Аннотация к рабочей программе дисциплины «Защита информации»

Цель преподавания дисциплины

Дать студентам знания о принципах информационной безопасности и алгоритмах криптографической защиты информации.

Задачи изучения дисциплины

– ознакомление студентов с категориями информационной безопасности, с угрозами безопасности;

– ознакомление студентов с современными стандартами криптографической защиты информации, основанными на блочных и поточных алгоритмах шифрования;

– ознакомление студентов с алгоритмами аутентификации пользователей и алгоритмами электронной цифровой подписи;

– ознакомление студентов с принципами защиты информации от сетевых атак.

Индикаторы компетенций формируемые в результате освоения дисциплины

В результате освоения дисциплины студент формирует и демонстрирует следующие профессиональные компетенции:

– способен обеспечивать информационную безопасность (ПК-3), формулирует критерии безопасности обработки информации в автоматизированных системах (ПК-3.1), управляет функционированием программных средств защиты информации в компьютерных сетях (ПК-3.2), устанавливает программное обеспечение в соответствии с требованиями по защите информации (ПК-3.3).

Разделы дисциплины

Основные понятия информационной безопасности. Основные виды и источники атак на информацию, методы защиты информации. Категории информационной безопасности. Принципы криптографической защиты информации. Классификация шифров. Разновидности криптоаналитических атак.

Исторические шифры. Моноалфавитные подстановки. Полиалфавитные подстановки. Многопетлевые полиалфавитные подстановки. Перестановки.

Поточные шифры. Шифрование гаммированием. Методы генерации гаммы. Генераторы псевдослучайных последовательностей. Одноразовая система шифрования.

Блочные шифры. Построение блочных шифров. Сеть Фейстеля. Стандарт шифрования данных DES. Режимы применения блочных шифров. Способы усиления блочных шифров. Конечные поля. Стандарт шифрования данных AES.

Асимметричные криптосистемы. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Схема шифрования Эль Гамаля. Комбинированный метод шифрования.

Электронная цифровая подпись. Однонаправленные хеш-функции. Алгоритм хеширования SHA. Схемы хеширования на основе симметричных блочных алгоритмов. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля.

Управление криптографическими ключами. Генерация и хранение ключей. Распределение ключей. Протокол Kerberos. Инфраструктура открытого ключа (Public Key Infrastructure). Алгоритм распределения ключей Диффи-Хеллмана.

Защита компьютерных сетей. Разновидности сетевых атак. Межсетевые экраны. Системы обнаружения вторжений. Протокол SSL. Протокол IPSec. Сети VPN.

Администрирование сетей. Логическая структура Active Directory. Проектирование структуры. Физическая структура сети с Active Directory. Доверительные отношения в сетях Windows Server 2003. Управление учетными записями в сетях Windows Server 2003. Групповая политика в сетях Windows Server 2003 (GPO).

Безопасность операционных систем. Основные понятия. Разграничение доступа. Разрешения NTFS. Защита от вирусов.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
информатики.
(наименование ф-та полностью)

Т.А. Ширабакина
(подпись, инициалы, фамилия)

«29» 06 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации
(наименование дисциплины)

ОПОП ВО 09.03.01 Информатика и вычислительная техника,
шифр и наименование направления подготовки (специальности)

направленность (профиль, специализация) «Интеллектуальные системы в цифровой экономике»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника на основании учебного плана ОПОП ВО 09.03.01 Информатика и вычислительная техника, направленность «Интеллектуальные системы в цифровой экономике», одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 09.03.01 Информатика и вычислительная техника, направленность «Интеллектуальные системы в цифровой экономике» на заседании кафедры вычислительной техники №11 «18» 06 2021 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________ Титов В.С.

Разработчик программы
д.т.н., доцент ____________________ Егоров С.И.

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки ____________________ МакаровскаяВ.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.01 Информатика и вычислительная техника, направленность «Интеллектуальные системы в цифровой экономике», одобренного Ученым советом университета протокол №_«__»___20__г., на заседании кафедры____________________.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.01 Информатика и вычислительная техника, направленность «Интеллектуальные системы в цифровой экономике», одобренного Ученым советом университета протокол №_«__»___20__г., на заседании кафедры____________________.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.01 Информатика и вычислительная техника, направленность «Интеллектуальные системы в цифровой экономике», одобренного Ученым советом университета протокол №_«__»___20__г., на заседании кафедры____________________.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________

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

1.1 Цель преподавания дисциплины

Цель преподавания дисциплины – дать студентам знания о принципах информационной безопасности и алгоритмах криптографической защиты информации.

1.2 Задачи изучения дисциплины

К задачам изучения дисциплины относятся:

– ознакомление студентов с категориями информационной безопасности, с угрозами безопасности;

– ознакомление студентов с современными стандартами криптографической защиты информации, основанными на блочных и поточных алгоритмах шифрования;

– ознакомление студентов с алгоритмами аутентификации пользователей и алгоритмами электронной цифровой подписи;-

– ознакомление студентов с принципами защиты информации от сетевых атак.

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

Таблица 1.3 – Результаты обучения по дисциплине

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*		
ПК-3	Способен обеспечивать информационную безопасность	ПК-3.1 Формулирует критерии безопасности обработки информации в автоматизированных системах	Знать: основные угрозы информационной безопасности АИС, категории информационной безопасности, методы защиты информации в АИС, шифры DES, AES, RSA, принципы построения асимметричных криптосистем. Уметь: прогнозировать угрозы информационной безопасности АИС, применять одноразовую систему шифрования, применять поточные шифры. применять шифры DES, AES, RSA, использовать ЭЦП RSA, применять методы защиты информации. Владеть (или иметь опыт деятельности): навыками криптоанализа простых шифров,

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*		
			навыками применения шифра ГОСТ, методами усиления шифров.
		ПК-3.2 Управляет функционированием программных средств защиты информации в компьютерных сетях	Знать: методику настройки клиентов VPN, серверов VPN, и шлюзов VPN, организацию домена. Уметь: настраивать клиентов VPN, вводить в домен пользователей и компьютеры. Владеть (или иметь опыт деятельности): навыками настройки фильтрующих маршрутизаторов, навыками настройки шлюзов сетевого уровня, навыками настройки шлюзов прикладного уровня. навыками настройками Active Directory.
		ПК-3.3 Устанавливает программное обеспечение в соответствии с требованиями по защите информации	Знать: политики безопасности (GPO). разрешения NTFS. Уметь: настраивать политики безопасности, назначать разрешения NTFS на файлы и каталоги. Владеть (или иметь опыт деятельности): навыками планирования политик безопасности, навыками безопасного хранения данных на дисках.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита информации» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность «Интеллектуальные системы в цифровой экономике». Дисциплина изучается на 4 курсе в 7 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 4 зачетных единиц (з.е.), 144 часа.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	55,15
в том числе:	
лекции	36
лабораторные занятия	18, из них практическая подготовка – 12
практические занятия	0
Самостоятельная работа обучающихся (всего)	61,85
Контроль/экз (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1.15

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)

№	Раздел (тема) дисциплины	Содержание
1	Основные понятия информационной безопасности.	Основные виды и источники атак на информацию, методы защиты информации. Категории информационной безопасности. Принципы криптографической защиты информации. Классификация шифров. Разновидности криптоаналитических атак.
2	Исторические шифры.	Моноалфавитные подстановки. Полиалфавитные подстановки. Многопетлевые полиалфавитные подстановки. Перестановки.
3	Поточные шифры.	Шифрование гаммированием. Методы генерации гаммы. Генераторы псевдослучайных последовательностей. Одноразовая система шифрования.
4	Блочные шифры.	Построение блочных шифров. Сеть Фейстеля. Стандарт шифрования данных DES. Режимы применения блочных шифров. Способы усиления блочных шифров. Конечные поля. Стандарт шифрования данных AES.
5	Асимметричные криптосистемы.	Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Схема шифрования Эль Гамаля. Комбинированный метод шифрования.
6	Электронная цифровая подпись.	Однонаправленные хеш-функции. Алгоритм хеширования SHA. Схемы хеширования на основе симметрич-

		ных блочных алгоритмов. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля.
7	Управление криптографическими ключами.	Генерация и хранение ключей. Распределение ключей. Протокол Kerberos. Инфраструктура открытого ключа (Public Key Infrastructure). Алгоритм распределения ключей Диффи-Хеллмана.
8	Защита компьютерных сетей.	Разновидности сетевых атак. Межсетевые экраны. Системы обнаружения вторжений. Протокол SSL (Secire Socket Layer). Протокол IPSec. Сети VPN.
9	Администрирование сетей.	Логическая структура Active Directory. Проектирование структуры. Физическая структура сети с Active Directory. Доверительные отношения в сетях Windows Server 2003. Управление учетными записями в сетях Windows Server 2003. Групповая политика в сетях Windows Server 2003 (GPO).
10	Безопасность операционных систем.	Основные понятия. Разграничение доступа. Разрешения NTFS. Защита от вирусов.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел, (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости	Компетенции
		лек	лаб	пр.			
1	2	3	4	5	6	7	8
1.	Основные понятия информационной безопасности.	2			У1,У4, МУ6, МУ7	С(3)	ПК-3.1
2.	Исторические шифры.	2	1		У3,У4, МУ1	ЗЛР(3) С(3)	ПК-3.1
3.	Поточные шифры.	2	2		У1, У2, МУ2	ЗЛР(6) С(6)	ПК-3.1
4.	Блочные шифры.	6	3		У1, У4, МУ3	ЗЛР(9) С(9)	ПК-3.1
5.	Асимметричные криптосистемы.	4			У1, У4, МУ6, МУ7	С(9)	ПК-3.1
6.	Электронная цифровая подпись.	2			У1, У4, МУ6, МУ7	С(13)	ПК-3.1

7.	Управление криптографическими ключами.	6			У4, У5, МУ6, МУ7	С(16)	ПК-3.2
8.	Защита компьютерных сетей.	6	4		У2,У4, МУ4	ЗЛР(12) С(12)	ПК-3.2
9.	Администрирование сетей.	4	5		У2,МУ5	ЗЛР(15) С(15)	ПК-3.3
10.	Безопасность операционных систем.	2	5		У2, МУ5	ЗЛР(18) С(18)	ПК-3.3
	Итого	36					

Примечание:
У – учебное пособие, учебник;
МУ – методические указания;
С – собеседование;
ЗЛР – защита лабораторных работ;

4.2 Лабораторные и (или) практические занятия

Таблица 4.2.1 Лабораторные работы

№ п/п	Наименование лабораторной работы	Объем, час.
1.	Шифрование методом прямой замены	4, из них практическая подготовка – 2
2.	Шифрование методом полиалфавитной замены	4, из них практическая подготовка – 2
3.	Шифрование методом перестановок	2
4.	Сеть VPN.	4, из них практическая подготовка – 4
5.	Active Directory.	4, из них практическая подготовка – 4
Итого:		18, из них практическая подготовка – 12

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 Самостоятельная работа студентов (СРС)

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	Основные понятия информационной безопасности.	1-3	10
2	Асимметричные криптосистемы.	4-9	10
3	Алгоритмы электронной цифровой подписи.	10-13	10

4	Управление криптографическими ключами.	14-16	10
6	Подготовка к лабораторным работам	в течение семестра	21,85
Итого:			61,85

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 УП и 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;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:
  – методических указаний по выполнению самостоятельной работы [6,7];
  – вопросов для собеседований и экзамена;
  – методических указаний к выполнению лабораторных 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. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами по защите информации.

Расчетный удельный вес занятий, проводимых в интерактивной форме не менее 12 часов.

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

№ п/п	Наименование раздела (лекции и лабораторные занятия)	Используемые интерактивные образовательные технологии	Обьем в часах
1	2	3	4
1.	Диалог о проблемах и перспективах защиты информации (ЛК)	Диалог с аудиторией	1
2.	Блочные шифры. (ЛК)	Диалог с аудиторией	1
3.	Асимметричные криптосистемы. (ЛК)	Диалог с аудиторией	1
4.	Электронная цифровая подпись. (ЛК)	Диалог с аудиторией	1
5.	Управление криптографическими	Диалог с аудиторией	1

	ключами. (ЛК)		
6.	Защита компьютерных сетей. (ЛК)	Диалог с аудиторией	1
7.	Администрирование сетей. (ЛК)	Диалог с аудиторией	1
8.	Безопасность операционных систем (ЛК).	Диалог с аудиторией	1
9.	Моноалфавитные шифры (ЛЗ)	Разбор ситуации	1
10.	Полиалфавитные шифры (ЛЗ)	Разбор ситуации	1
11.	Работа с сетевым монитором (ЛЗ)	Разбор ситуации	1
12.	Установка и настройка Active Directory. (ЛЗ)	Разбор ситуации	1
	Итого	В часах	12

Примечание:

ЛК-лекция;

ЛЗ- лабораторное занятие.

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности «Интеллектуальные системы в цифровой экономике», программы бакалавриата 09.03.01 Информатика и вычислительная техника.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях (оборудованных в подразделениях университета).

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован исторический и научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование профессиональной культуры обучающихся. Содержание дисциплины способствует правовому и профессионально-трудовому воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал содержания, демонстрирующего обучающимся образцы высокого профессионализма ученых, их ответственности за результаты и последствия деятельности для природы, человека и общества;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7 Фонд оценочных тестов для проведения промежуточной аттестации.

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

Таблица 7 1 Этапы формирования компетенции

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	Начальный	Основной	Завершающий
1	2	3	4
ПК-3 Способен обеспечивать информационную безопасность	Учебная ознакомительная практика	Операционные системы, Базы данных, Сети и телекоммуникации	Защита информации, Выполнение 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 и критерии определения уровня сформированности компетенций (частей 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 уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-3/ завершающий	ПК-3.1 Формулирует критерии безопасности обработки информации в автоматизированных системах ПК-3.2 Управляет функционированием программных средств защиты информации в компьютерных сетях ПК-3.3 Устанавливает программное обеспечение в соответствии с требованиями по защите информации	Знать: основные угрозы информационной безопасности АИС, разрешения NTFS, основные поточные шифры, принципы построения асимметричных криптосистем, методику настройки клиентов VPN. Уметь: прогнозировать угрозы информационной безопасности АИС, назначать разрешения NTFS на файлы и каталоги. применять поточные шифры. настраивать клиентов VPN, назначать разрешения NTFS на файлы и каталоги.	Знать: дополнительно к пороговому уровню методы защиты информации в АИС, шифр DES, методику настройки серверов VPN, политики безопасности (GPO). Уметь: дополнительно к пороговому уровню применять методы защиты информации, применять шифр DES, использовать ЭЦП RSA, настраивать серверы VPN, настраивать политики безопасности.	Знать: дополнительно к продвинутому уровню категории информационной безопасности, шифр AES, методику настройки шлюзов VPN, организацию домена. Уметь: дополнительно к продвинутому уровню применять одноразовую систему шифрования, применять шифр AES, настраивать шлюзы VPN, вводить в домен пользователей и компьютеры.

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 уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		Владеть (или иметь опыт деятельности): навыками криптоанализа шифров – моноалфавитных подстановок, навыками применения шифра ГОСТ, навыками настройки фильтрующих маршрутизаторов, навыками безопасного хранения данных на дисках.	Владеть (или иметь опыт деятельности): дополнительно к пороговому уровню навыками криптоанализа шифров – полиалфавитных подстановок, методами усиления шифра DES, навыками настройки шлюзов сетевого уровня, навыками планирования политик безопасности.	Владеть (или иметь опыт деятельности): дополнительно к продвинутому уровню навыками криптоанализа шифров – перестановок, методами усиления шифра AES, навыками применения криптосистемы Эль-Гамаля, навыками настройки шлюзов прикладного уровня, навыками настройками Active Directory.

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 информационной безопасности.	ПК-3.1	Лекция, СРС	вопросы для собеседования	1 - 8	Согласно табл.7.2.
2	Исторические шифры.	ПК-3.1	Лекция, СРС, лабораторная работа	Задания и контрольные вопросы к лаб. №1, в т.ч. для контроля результатов практической подготовки	1 – 30, 1 - 5	Согласно табл.7.2.

				вопросы для собеседования	1 - 8	
3	Поточные шифры.	ПК-3.1	Лекция, СРС, лабораторная работа	Задания и контрольные вопросы к лаб. №2, в т.ч. для контроля результатов практической подготовки	1 – 20, 1 - 6	Согласно табл.7.2.
				вопросы для собеседования	1 - 4	
4	Блочные шифры.	ПК-3.1	Лекция, СРС, лабораторная работа	Задания и контрольные вопросы к лаб. №3	1 – 15, 1 - 4	Согласно табл.7.2.
				вопросы для собеседования	1 - 12	
5	Асимметричные криптосистемы.	ПК-3.1	Лекция, СРС	вопросы для собеседования	1 - 5	Согласно табл.7.2.
6	Электронная цифровая подпись.	ПК-3.1	Лекция, СРС	вопросы для собеседования	1 - 5	Согласно табл.7.2.
7	Управление криптографическими ключами.	ПК-3.2	Лекция, СРС	вопросы для собеседования	1 - 7	Согласно табл.7.2.
8	Защита компьютерных сетей.	ПК-3.2	Лекция, СРС, лабораторная работа	Задания и контрольные вопросы к лаб. №4, в т.ч. для контроля результатов практической подготовки		Согласно табл.7.2.
				вопросы для собеседования	1 - 14	
9	Администрирование сетей.	ПК-3.3	Лекция, СРС, лабораторная работа	Задания и контрольные вопросы к лаб. №5, в т.ч. для контроля результатов практической подготовки	часть 1: 1 – 3, 1 - 8 часть 2: 1 – 5, 1 - 14	Согласно табл.7.2.
				вопросы для собеседования	1 - 6	
10	Безопасность опера-	ПК-3.3	Лекция,	Задания и	часть 3:	Согласно

	ционных систем.		СРС, лабораторная работа	контрольные вопросы к лаб. №5, в т.ч. для контроля результатов практической подготовки	1 – 9, 1 - 6	табл.7.2.
				вопросы для собеседования	1 - 4	

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования по разделу (теме) 1. «Основные понятия информационной безопасности»

1. Основные виды и источники атак на информацию.
2. Методы защиты информации.
3. Политики безопасности.
4. Категории информационной безопасности.
5. Понятие криптографии.
6. Криптоанализ.
7. Классификация методов шифрования информации.
8. Разновидности криптоаналитических атак.

Производственная задача для контроля результатов практической подготовки обучающихся в лабораторной работе № 4:

Установите сервер виртуальной частной сети (VPN).

Производственная задача для контроля результатов практической подготовки обучающихся в лабораторной работе № 5:

Включите рабочую станцию в домен.

Оценивание компетенций, формируемых в ходе выполнения и защиты лабораторных работ в виде балльной оценки, осуществляется в соответствии с таблицами 7.4.

Оценка знаний на экзамене осуществляется путем ответов на вопросы билета

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме тестирования (бланкового и/или компьютерного).

Для тестирования используются контрольно-измерительные материалы (КИМ) – 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.

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 и компетенции проверяются с помощью 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.

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 контроль изучения дисциплины

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
ЛР №1 Шифры - моноалфавитные подстановки.	3	Выполнил, но не защитил	6	Выполнил и защитил
ЛР №2 Шифры - полиалфавитные подстановки.	3	Выполнил, но не защитил	6	Выполнил и защитил
ЛР №3 Блочные шифры - перестановки.	3	Выполнил, но не защитил	6	Выполнил и защитил
ЛР №4 Сетевой анализатор. Сети VPN.	3	Выполнил, но не защитил	6	Выполнил и защитил
ЛР №5 Active Directory.	4	Выполнил, но не защитил	8	Выполнил и защитил
Самостоятельная работа	8	По итогам собеседований	16	По итогам собеседований
Посещаемость	0		16	
Экзамен	0	Не ответил ни на один вопрос	36	Ответил на все вопросы
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.

Максимальное количество баллов за тестирование –36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. - Режим доступа - http://biblioclub.ru/index.php?page=book&id=429070

2. Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. - Режим доступа - http://biblioclub.ru/index.php?page=book&id=208567

8.2 Дополнительная учебная литература

3. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях : [Текст] / М.А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2001. – 368 с.

4. Романец, Ю.В. Защита информации в компьютерных системах и сетях : [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

5. Фергюсон, Н. Прикладная криптография [Текст] / Н. Фергюсон, Б. Шнайер - М.: Вильямс, 2005. - 424 с.

8.3 Перечень методических указаний

1. Шифрование методом прямой замены :[Электронный ресурс] : методические указания к лабораторной работе для студентов направлений подготовки 09.03.01 / сост. М. А. Ефремов, С. И. Егоров. – Курск : ЮЗГУ, 2019. - 14 с.

2. Шифрование методом полиалфавитной замены :[Электронный ресурс] : методические указания к лабораторной работе для студентов направлений подготовки 09.03.01 / сост. М. А. Ефремов, С. И. Егоров. – Курск : ЮЗГУ, 2019. - 9 с.

3. Шифрование методом перестановок: [Электронный ресурс] : методические указания по к лабораторной работе для студентов направлений подготовки 09.03.01 / сост. М. А. Ефремов, С. И. Егоров. – Курск : ЮЗГУ, 2019. - 9 с.

4. Сеть VPN : [Электронный ресурс] : методические указания к лабораторной работе для студентов направлений подготовки 09.03.01 / сост. С.И.Егоров. - Курск : ЮЗГУ, 2017. - 9 с.

5. Active Directory : [Электронный ресурс] : методические указания к лабораторной работе для студентов направлений подготовки 09.03.01 / сост. С. И. Егоров. – Курск : ЮЗГУ, 2017. - 15 с.

6. Защита информации : [Электронный ресурс] : методические указания по выполнению самостоятельной работы /Юго-Зап. гос. ун-т; сост.: С. И. Егоров. – Курск : ЮЗГУ, 2017. -14 с.

7. Организация самостоятельной работы студентов : [Электронный ресурс] : методические указания для студентов направлений подготовки 09.03.01 и 09.04.01 «Информатика и вычислительная техника» / Юго-Зап. гос. ун-т; сост.: В. С. Титов, И. Е. Чернецкая, Т. А. Ширабакина. - Курск : ЮЗГУ, 2017. - 39 с.

8.4 Другие учебно-методические материалы.

Отраслевые научно-технические журналы в библиотеке университета:

- Телекоммуникации;
- Сети и системы связи.

Словарь-справочник по информационной безопасности для парламентской ассамблеи ОДКБ / под общей ред. М.А. Вуса и М.М. Кучерявого – СПб.: СПИИРАН. Изд-во «Анатолия». «Полиграфические технологии», 2014. – 96 с.

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

1. http://citforum.ru/security/ - Учебные пособия и обзоры по защите информации.
2. Сайт – справочник по сетям http://www.netfaq.ru/net_faq.

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Защита информации» являются лекции 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 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.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

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

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информации»: 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 лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы 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 закрепление освоенного материала является конспектирование, без которого немыслима 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 «Защита информации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Защита информации» - 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)

1. ОС Windows 7 (https://www.microsoft.com, договор IT 000012385).
2. Пакет прикладных программ OpenOffice (http://www.openoffice.org, бесплатная, GNU General Public License).
3. Oracle VM VirtualBox (https://www.virtualbox.org, бесплатная версия, GNU General Public License version 2);
4. Windows Server 2008 (https://www.microsoft.com, договор IT 000012385).

5. 12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

6.
7. Стандартно оборудованные лекционные аудитории и аудитории для проведения занятий семинарского типа.
8. Компьютерный класс оснащенный
9. ПК ВаРИАНт PD2160/I C33/2*512 Mb/HDD 160Gb/DVD-ROM/FDD/ATX 350W/Km/WXP/DFF/17’TFTE 700
10. или
11. Интерактивная панель Интерактивная панель JeminiCo. JQ75MW с ОПС модулем и мобильной стойкой; Компьютер в сборе (ТИП-2)
12. или
13. Рабочая станция Core 2 Duo 1863/2*DDR2 1024 Mb/2*HDD 200G/SVGA/DVD-RW/20’LCD*2/Secret Net; ПЭВМ INTEL Gore i3-7100/H110M-R C/SI White Box LGA1151.mATX/8GB/1TB/DVDRW/LCD 21.5”/k+m/
14. в зависимости от предоставленной аудитории.

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. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). 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, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изме-нения	Номера страниц				Всего страниц	Дата	Основание для изменения и под-пись лица, прово-дившего изменения
	изме-ненных	замененных	аннулированных	новых			
1		17-18			2	01.07.23	Протокол №13 от 01.09.2023