

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Емельянов Сергей Геннадьевич
Должность: ректор
Дата подписания: 17.10.2024 12:49:07
Уникальный программный ключ:
9ba7d3e34c012eba476ffd2d064cf2781953be730df2374d16f3c0ce536f0fc6

МИНОБРАЗОВАНИЯ И НАУКИ РОССИИ

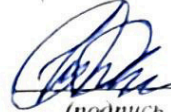
Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

экономики и менеджмента

(наименование ф-та полностью)



Т.Ю. Ткачёва

(подпись, инициалы, фамилия)

« 21 » 06 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

(наименование дисциплины)

ОПОП ВО

38.03.03 «Управление персоналом»

шифр и наименование направления подготовки (специальности)

направленность (профиль, специализация) «Управление персоналом организации»

наименование направленности (профиля, специализации)

форма обучения

очно-заочная

(очная, очно-заочная, заочная)

Курск – 2024

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

1.1 Цель дисциплины

Дисциплина «Защита информации» изучается с целью ознакомления студентов с основами теории защиты информационных систем, правовым регулированием в области защиты информации, принципами организации аппаратно-программных способов защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности для использования полученных знаний в дальнейшем образовательном процессе на старших курсах.

1.2 Задачи дисциплины

- ознакомить студентов с основами правового регулирования в области защиты информации;
- ознакомить студентов с основными положениями теории безопасности информационных систем;
- обучить принципам организации аппаратно-программных способов защиты информации;
- научить студентов универсальным методами защиты информации и условиями их применения.

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

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
ОПК-5	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	ОПК-5.1 Использует информационно-коммуникационные технологии при поиске необходимой информации.	Знать: способы сбора, анализа и обработки данных, нормативных и методических материалов для анализа внутренних и внешних факторов, влияющих на эффективность деятельности персонала организации. Уметь: анализировать научно-техническую информацию для решения возникающих профессиональных задач с учетом информационной безопасности. Владеть: навыками осуществлять сбор, анализ и обработку данных научно-технической информации, нормативных и методических материалов, необходимых для анализа внутренних и внешних факторов, влияющих на эффективность деятельности персонала организации с учетом требований обеспечения информационной безопасности.
		ОПК-5.2 Решает стандартные задачи профессиональной деятельности с использованием информационных технологий и программных средств.	Знать: полный перечень требуемой информации для ведения кадрового делопроизводства и организации архивного хранения кадровых документов; знать основы кадровой документацией и действующие локальные нормативно-правовые акты. Уметь: вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами; обеспечить защиту персональных данных сотрудников. Владеть: навыками обеспечить защиту персональных данных сотрудников с учетом составления кадровой отчетности и действующими нормативно-правовыми актами по информационной безопасности.

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		ОПК-5.3 Выбирает современные информационные технологии и прикладные программные средства для решения поставленных задач.	Знать: способы сбора, анализа и обработки данных, нормативных и методических материалов для анализа внутренних и внешних факторов, влияющих на эффективность деятельности персонала организации. Уметь: анализировать научно-техническую информацию для решения возникающих профессиональных задач с учетом информационной безопасности. Владеть: навыками осуществлять сбор, анализ и обработку данных научно-технической информации, нормативных и методических материалов, необходимых для анализа внутренних и внешних факторов, влияющих на эффективность деятельности персонала организации с учетом требований обеспечения информационной безопасности.
ОПК-6	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-6.1 Ориентируется в современных информационных технологиях.	Знать: способы сбора, анализа и обработки данных научно-технической информации, нормативных и методических материалов для решения различного рода профессиональных задач и иных форм профессионального развития персонала. Уметь: анализировать научно-техническую информацию для решения возникающих профессиональных задач. Владеть: навыками осуществлять сбор, анализ и обработку данных научно-технической информации, нормативных и методических материалов, необходимых для решения профессиональных задач и иных форм профессионального развития персонала с учетом требований обеспечения информационной безопасности.

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		ОПК-6.2 Использует в повседневной практике современные информационнокоммуникационные технологии и программные средства.	Знать: основные требования информационной безопасности для работы с корпоративными коммуникационными каналами и средствами передачи информации. Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств с учетом основных требований информационной безопасности. Владеть: навыками информационного обеспечения процессов внутренних коммуникаций для решения задач профессиональной деятельности с учетом основных требований информационной безопасности.
		ОПК-6.3 Применяет современные информационные технологии и программные средства для решения задач профессиональной деятельности.	Знать: основные требования информационной безопасности; принципы работы программных, программно – аппаратных средств и технических средств обработки деловой информации с учетом основных требований информационной безопасности. Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств обработки деловой информации. Владеть: методами и программными средствами обработки деловой информации; навыками взаимодействовать со службами информационных технологий; навыками эффективно использовать корпоративные информационные системы при решении задач управления персоналом с учетом основных требований информационной безопасности.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита информации» (Б1.О.16), входит в обязательную часть цикла подготовки бакалавров. формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы бакалавриата 38.03.03 «Управление персоналом», направленность «Управление персоналом». Изучается на 2 курсе в 4 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 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3 –Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	16,1
в том числе:	
лекции	8
лабораторные занятия	0
практические занятия	8
Самостоятельная работа обучающихся (всего)	87,9
Контроль/зачет (подготовка к зачету)	4
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрена
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрена

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
1	2	3
1	Защита информации. Основные понятия и определения.	Предмет и объект защиты. Свойства информации. Сложность объективной оценки количества информации. Информация с ограниченным доступом, ее характеристики. Система защиты информации в КС.
2	Угрозы безопасности информации в компьютерных системах.	Классификация информационных угроз. Случайные и преднамеренные угрозы. Несанкционированный доступ к информации. Несанкционированная модификация структур. Вредительские программы. Классификация злоумышленников.
3	Комплексная защита информации и правовое регулирование информационной безопасности.	Универсальные подходы к решению проблемы информационной безопасности. Вопросы информационной безопасности в «Концепции национальной безопасности Российской Федерации». Основные законы РФ в области защиты информации. Лицензирование и сертификация в области защиты информации. Организационные методы защиты информации.
4	Защита информации от случайных угроз.	Дублирование информации. Повышение надежности компьютерных систем. Создание отказоустойчивых компьютерных систем. Оптимизация взаимодействия человека и системы. Блокировка ошибочных операций.
5	Методы и средства защиты информации от традиционного шпионажа и диверсий.	Система охраны объекта КС. Инженерные конструкции. Разновидности датчиков сигнализации. Средства видеоконтроля. Подсистемы доступа на объект. Идентификация, аутентификация и парольная защита.
6	Средства защиты информации от утечки по виброакустическому и электромагнитному каналам.	Средства радио контроля помещений. Средства поиска закладок. Средства подавления закладных устройств. Защита от злоумышленных действий обслуживающего персонала и пользователей. Пассивные методы защиты от побочных электромагнитных излучений и наводок. Экранирование. Активные методы защиты от ПЭМИН.
7	Методы защиты информации от несанкционированного изменения структуры компьютерной системы.	Требования к защищенности систем от несанкционированного изменения структуры (НИС). Основные принципы разработки аппаратно-программных средств, учитывающие защиту от НИС. Защита от закладок при разработке программ. Защита от НИС в процессе эксплуатации системы. Разграничение доступа к оборудованию.
8	Защита информации в компьютерных системах от несанкционированного доступа.	Система разграничения доступа к информации в компьютерных системах. Дискреционное и мандатное управление доступом. Состав системы разграничения доступом. Система защиты программных средств от копирования и исследования.
9	Криптографические методы защиты информации.	Основные виды криптографического преобразования информации. Шифрование, стеганография, кодирование, сжатие. Шифрование с симметричным ключом. Шифрование с открытым ключом.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности		Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		лек., час	№ пр			
1	2	3	4	5	6	7
1	Защита информации. Основные понятия и определения.	2	1	О-1,2 Д-1-4 МУ-1	С, КО2	ОПК-5
2	Угрозы безопасности информации в компьютерных системах.	2	2	О-1,2 Д-4, 8	С4	ОПК-5
3	Комплексная защита информации и правовое регулирование информационной безопасности.	2	2	О-1,2 Д-5,8 МУ-2	С, КО6	ОПК-6
4	Защита информации от случайных угроз.	2	2	О-1,2 Д-4,6-8	Р8	ОПК-5
5	Методы и средства защиты информации от традиционного шпионажа и диверсий.	2	3	О-1,2 Д-4,8 МУ-3	С, КО10	ОПК-5
6	Средства защиты информации от утечки по виброакустическому и электромагнитному каналам.	2	2	О-2 Д-7,8	Р12	ОПК-5, ОПК-6
7	Методы защиты информации от несанкционированного изменения структуры компьютерной системы.	2	2	О-1,2 Д-6,8 МУ-4	С, КО14	ОПК-5, ОПК-6
8	Защита информации в компьютерных системах от несанкционированного доступа.	2	2	О-1,2 Д-2,4 МУ-5	С, КО16	ОПК-6
9	Криптографические методы защиты информации.	2	3	О-1,2 Д-3-8 МУ-6	С, КО18	ОПК-5, ОПК-6

С – собеседование, КО – контрольный опрос, Р – реферат.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Шифрование методом простой замены	1
2	Шифрование методом полиалфавитной замены	1
3	Шифрование методом перестановок (маршруты Гамильтона)	1
4	Схема Шамира разделения секрета	2
5	Шифрование аналитическими методами (методами матричной алгебры)	1
6	Системы с открытым ключом. Алгоритм RSA.	2
Итого		8

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Защита информации. Основные понятия и определения.	2 неделя	10
2.	Угрозы безопасности информации в компьютерных системах.	4 неделя	10
3.	Комплексная защита информации и правовое регулирование информационной безопасности.	6 неделя	10
4.	Защита информации от случайных угроз.	8 неделя	10
5.	Методы и средства защиты информации от традиционного шпионажа и диверсий.	10 неделя	10
6.	Средства защиты информации от утечки по виброакустическому и электромагнитному каналам.	12 неделя	10
7.	Методы защиты информации от несанкционированного изменения структуры компьютерной системы.	14 неделя	10
8.	Защита информации в компьютерных системах от несанкционированного доступа.	16 неделя	10
9.	Криптографические методы защиты информации.	18 неделя	7,9
Итого			87,9

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 ме-

тодическими 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 рекомендаций, пособий по организации самостоятельной работы аспирантов;

- заданий для самостоятельной работы;

- тем рефератов и докладов;

- вопросов к экзаменам и зачетам;

- 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 универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета по труду и занятости населения Курской области.

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1.	Лекция «Конфиденциальная информация и ее защита»	Разбор конкретных ситуаций по классификации конфиденциальной информации и способах ее защиты	0,5

2.	Выполнение лабораторной работы «Схема Шамира разделения секрета»	Выполнение студентами интерактивных заданий по реализации схем разделения секрета	0,3
3.	Лекция «Криптографические методы защиты информации»	Разбор конкретных ситуаций по применимости криптографических методов защиты информации в зависимости от типа информационных систем	0,5
4.	Выполнение лабораторной работы «Системы с открытым ключом. Алгоритм RSA»	Выполнение студентами интерактивных заданий по реализации систем с открытым ключом	0,3
5.	Лекция «Угроза безопасности информации АСОД и субъектов информационных отношений»	Разбор конкретных ситуаций по классификации угроз безопасности информации АСОД и субъектов информационных отношений, и способах их защиты	0,4
Итого			2

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

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении / прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5)	Введение в направление подготовки Культура речи и деловое общение Экономическая информатика Информационные технологии в управлении персоналом Защита информации Информационная безопасность Практика по получению первичных профессиональных умений и навыков	Логистика Управление запасами Практика по получению профессиональных умений и опыта профессиональной деятельности	Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6)	Статистика Защита информации Информационная безопасность	Документационное обеспечение управления персоналом Практика по получению профессиональных умений и опыта профессиональной деятельности	Управленческий учет и учет персонала Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
---	--	---	--

*Этапы для РПД всех форм обучения определяются по учебному плану очной формы обучения следующим образом:

Этап	Учебный план очной формы обучения/ семестр изучения дисциплины		
	Бакалавриат	Специалитет	Магистратура
<i>Начальный</i>	1-3 семестры	1-3 семестры	1 семестр
<i>Основной</i>	4-6 семестры	4-6 семестры	2 семестр
<i>Завершающий</i>	7-8 семестры	7-10 семестры	3-4 семестр

** Если при заполнении таблицы обнаруживается, что *один или два этапа* не обеспечены дисциплинами, практиками, НИР, необходимо:

- при наличии дисциплин, изучающихся в разных семестрах, – распределить их по этапам в зависимости от № семестра изучения (начальный этап соответствует более раннему семестру, основной и завершающий – более поздним семестрам);

- при наличии дисциплин, изучающихся в одном семестре, – все дисциплины указать для всех этапов.

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

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

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо)	Высокий уро- вень («отлично»)
1	2	3	4	5
ОПК-5 основной.	ОПК-5.1 Использует информацион- нокомму- никационные технологии при поиске необхо- димой инфор- мации.	<p>Знать: способы сбо- ра, анализа и обра- ботки данных, нор- мативных и методи- ческих материалов для анализа внут- ренних факторов.</p> <p>Уметь: анализиро- вать научно- техническую ин- формацию для ре- шения возникающих профессиональных задач.</p> <p>Владеть: навыками осуществлять сбор и обработку данных научно-технической информации, норма- тивных и методиче- ских материалов, не- обходимых для ана- лиза внутренних и внешних факторов, влияющих на эффек- тивность деятельно- сти персонала орга- низации.</p>	<p>Знать: способы сбора и обработки данных, норматив- ных и методиче- ских материалов для анализа внут- ренних и внешних факторов, влияю- щих на эффектив- ность деятельности персонала органи- зации.</p> <p>Уметь: анализи- ровать техниче- скую информацию для решения воз- никающих профес- сиональных задач с учетом информа- ционной безопас- ности.</p> <p>Владеть: навыками осуществлять сбор, анализ и обработку данных техниче- ской информации, нормативных и ме- тодических мате- риалов, необходи- мых для анализа внутренних и внешних факторов, влияющих на эф- фективность дея- тельности персона- ла организации с учетом требований обеспечения ин- формационной</p>	<p>Знать: спосо- бы сбора, ана- лиза и обра- ботки данных, нормативных и методических материалов для анализа внут- ренних и внешних фак- торов, влияю- щих на эффек- тивность дея- тельности пер- сонала органи- зации.</p> <p>Уметь: анали- зировать науч- но-техничес- кую информа- цию для реше- ния возникаю- щих профес- сиональных задач с учетом информацион- ной безопасно- сти.</p> <p>Владеть: на- выками осуще- ствлять сбор, анализ и обра- ботку данных научно- технической информации, нормативных и методических материалов,</p>

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо))	Высокий уро- вень («отлично»)
1	2	3	4	5
			безопасности.	необходимых для анализа внутренних и внешних факторов, влияющих на эффективность деятельности персонала организации с учетом требований обеспечения информационной безопасности.
	ОПК-5.2 Решает стандартные задачи профессиональной деятельности с использованием информационных технологий и программных средств.	Знать: полный перечень требуемой информации для ведения кадрового делопроизводства и организации архивного хранения кадровых документов; знать основы кадровой. Уметь: вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами. Владеть: навыками обеспечить защиту персональных данных сотрудников с учетом составления кадровой отчетно-	Знать: полный перечень требуемой информации для ведения кадрового делопроизводства и организации архивного хранения кадровых документов; знать основы кадровой документацией и действующие акты. Уметь: вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами; обеспечить защиту данных. Владеть: навыками обеспечить защиту	Знать: полный перечень требуемой информации для ведения кадрового делопроизводства и организации архивного хранения кадровых документов; знать основы кадровой документацией и действующие локальные нормативно-правовые акты. Уметь: вести кадровое делопроизводство и организовывать архивное хранение кадровых докумен-

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо))	Высокий уро- вень («отлично»)
1	2	3	4	5
		сти.	персональных дан- ных сотрудников с учетом составления кадровой отчетно- сти и действующи- ми правовыми ак- тами.	тов в соответ- ствии с дейст- вующими нор- мативно- правовыми ак- тами; обеспе- чить защиту персональных данных со- трудников. Владеть: на- выками обес- печить защиту персональных данных со- трудников с учетом состав- ления кадровой отчетности и действующими нормативно- правовыми ак- тами по ин- формационной безопасности.
	ОПК-5.3 Выбирает со- временные ин- формационные технологии и прикладные программные средства для решения по- ставленных за- дач.	Знать: способы сбо- ра и обработки дан- ных, методических материалов для ана- лиза внутренних и внешних факторов, влияющих на эффек- тивность деятельно- сти персонала орга- низации. Уметь: анализиро- вать техническую информацию для решения возникаю- щих профессиональ-	Знать: способы сбора, анализа и обработки данных, нормативных мате- риалов для анализа внутренних и внешних факторов, влияющих на эф- фективность дея- тельности персона- ла организации. Уметь: анализиро- вать техническую информацию для решения возни-	Знать: спосо- бы сбора, ана- лиза и обра- ботки данных, нормативных и методических материалов для анализа внут- ренних и внешних фак- торов, влияю- щих на эффек- тивность дея- тельности пер- сонала органи-

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо»)	Высокий уро- вень («отлично»)
1	2	3	4	5
		<p>ных задач.</p> <p>Владеть: навыками осуществлять сбор и обработку данных технической информации, методических материалов, необходимых для анализа внутренних и внешних факторов, влияющих на эффективность деятельности персонала организации с учетом требований обеспечения информационной безопасности.</p>	<p>кающих профес- сиональных задач с учетом информа- ционной безопас- ности.</p> <p>Владеть: навыками осуществлять сбор, анализ и обработку данных технической информации, нормативных и методических мате- риалов, необходи- мых для анализа внутренних и внешних факторов, влияющих на эф- фективность дея- тельности персона- ла организации с учетом требований обеспечения ин- формационной безопасности.</p>	<p>зации.</p> <p>Уметь: анали- зировать науч- но- техническую информацию для решения возникающих профессио- нальных задач с учетом ин- формационной безопасности.</p> <p>Владеть: на- выками осуще- ствлять сбор, анализ и обра- ботку данных научно- технической информации, нормативных и методических материалов, необходимых для анализа внутренних и внешних фак- торов, влияю- щих на эффек- тивность дея- тельности пер- сонала органи- зации с учетом требований обеспечения информацион- ной безопасно- сти.</p>

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо»)	Высокий уро- вень («отлично»)
1	2	3	4	5
ОПК-6 основной.	ОПК-6.1 Ориентируется в современных информацион- ных технологи- ях.	<p>Знать: способы сбо- ра и обработки дан- ных технической информации, норма- тивных и методиче- ских материалов для решения различного рода профессио- нальных задач.</p> <p>Уметь: анализиро- вать техническую информацию для решения возникаю- щих профессиональ- ных задач.</p> <p>Владеть: навыками осуществлять сбор и обработку данных технической инфор- мации, методиче- ских материалов, не- обходимых для ре- шения профессио- нальных задач и иных форм профес- сионального разви- тия персонала с уче- том требований ин- формационной безо- пасности.</p>	<p>Знать: способы сбора и обработки данных техниче- ской информации, нормативных и ме- тодических мате- риалов для реше- ния различного ро- да профессиональ- ных задач и иных форм профессио- нального развития персонала.</p> <p>Уметь: анализиро- вать техническую информацию для решения возни- кающих профес- сиональных задач.</p> <p>Владеть: навыками осуществлять сбор, анализ и обработку данных научно- технической ин- формации, норма- тивных и методи- ческих материалов, необходимых для решения профес- сиональных задач и иных форм профес- сионального разви- тия персонала.</p>	<p>Знать: спосо- бы сбора, ана- лиза и обра- ботки данных научно- технической информации, нормативных и методических материалов для решения раз- личного рода профессио- нальных задач и иных форм профессио- нального раз- вития персона- ла.</p> <p>Уметь: анали- зировать науч- но- техническую информацию для решения возникающих профессио- нальных задач.</p> <p>Владеть: на- выками осуще- ствлять сбор, анализ и обра- ботку данных научно- технической информации, нормативных и методических материалов, необходимых</p>

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо))	Высокий уро- вень («отлично»)
1	2	3	4	5
				для решения профессиональных задач и иных форм профессионального развития персонала с учетом требований информационной безопасности.
	ОПК-6.2 Использует в повседневной практике современные информационно-коммуникационные технологии и программные средства.	Знать: основные требования информационной безопасности для работы с корпоративными коммуникационными каналами. Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по установке, настройке и обслуживанию программных, средств с учетом основных требований информационной безопасности. Владеть: навыками информационного обеспечения процессов внутренних коммуникаций для решения задач профессиональной деятельности.	Знать: основные требования информационной безопасности для работы с корпоративными коммуникационными каналами и средствами передачи информации. Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по установке, настройке и обслуживанию программных, программно-аппаратных средств с учетом основных требований информационной безопасности. Владеть: навыками информационного	Знать: основные требования информационной безопасности для работы с корпоративными коммуникационными каналами и средствами передачи информации. Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств с уче-

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо»)	Высокий уро- вень («отлично»)
1	2	3	4	5
			обеспечения процессов внутренних коммуникаций для решения задач профессиональной деятельности с учетом основных требований информационной безопасности.	том основных требований информационной безопасности. Владеть: навыками информационного обеспечения процессов внутренних коммуникаций для решения задач профессиональной и научной деятельности с учетом основных требований информационной безопасности.
	ОПК-6.3 Применяет современные информационные технологии и программные средства для решения задач профессиональной деятельности.	Знать: основные требования информационной безопасности; принципы работы программных средств и технических средств обработки деловой информации с учетом основных требований информационной безопасности. Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по ус-	Знать: основные требования информационной безопасности; принципы работы программных, аппаратных средств и технических средств обработки деловой информации с учетом основных требований информационной безопасности. Уметь: применять все полученные знания при решении разного рода	Знать: основные требования информационной безопасности; принципы работы программных, программно – аппаратных средств и технических средств обработки деловой информации с учетом основных требований информационной безо-

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо»)	Высокий уро- вень («отлично»)
1	2	3	4	5
		<p>тановке, настройке и обслуживанию программных, аппаратных и технических средств обработки деловой информации.</p> <p>Владеть: методами и программными средствами обработки деловой информации; навыками взаимодействовать со службами информационных технологий; навыками эффективно использовать корпоративные информационные системы при решении задач управления персоналом.</p>	<p>задач профессиональной деятельности по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств обработки деловой информации.</p> <p>Владеть: методами и программными средствами обработки деловой информации; навыками взаимодействовать со службами информационных технологий; навыками эффективно использовать корпоративные информационные системы при решении задач управления персоналом с учетом основных требований информационной безопасности.</p>	<p>пасности.</p> <p>Уметь: применять все полученные знания при решении разного рода задач профессиональной деятельности по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств обработки деловой информации и научной.</p> <p>Владеть: методами и программными средствами обработки деловой, научной информации; навыками взаимодействовать со службами информационных технологий; навыками эффективно использовать корпоративные информационные системы при решении</p>

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисципли- ной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворитель- но»)	Продвинутый уро- вень (хорошо)	Высокий уро- вень («отлично»)
1	2	3	4	5
				задач управле- ния персона- лом с учетом основных тре- бований ин- формационной безопасности.

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 кон- троли- руемой компе- тенции (или её части)	Технология форми- рования	Оценочные средства		Описание шкал оценивания
				наиме- нование	№№ за- даний	
1	2	3	4	5	6	7
1	Защита ин- формации. Основные понятия и определения.	ОПК-5	Лекция, СРС, лабо- раторное занятие	собесе- дование кон- троль- ные во- просы к лб. №1	1-7 1-5	Согласно табл.7.2
2	Угрозы безопасности информации в компью- терных сис- темах.	ОПК-5	Лекция, СРС	собесе- дование	1-9	

3	Комплексная защита информации и правовое регулирование информационной безопасности.	ОПК-5 ОПК-6	Лекция, СРС, лабораторное занятие	собеседование	1-10	Согласно табл.7.2
				контрольные вопросы к лб. №2	1-5	
4	Защита информации от случайных угроз.	ОПК-5	Лекция, СРС	собеседование	1-6	Согласно табл.7.2
5	Методы и средства защиты информации от традиционного шпионажа и диверсий.	ОПК-6	Лекция, СРС, лабораторное занятие	собеседование	1-7	Согласно табл.7.2
				контрольные вопросы к лб. №3	1-6	
6	Средства защиты информации от утечки по виброакустическому и электромагнитному каналам.	ОПК-5, ОПК-6	Лекция, СРС	собеседование	1-13	Согласно табл.7.2
7	Методы защиты информации от несанкционированного изменения структуры компьютерной системы.	ОПК-5, ОПК-6	Лекция, СРС, лабораторное занятие	собеседование	1-6	Согласно табл.7.2
				контрольные вопросы к лб. №4	1-4	
8	Защита информации в компьютерных системах от несанкционированного доступа.	ОПК-6	Лекция, СРС, лабораторное занятие	собеседование	1-10	Согласно табл.7.2
				контрольные вопросы к лб. №5	1-6	

9	Криптографические методы защиты информации.	ОПК-5, ОПК-6	Лекция, СРС, лабораторное занятие	собеседование	1-12	Согласно табл.7.2
				контрольные вопросы к лб. №6	1-5	

БТЗ – банк вопросов и заданий в тестовой форме.

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы в тестовой форме по разделу (теме) 3. «Комплексная защита информации и правовое регулирование информационной безопасности»

- А) «Концепции национальной безопасности Российской Федерации».
- Б) Разделение информации по категориям доступа.
- В) Перечень сведений, доступ к которым не может быть ограничен.
- Г) Понятие коммерческая тайна.
- Д) Понятие государственной тайны.
- Е) Понятие служебная тайна.
- Ж) Понятие профессиональная тайны и персональные данные.
- И) Организационное обеспечение информационной безопасности. Лицензирование и сертификация в области защиты информации.

Вопросы для собеседования по разделу (теме) 2. «Шифрование методом полиалфавитной замены»

1. На чем основан метод полиалфавитной замены?
2. Что такое матрица Вижинера?
3. Как строится матрица Вижинера?
4. Как осуществляется шифрование сообщения данным методом?
5. Как осуществляется расшифрование сообщения?

Темы рефератов

1. Криптографические системы защиты данных.
2. Информация и личная безопасность.
3. Ответственность за нарушения в сфере информационного права.
4. Компьютерная преступность и компьютерная безопасность.
5. Преступления в сфере компьютерной информации.
6. Защита информации в глобальной сети.
7. Российский рынок информационной безопасности.
8. Ответственность за нарушения в сфере информационного права.

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 зачета. Зачет проводится в виде *компьютерного* тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы издания 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. Понятие государственной тайны.

- A. Отнесение сведений к государственной тайне.
- B. Определение степеней секретности сведений.
- C. Допуск к государственной тайне.
- D. Защита государственной тайны.

- Е. Средства защиты информации; технические, криптографические, программные.
- Ф. Доступ к сведениям, составляющим государственную тайну.

Задание в открытой форме:

Вопросы собеседования по разделу (теме) 3. «Комплексная защита информации и правовое регулирование информационной безопасности»

1. Разделение информации по категориям доступа происходит
2. Перечень сведений, доступ к которым не может быть ограничен осуществляется .
3. Понятие коммерческая тайна выполняется
4. Понятие служебная тайна осуществляется
5. Понятие профессиональная тайна выполняется
6. Понятие персональные данные происходит
7. Организационное обеспечение информационной безопасности осуществляется .
8. Лицензирование и сертификация в области защиты информации выполняется .

Задание на установление правильной последовательности

1. Выбор нормативного алфавита.
2. Выбор алфавита шифрования.
3. Установление взаимно однозначного соответствия между символами и матричного алфавита и символами алфавита шифрования.
4. Шифрование исходного сообщения.
5. Использование таблицы (матрицы) Вижинера для шифрования.

Задание на установление соответствия:

При N-алфавитной замене символ so_i из исходного алфавита A_0 заменяется символом S_{11} из алфавита A_1 , S_{02} заменяется символом S_{22} из алфавита A_2 и так далее.

После замены s_{0n} символом S_{nn} из A_n символ $so_{(n+1)}$ замещается символом $S_{1(n+1)}$ из алфавита A_1 и так далее.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера T_v , которая представляет собой квадратную матрицу $[R \times R]$, где R - количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность $[32 \times 32]$.

Компетентностно-ориентированная задача:

Шифры - шифр Виженера
полиалфавитный шифр замены

a b c d e f g h i j k l m n o p q r s t u v v w x y Z
 fwp bye Qxc kog wa sr hund Zim
 F Z N C B T G O Y C R E M H L S X I U W A Q D
 hello-> QNTKG Шифр Виженера
 t h i s i s a t e s t m e s s a g e
 s e s a m e s e s a m e s e s a m e
 l l a s u w s x w s f q w w k A

п

Метод взлома - тест Казисского

Криптография - исторические шифры

Компетентностно-ориентированная задача:

Алгоритм зашифрования с помощью таблицы Виженера представляет собой следующую последовательность шагов:

Шаг 1. Выбор ключа K длиной M символов.

Шаг 2. Построение матрицы шифрования $T_{Ш}=(Ц)$ размерностью $[(M+1), R]$ для выбранного ключа K .

Шаг 3. Под каждым символом $S_{ог}$ исходного текста длиной 1 символ размещается символ ключа k_m (рис. 20). Ключ повторяется необходимое число раз.

Шаг 4. Символы исходного текста последовательно замещаются символами, выбираемыми из $T_{Ш}$ по следующему правилу: определяется символ k^{TM} ключа K , соответствующий замещаемому символу $s_{ог}$; находится строка i в $T_{Ш}$, для которой выполняется условие $k_t=B_i$; определяется столбец j , для которого выполняется условие: $s_{ог}=b_{ij}$; символ $s_{от}$ замещается символом b_{ij} .

Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

Расшифрование осуществляется в следующей последовательности:

Шаг 1. Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.

Шаг 2. Последовательно выбираются символы $s_{г}$ из шифртекста и соответствующие символы ключа k_m . В матрице $T_{Ш}$ определяется строка i , для которой выполняется условие $k_{щ}=B_i$. В строке i определяется элемент $b_{y=(s)г}$. В расшифрованный текст на позицию $г$ помещается символ b_{ij} .

Шаг 3. Расшифрованный текст записывается без деления на блоки. Убираются служебные символы.

Пример. Требуется с помощью ключа $K = \langle \text{ЗОНД} \rangle$ зашифровать исходный текст $T = \langle \text{БЕЗОБЛАЧНОЕ_НЕБО} \rangle$.

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 Обально-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
Выполнение работы «Шифрование методом простой замены»	2	но «не защитил»	4	и «защитил»
Выполнение лабораторной работы «Шифрование методом полиалфавитной замены»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование методом перестановок»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Схема Шамира разделения секрета»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование аналитическими методами (методами матричной алгебры)»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы по исследованию шифрования с открытым ключом	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	12		24	
Итого:	24		48	
Посещаемость	0		16	
Зачет	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 –2балла,
- 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. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 255 с. - URL: <http://biblioclub.ru/index.php?page=book&id=276557> (дата обращения: 21.02.2024) . - Режим доступа: по подписке. - Текст : электронный.

2. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын. - Томск : Эль Контент, 2011. - 148 с. - URL: <http://biblioclub.ru/index.php?page=book&id=208694> (дата обращения: 26.09.2024) . - Режим доступа: по подписке. - Текст : электронный.

3. Пушкарев, В. П. Защита информационных процессов в компьютерных системах (безопасность жизнедеятельности 2) : учебное пособие / В. П. Пушкарев, В. В. Пушкарев ; Томский государственный университет систем управления и радиоэлектроники (ТУСУР). Кафедра средств радиосвязи (СРС). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2005. - 131 с. - URL: <https://biblioclub.ru/index.php?page=book&id=208718> (дата обращения: 30.03.2024) . - Режим доступа: по подписке. - Текст : электронный.

8.2 Дополнительная учебная литература

4. Гулятьева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гулятьева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. – URL: <https://biblioclub.ru/index.php?page=book&id=574729> (дата обращения: 08.09.2024). – Режим доступа: по подписке. – Текст : электронный.

5. Защита информации в системах мобильной связи : учебное пособие / А. А. Чекалин [и др.]. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2005. - 171 с. - Текст : непосредственный.

6. Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. - Ростов-на-Дону : Южный федеральный университет, 2016. - 74 с. - URL: <https://biblioclub.ru/index.php?page=book&id=493175> (дата обращения 08.09.2024) . - Режим доступа: по подписке. - Текст : электронный.

8.3 Перечень методических указаний

1. Шифрование методом прямой замены : методические указания по выполнению лабораторной работы для студентов направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, С. И. Егоров. - Курск : ЮЗГУ, 2019. - 14 с. - Загл. с титул. экрана. - Текст : электронный.

2. Шифрование методом полиалфавитной замены : методические указания по выполнению лабораторной работы для студентов направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03 / Юго-Зап. гос. ун-т ; сост.: М. А. Ефремов, С. И. Егоров. - Курск : ЮЗГУ, 2019. - 9 с. - Загл. с титул. экрана. - Текст : электронный.

3. Шифрование методом перестановок : методические указания по выполнению лабораторной работы для студентов направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Курск : ЮЗГУ, 2019. - 9 с. - Загл. с титул. экрана. - Текст : электронный.

8.4 Другие учебно-методические материалы

Периодические издания:

1. Журнал «Защита информации - odpiska@insideazi.ru, <http://www.insideazi.ru>.
2. Проблемы информационной безопасности. Компьютерные системы - ojs@ic.spbstu.ru.
3. Журнал «Проблемы правовой и технической защиты информации» - conf_kib@asu.ru.
4. Журнал «Информация и безопасность» - borisoglebsk@vgasu.vrn.ru
5. Журнал «Вестник УрФО. Безопасность в информационной сфере» - urvest@mail.ru.
6. Журнал «Information Security/ Информационная безопасность» - public@akc.ru.

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

1. <http://biblioclub.ru> - Электронно-библиотечная система «Университетская библиотека онлайн».
2. www.elibrary.ru/defaultx.asp - научная электронная библиотека.
3. www.edu.ru - федеральный портал «Российское образование».
4. www.consultant.ru - Официальный сайт компании «Консультант Плюс».
5. Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>.
6. Научно-информационный портал ВИНТИ РАН [официальный сайт]. Режим доступа: <http://www.consultant.ru/>

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 практическим 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 лабораторных занятиях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседо-

вании). 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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Защита информации» с целью освоения 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)

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, открытая среда разработки программного обеспечения Lazarus (Свободное ПО <http://www.lazarus.freepascal.org/>)

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 Тб, монитор Aок 21". Проекционный экран на штативе. Мультимедиацентр: ноутбук ASUSX50VLPMD-T2330/14"/1024Mb /160Gb/сумка/ проектор inFocusIN24+

13. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменение
	изменённых	заменённых	аннулированных	новых			