и обратная формулировка задачи защиты информации, понятие системного подхода к защите информации;
8. Системный подход к проектированию КСЗИ, принципы системного подхода;

9. Основные принципы построения систем защиты информации, этапы создания КЗСИ;

10. Моделирование угроз безопасности информации;

11. Функции систем защиты информации, функциональные требования КСЗИ;

12. Управление КСЗИ, особенности управления КСЗИ. процесс принятия решений при управлении КСЗИ;

12. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Изучение дисциплины инвалидами и лицами с ограниченными возможностями здоровья организуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При проведении учебных занятий обеспечивается соблюдение следующих требований:

– учебные занятия проводятся для инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся в ходе учебных занятий;

– присутствие ассистента из числа работников БГТУ или привлеченных лиц, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с педагогическим работником и т. п.);

– обучающиеся с учетом их индивидуальных особенностей могут пользоваться необходимыми им техническими средствами;

– материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже; наличие специальных кресел и других приспособлений).

Университетом созданы специальные условия для получения высшего образования обучающимися с ОВЗ:

1) для лиц с ограниченными возможностями здоровья по зрению:

– наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

– размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых по-

требностей) справочной информации о расписании учебных занятий (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

– присутствие ассистента, оказывающего обучающемуся необходимую помощь;

– обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

– обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию организации;

2) для лиц с ограниченными возможностями здоровья по слуху:

– дублирование звуковой справочной информации о расписании учебных занятий визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);

– обеспечение надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения Университета, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров; наличие специальных кресел и других приспособлений).

13. ВОСПИТАТЕЛЬНАЯ РАБОТА

В соответствии с Федеральным законом от 31.07.2020г. № 304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся» воспитание - «деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающихся на основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование у обучающихся чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению, взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации, природе и окружающей среде».

В учебном процессе воспитательная работа с обучающимися реализуется средствами учебных дисциплин.

Воспитательная деятельность в ходе преподавания дисциплины направленна на формирование у обучающегося системы убеждений, нравственных

норм и общекультурных качеств, на оказание им помощи в жизненном самоопределении, нравственном, гражданском и профессиональном становлении, на создание условий для самореализации личности. Воспитательная работа также ориентирует обучающихся на будущую профессиональную деятельность, формируя не только личностные, но и профессионально значимые качества.

Воспитательные задачи во время учебных занятий выполняются в скрытой (контекстной) и открытой (целенаправленной) формах. Скрытая форма воспитательной работы представляет собой воздействие всего хода педагогического процесса на становление личностных качеств обучающихся. Например, соблюдение педагогическим работником трудовой дисциплины, демонстрация преданности науке, заинтересованность в успехе обучающихся, правильная речь, хорошие манеры и т. п. имеют положительное воспитательное значение и формируют у обучающихся добросовестность, исполнительность, трудолюбие, ответственность и другие положительные качества. Обучающиеся неосознанно перенимают данные черты у педагогического работника.

Воспитание в открытой форме – это целенаправленное воздействие содержанием учебной дисциплины на становление личности обучающегося. Например, решение проблем и исследовательская работа формируют у обучающихся умение аргументировать, самостоятельно мыслить, вкус к научному поиску, развивают творчество, профессиональные умения, и т. п.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
Теория построения комплексных систем защиты информации

(наименование дисциплины)

10.06.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Методы и системы защиты информации, информационная безопасность

(направленность (профиль)/ специализация образовательной программы)

высшее образование – подготовка кадров высшей квалификации

(уровень образования)

Исследователь. Преподаватель-исследователь

(квалификация, присваиваемая по специальности или направлению подготовки)

Очная

(форма обучения)

2020

(год набора)

1. Цель освоения дисциплины.

Цель дисциплины: создание у обучающихся целостного представления о современных тенденциях в области исследования, модификации, разработки и проектирования комплексных систем защиты информации.

2. Место дисциплины в структуре ОПОП:

Дисциплина входит в обязательную часть образовательной программы и реализуется на 2 курсе в 4 семестре.

3. Компетенции, формируемые в результате освоения дисциплины

ПК-1 – способность применять в научных исследованиях теорию и методологию обеспечения информационной безопасности и защиты информации;

ПК-2 – готовность ставить и решать инновационные задачи, связанные с разработкой моделей, методов и технических средств, повышающих эффективность эксплуатации существующих и создания новых средств защиты информации и обеспечения информационной безопасности с использованием глубоких фундаментальных и специальных знаний, аналитических методов и сложных моделей в условиях неопределенности;

ПК-3 – умение проводить анализ, самостоятельно ставить задачу исследования рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.

4. Общая трудоемкость дисциплины

3 зачетные единицы (108 академических часа).

5. Форма (формы) промежуточной аттестации обучающихся

Экзамен.

6. Основные разделы дисциплины: 1) Компоненты КСЗИ; 2) Модели, методы и методики теории построения комплексных систем защиты информации; 3) Концептуальный подход к разработке теории построения комплексных систем защиты информации.

7. Автор(ы):
Рытов Михаил Юрьевич, доцент, к.т.н.