

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ворошилова Ольга Леонидовна

Должность: декан ФЛИМК

Дата подписания: 26.02.2021 13:32:03

Уникальный программный ключ:

abd894de8ff3e434f187dcddc5d14b3be82fda3f663e010c359e4ba6bb821c5e

Аннотация к рабочей программе

дисциплины «Информационная безопасность»

Цель преподавания дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ комплексной защиты информационно-коммуникационных систем на основе применения программно-аппаратных и коммуникационных технических средств, устройств и комплексов, нормативных и технических требований к системам, сетям и средствам защиты информации.

Задачи изучения дисциплины

- изучение классификации угроз информационной безопасности;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- ознакомление с симметричными и ассиметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно - программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение основных юридических законов в области защиты информации.

Компетенции, формируемые в результате освоения дисциплины

ОПК-7 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Разделы дисциплины

Основные понятия и анализ угроз информационной безопасности. Проблемы информационной безопасности сетей Политика безопасности. Криптографическая защита информации Технологии аутентификации. Технологии межсетевых экранов. Технологии защиты от вирусов. Требования к системам защиты информации. Основы правового обеспечения защиты информации

МИНОБРНАУКИ РОССИИ

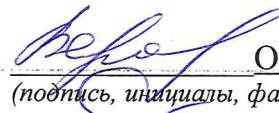
Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

Лингвистики и межкультурной
коммуникации

(наименование ф-та полностью)

 О.Л. Ворошилова
(подпись, инициалы, фамилия)

«31» 08 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

ОПОП ВО

45.03.03 Фундаментальная и прикладная лингвистика

(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Теоретическая и прикладная
лингвистика»

форма обучения

очная

(очная, очно-заочная, заочная)

Курск – 2020

Рабочая программа дисциплины Информационная безопасность составлена в соответствии с ФГОС ВО – бакалавриата по направлению подготовки 45.03.03 Фундаментальная и прикладная лингвистика на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета (протокол № 7 «25» февраля 2020 г.).

Рабочая программа дисциплины Информационная безопасность обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность «Теоретическая и прикладная лингвистика» на заседании кафедры информационной безопасности протокол № 1 «31» августа 2020 г.

Зав. кафедрой

Разработчик программы

к.в.н., доцент

Согласовано: на заседании кафедры теоретической и прикладной лингвистики, протокол № 1 «31» 08 2020 г.

Таныгин М.О.

Ханис А.Л.

Зав. кафедрой

Директор научной библиотеки

Степыкин Н.И.

Макаровская В.Г.

Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета протокол № 4 «25» 03 2019 г., на кафедры информационной безопасности протокол № 11 «28» 06 2021 г.

Зав. кафедрой

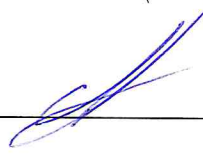
Рабочая программа дисциплины Информационная безопасность пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета протокол № 4 «25» 02 2020 г., на кафедры информационной безопасности протокол № 11 «30» 06 2022 г.

Зав. кафедрой

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность (профиль) «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета протокол № 9 от «25» 06 2022 г., на заседании кафедры ЧБ

(наименование кафедры, дата, номер протокола)

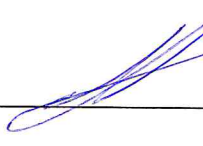
Зав. кафедрой

 Марухенникова А.П.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность (профиль) «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета протокол № 8 от «28» 02 2022 г., на заседании кафедры ЧБ

(наименование кафедры, дата, номер протокола)

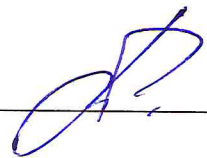
Зав. кафедрой

 Марухенникова А.П.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность (профиль) «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета протокол № 9 от «27» 02 2025 г., на заседании кафедры ЧБ № 11 от 24.06.2025

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

 Ташчикова М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 45.03.03 Фундаментальная и прикладная лингвистика, направленность (профиль) «Теоретическая и прикладная лингвистика», одобренного Ученым советом университета протокол № 9 от «27» 03 2024 г., на заседании кафедры ЧБ № 12 от 30.06.2026

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

 Ташчикова М.О.

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ комплексной защиты информационно-коммуникационных систем на основе применения программно-аппаратных и коммуникационных технических средств, устройств и комплексов, нормативных и технических требований к системам, сетям и средствам защиты информации.

1.2 Задачи дисциплины

- изучение классификации угроз информационной безопасности;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- ознакомление с симметричными и ассиметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно - программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение основных юридических законов в области защиты информации.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций
код компетенции	наименование компетенции		
ОПК-7	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-7.1 Работает с программными средствами и информационными ресурсами, необходимыми для решения профессиональных задач.	Знать: виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им. Уметь: правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры инфо-коммуникационных систем и сетевой защиты.
		ОПК-7.2 Учитывает требования информационной безопасности и условия их применения в профессиональной деятельности.	Знать: классификацию программно-аппаратных и телекоммуникационных средств, технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в области защиты информации. Уметь: проводить анализ защищенности вычислительной сети, настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков, определять оптимальный состав программных и аппаратных

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций
код компетенции	наименование компетенции		
			средств для построения инфо-коммуникационных сетей, применять действующие нормативные документы и юридические законы в области защиты информации. Владеть: навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфо-коммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации.
		ОПК -7.3 Решает профессиональные задачи, учитывая нормы библиографической и информационной культуры.	Знать: классификацию компьютерных вирусов, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, основные требования к системам защиты информации, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем, основные юридические законы в области защиты информации. Уметь: настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети, разрабатывать защищенные сайты с использованием языков HTML, JavaScript, PHP, проводить анализ информационных рисков. Владеть: навыками эксплуатации программных средств анализа и управления рисками, навыками разработки программ защиты данных, навыками разработки защищенных сайтов, разработки план-графиков разработки и установки программных средств защиты инфо-коммуникационных сетей.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Обязательная дисциплина «Информационная безопасность», входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы бакалавриата 45.03.03 Фундаментальная и прикладная лингвистика, направленность «Теоретическая и прикладная лингвистика». Дисциплина изучается на 3 курсе в 5 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 2 зачетные единицы (з.е.), 72 академических часов.

Таблица 3 - Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	36
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	
Самостоятельная работа обучающихся (всего)	35,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
-------	---------------------------	------------

	ны	
1	2	3
1	Основные понятия и анализ угроз информационной безопасности	Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности. Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.
2	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
3	Политика безопасности	Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети:
4	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные крипто-системы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.
5	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.

		Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
6	Технологии межсетевых экранов	
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.
---	--	--

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	2	-	-	У-1, У-2, У-3, У-4, У-5, У-7, МУ-1	УО - 2	ОПК-7
2	Проблемы информационной безопасности сетей	2	-	-	У-2, У-7, У-10, МУ-1	УО - 4	ОПК-7
3	Политика безопасности	2	1	-	У-1, У-3, У-5, У-7, МУ-1, МУ-2	УО, ЗЛР - 6	ОПК-7
4	Криптографическая защита информации	2	-	-	У-1, У-4, У-7, МУ-1, МУ-3	УО - 8 ЗЛР - 4,8	ОПК-7
5	Технологии аутентификации	2	2	-	У-4, У-6, У-7, У-10, МУ-1, МУ-3	УО, ЗЛР - 10	ОПК-7
6	Технологии межсетевых экранов	2	-	-	У-1, У-2, У-4, У-6, У-9, У-10, МУ-1	УО, ЗЛР - 12	ОПК-7
7	Технологии защиты от вирусов	2	-	-	У-2, У-4, У-8, У-9, У-	УО, ЗЛР - 14	ОПК-7

					10, МУ-1		
8	Требования к системам защиты информации	2	3,4,5	-	У-1-6, У-10, МУ-1, МУ-4, МУ-5, МУ-6,	УО – 16 ЗЛР – 12,14,16	ОПК-7
9	Основы правового обеспечения защиты информации	2	-	-	У-1-7, МУ-1	УО - 18	ОПК-7
	Всего	18	18	0			

УО – устный опрос, ЗЛР – лабораторная работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Разработка криптографической программы «Алгоритм RSA».	4
2	Эксплуатация антивирусной программы Kaspersky Internet Security	4
3	Разработка криптографической программы «Шифр Виженера».	4
4	Настройка межсетевого экрана в ОС Windows.	4
5	Шифрование с помощью программы TrueCrypt.	2
Итого		18

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и анализ угроз информационной безопасности	2 неделя	3,9
2	Проблемы информационной безопасности сетей	4 неделя	4
3	Политика безопасности	6 неделя	4
4	Криптографическая защита информации	8 неделя	4
5	Технологии аутентификации	10 неделя	4
6	Технологии межсетевых экранов	12 неделя	4
7	Технологии защиты от вирусов	14 неделя	4
8	Требования к системам защиты информации	16 неделя	4
9	Основы правового обеспечения защиты информации	18 неделя	4
Итого			35,9

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

- заданий для самостоятельной работы;

- вопросов и задач к зачёту;

- методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;

- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 - Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	Лекция №1. Основные понятия и анализ угроз информационной безопасности.	Анализ конкретных ситуаций	1
2	Лекция №2. Проблемы информационной безопасности сетей.	Анализ конкретных ситуаций	1
3	Лекция №3. Политика безопасности.	Анализ конкретных ситуаций	1
4	Лекция №8. Требования к системам защиты информации.	Анализ конкретных ситуаций	1
5	Лабораторное занятие №2. Эксплуатация антивирусной программы Kaspersky Internet Security.	Анализ конкретных ситуаций	1
6	Лабораторное занятие №3. Разработка криптографической программы «Шифр Виженера».	Анализ конкретных ситуаций	1
7	Лабораторное занятие №4. Настройка межсетевого экрана в ОС Windows.	Анализ конкретных ситуаций	1
8	Лабораторное занятие №5. Шифрование с помощью программы TrueCrypt.	Анализ конкретных ситуаций	1
Итого			8

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
ОПК-7. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Информационная безопасность		Производственная практика (научно-исследовательская работа) Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисциплиной)	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ОПК-7, основной.	ОПК-7.1 Работает с программными средствами и информационными ресурсами, необходимыми для решения профессиональных задач.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

	ОПК -7.2 Учитывает требования информационной безопасности и условия их применения в профессиональной деятельности.	Знать: нормативно-правовые акты и законодательства Российской Федерации, регулирующие вопросы защиты информации Уметь: Определять сферу действия документа Владеть навыками: Составление иерархической системы	Знать: основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации Уметь: определять какая цель в разборе документа Владеть навыками: Составление интеллектуальной карты	Знать: ответственность за нарушения в сфере информационной безопасности Уметь: определять статус документа по отношению к задаче Владеть навыками: квалифицировать нарушения в сфере информационной безопасности.
	ОПК -7.3 Решает профессиональные задачи, учитывая нормы библиографической и информационной культуры.	Знать: используемые в работе с ОС программные средства Уметь: использовать в работе с ОС программные средства разработки ПО и администрирования Владеть навыками: навыками работы с информационно-техническими средствами	Знать: инструментальные средства проведения проверок информационных систем Уметь: анализ кода программных СЗИ Владеть навыками: методы проектирования информационных систем с учетом требований информационной безопасности	Знать: основные угрозы работоспособности программным компонентам СЗИ Уметь: выявлять недекларируемые возможности программных систем Владеть навыками: использования особенностей реализации ПО для обеспечения ИБ

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,

характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	ОПК-7	Лекция, СРС	Вопросы для устного опроса	1-3	Согласно таблице 7.2
2	Проблемы информационной безопасности сетей	ОПК-7	Лекция, СРС	Вопросы для устного опроса	4-14	Согласно таблице 7.2
3	Политика безопасности	ОПК-7	Лекция, СРС, лабораторная работа №1	Вопросы для устного опроса КВЗЛР №1	15-17 1-4	Согласно таблице 7.2
4	Криптографическая защита информации	ОПК-7	Лекция, СРС	Вопросы для устного опроса	18-24 1 – 3	Согласно таблице 7.2
5	Технологии аутентификации	ОПК-7	Лекция, лабораторная работа №2, СРС	Вопросы для устного опроса КВЗЛР №2	25-30 1 - 4	Согласно таблице 7.2
6	Технологии межсетевых экранов	ОПК-7	Лекция, СРС	Вопросы для устного опроса	31-33	Согласно таблице 7.2
7	Технологии защиты от вирусов	ОПК-7	Лекция, СРС	Вопросы для устного опроса	34-41	Согласно таблице 7.2
8	Требования к системам защиты информации	ОПК-7	Лекция, лабораторные работы №3,4,5, СРС	Вопросы для устного опроса КВЗЛР №3 КВЗЛР №4 КВЗЛР №5	42-46 1-4 1-4 1-4	Согласно таблице 7.2

9	Основы правового обеспечения защиты информации	ОПК-7	Лекция, СРС	Вопросы для устного опроса	47-60	Согласно таблице 7.2

СРС – самостоятельная работа студента, КВЗЛР – контрольные вопросы для защиты лабораторных работ, КВЗПР - контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Основные понятия и анализ угроз информационной безопасности».

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности автоматизированных систем.
3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.

Контрольные вопросы для защиты практической работы №1:

Разработка криптографической программы «Шифр Виженера»

1. Квадрат (таблица) Виженера
2. Алфавитный шифр
3. Количество символов в строке для русского алфавита

Контрольные вопросы для защиты лабораторной работы №1

Анализ и управление информационными рисками в программе «Гриф»

1. Назначение системы Гриф
2. Модуль управления системы Гриф
3. Виды защищённости информации на ресурсе
4. Алгоритм задания контрмер

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

Промежуточная аттестация по дисциплине проводится в форме зачёта. Зачёт проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) — вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки знаний используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Какая угроза информационной безопасности является пассивной:
 - А) Копирование секретных данных.
 - Б) Внедрение вредоносного программного обеспечения.

В) Кража носителей информации.

Г) Удаление файла.

Задание в открытой форме:

1. Угрозы нарушения целостности информации приводят к
2. В автоматизированной системе перехват данных, передаваемых по каналам связи относится к уровню
3. Пассивной угрозой информационной безопасности является

Задание на установление правильной последовательности.

Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ
2. 30 Гбайт
3. 50 Килобайт
4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

способов и видов информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

Компетентностно-ориентированная задача:

Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- положение П 02.016–2018 О балльно - рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по темам 1-3	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 4-6	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 7-9	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Практическая работа № 1 «Эксплуатация антивирусной программы Kaspersky Internet Security»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 2 «Настройка межсетевого экрана Comodo Firewall»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 3 «Менеджер паролей – программа Password Commander»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%

Практическая работа № 4 «Анализ и управление информационными рисками в программе “Гриф”»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Практическая работа № 5 «Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №1 «Разработка криптографической программы «Алгоритм RSA»»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №2 «Разработка криптографической программы «Шифр Виженера»»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №3 «Настройка межсетевого экрана в ОС Windows»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4 «Шифрование с помощью программы True Crypt»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный.

Ч. 1. - 150 с. : ил., табл.

10. Спешаков А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спешаков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный.

Ч. 2. - 303 с. : ил., табл.

8.3 Перечень методических указаний

1. Методические указания по организации самостоятельной работы студентов [Электронный ресурс] : по дисциплине «Основы информационной безопасности» для студентов специальности 09.03.02 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с.

2. Разработка криптографических программ на языке Delphi [Электронный ресурс] : методические указания по выполнению лабораторных работ по дисциплинам «Информационная безопасность», «Методы и средства защиты компьютерной информации», «Защита информационных процессов в компьютерных системах» для студентов направлений подготовки бакалавров 230400.62, 230700.62, 010500.62, 231000.62, 090900.62 / ЮЗГУ ; сост.: К. А. Тезик, А. Л. Марухленко. - Курск : ЮЗГУ, 2015. - 50 с.

3. Антивирусная программа: Kaspersky Internet Security [Электронный ресурс] : методические указания по выполнению лабораторных и практических занятий для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00, 38.00.00 / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2018. - 14 с.

4. Программная реализация модели потокового шифратора [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, А. Л. Ханис. - Электрон. текстовые дан. (456 КБ). - Курск : ЮЗГУ, 2015. - 20 с.

5. Фаервол Comodo Firewall [Электронный ресурс] : методические указания по выполнению лабораторных и практических занятий по дисциплинам «Защита информационных процессов в компьютерных системах» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00, 38.00.00 / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2018. - 15 с.

6. Шифрование с помощью программы TrueCrypt [Электронный ресурс] : методические указания по выполнению лабораторных работ по дисциплинам «Методы и средства защиты компьютерной информации», для студентов направления подготовки бакалавров 09.03.04, «Информационная безопасность»

для студентов направлений подготовки бакалавров 09.03.02, 09.03.03, 45.03.03. /
Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2017. - 20 с.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт-Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.» - <http://window.edu.ru/>
3. Журнал «Проблемы информационной безопасности. Компьютерные системы» - <http://window.edu.ru/>
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

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

1. <http://e.lanbook.com> - Электронно-библиотечная система «Лань».
2. <http://www.iqlib.ru> - Электронно-библиотечная система IQLib.
3. <http://window.edu.ru> -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. <http://biblioclub.ru> – Электронно-библиотечная система «Университетская библиотека онлайн».
5. <http://www.fsb.ru> - Федеральная служба безопасности [официальный сайт].
6. <http://fstec.ru> - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. <http://microsoft.com> - Корпорация Microsoft [официальный сайт].
8. <http://www.consultant.ru> Компания «Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность» являются лекции, практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические и лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информационных процессов в компьютерных системах»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программа анализа и управления информационными рисками
“Триф”.(свободное ПО).

Программа хранения паролей Password Commander (свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFI LAN-guard Network Security Scanner.

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aoc 21". Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проектор inFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитывать задание, оформить ответ, общаться с преподавателем).

[illegible]