Аннотация к рабочей программе дисциплины «Информационная безопасность»

Цель преподавания дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации.

Задачи изучения дисциплины

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

Компетенции, формируемые в результате освоения дисциплины

– ОПК-6: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

Разделы дисциплины

1 Основные понятия и анализ угроз информационной безопасности
2 Проблемы информационной безопасности сетей
3 Политика безопасности
4 Криптографическая защита информации
5 Технологии аутентификации
6 Технологии межсетевых экранов
7 Технологии защиты от вирусов
8 Требования к системам защиты информации
9 Основы правового обеспечения защиты информации

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декана факультета
Экономики и менеджмента
(наименование ф-та полностью)
Т.Ю. Ткачева
(подпись, инициалы, фамилия)
«31» августа 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

ОПОП ВО 38.05.01 Экономическая безопасность

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

направленность (специализация) «Экономико-правовое обеспечение экономической безопасности»

наименование направленности (профиля, специализации)

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по специальности 38.05.01 Экономическая безопасность на основании учебного плана ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», одобренного Ученым советом университета (протокол № 7 от 28.02.2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности»на заседании кафедры информационной безопасности, протокол № 11 «30» 06 2022 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доц. _____ Марухленко А.Л.
(ученая степень и ученое звание, Ф.И.О.)

Согласовано: на заседании кафедры экономической безопасности налогообложения протокол № 1 «31» 08 2022 г.

Зав. кафедрой _____ Афанасьева Л.В.

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ, протокол № 12 от 29.06.2023г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Марухленко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», одобренного Ученым советом университета протокол № ___ «__» _____ 20___ г., на заседании кафедры ИБ, протокол № 11 от 27.06.2024г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Марухленко А.Л.

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

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации.

1.2 Задачи дисциплины

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

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

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	ОПК-6.1 Применяет современные инструментальные средства для обработки экономической информации	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им. ***Уметь:*** правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
		ОПК-6.2 Выполняет профессиональные задачи с использованием современных информационных технологий	***Знать:*** алгоритмы работы криптографических систем, методы аутентификации и принципы работы аппаратно-программных систем идентификации и аутентификации, функции, классификацию и схемы подключения межсетевых экранов. ***Уметь:*** правильно эксплуатировать и разрабатывать криптографические программы, предлагать конкретные меры по усилению парольной защиты,

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*		
			применять антивирусные программные комплексы. ***Владеть:*** навыками защиты информации в компьютерных системах, навыками анализа защищенности локальной вычислительной сети.
		ОПК-6.3 Интерпретирует и критически оценивает решения профессиональных задач с помощью современных информационных технологий и программных средств	***Знать:*** классификацию компьютерных вирусов, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, основные требования к системам защиты информации, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем, основные юридические законы в области защиты информации. ***Уметь:*** настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети, разрабатывать защищенные сайты с использованием языков HTML, JavaScript, PHP, проводить анализ информационных рисков. ***Владеть:*** навыками эксплуатации программных средств анализа и управления рисками, навыками разработки криптографических программ, навыками разработки защищенных сайтов.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность», входит в обязательную часть блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы специалитета 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности». Дисциплина изучается на 3 курсе в 5 семестре.

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

Общая трудоемкость (объем) дисциплины составляет 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)	54
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	18
Самостоятельная работа обучающихся (всего)	53,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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

4.1 Содержание дисциплины

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

№ п/п	Раздел, (тема) дисциплины	Содержание

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

		идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	2	-	1	У-1-6 МУ-1-6	УО, ЗПР - 2	ОПК-6
2	Проблемы информационной безопасности сетей	2	-	2	У-1-6 МУ-1-6	УО, ЗПР - 4	ОПК-6
3	Политика безопасности	2	-	3	У-1-6 МУ-1-6	УО, ЗПР - 6	ОПК-6
4	Криптографическая защита информации	2	-	4	У-1-6 МУ-1-6	УО, ЗПР – 8	ОПК-6
5	Технологии аутентификации	2	-	5	У-1-6 МУ-1-6	УО, ЗПР - 10	ОПК-6
6	Технологии межсетевых экранов	2	-	6	У-1-6 МУ-1-6	УО, ЗПР - 12	ОПК-6
7	Технологии защиты от вирусов	2	-	7	У-1-6 МУ-1-6	УО, ЗПР - 14	ОПК-6
8	Требования к системам защиты информации	2	-	8	У-1-6 МУ-1-6	УО, ЗПР – 16	ОПК-6
9	Основы правового обеспечения защиты информации	2	-	9	У-1-6 МУ-1-6	УО, ЗПР - 18	ОПК-6
	Всего	18					

УО – устный опрос, ЗЛР – лабораторная работа, ЗПР – практическая работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
1	Разработка криптографической программы «Шифр Виженера»	4
2	Разработка криптографической программы «Алгоритм RSA»	4
3	Менеджер паролей – программа Password Commander.	4
4	Настройка межсетевого экрана Comodo Firewall	4

5	Эксплуатация антивирусной программы Kaspersky Internet Security	4
6	Анализ и управление информационными рисками в программе “Гриф”.	4
7	Разработка Web - приложений на языке HTML.	4
8	Разработка и защита Web - приложений с клиентскими сценариями на языке JavaScript.	4
9	Разработка и защита Web - приложений с серверными сценариями на языке PHP.	4
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и анализ угроз информационной безопасности	2 неделя	4,9
2	Проблемы информационной безопасности сетей	4 неделя	5
3	Политика безопасности	6 неделя	6
4	Криптографическая защита информации	8 неделя	6
5	Технологии аутентификации	10 неделя	6
6	Технологии межсетевых экранов	12 неделя	6
7	Технологии защиты от вирусов	14 неделя	6
8	Требования к системам защиты информации	16 неделя	7
9	Основы правового обеспечения защиты информации	18 неделя	7
Итого			53,9

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

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

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

библиотекой университета:

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

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

кафедрой:

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

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

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

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

типографией университета:

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

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

6. Образовательные технологии

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

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

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Практическое занятие №1. Разработка криптографической программы «Шифр Виженера»	Анализ конкретных ситуаций	1
2	Практическое занятие №2. Разработка криптографической программы «Алгоритм RSA»	Анализ конкретных ситуаций	1
3	Практическое занятие №3. Менеджер паролей – программа Password Commander.	Анализ конкретных ситуаций	1
4	Практическое занятие №4. Настройка межсетевого экрана Comodo Firewall	Анализ конкретных ситуаций	1

5	Практическое занятие №5. Эксплуатация антивирусной программы Kaspersky Internet Security	Анализ конкретных ситуаций	2
Итого			6

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован 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 общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– 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 средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	Статистика Информатика	Информационная безопасность Деньги, кредит, банки Учебная ознакомительная практика	Деньги, кредит, банки

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ОПК-6, основной.	ОПК-6.1 Применяет современные инструментальные средства для обработки экономической информации	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать за-

			Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	щищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-6.2 Выполняет профессиональные задачи с использованием современных информационных технологий	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-6.3 Интерпретирует и критически оценивает решения профессиональных задач с помо-	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь:

	щью современных информационных технологий и программных средств	безопасности. Владеть: навыками применения программных средств защиты информации.	решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №1	1-3 1 – 3	Согласно таблице 7.2

2	Проблемы информационной безопасности сетей	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №2	4-14 1 – 3	Согласно таблице 7.2
3	Политика безопасности	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №3	15-17 1-4	Согласно таблице 7.2
4	Криптографическая защита информации	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №4	18-24 1 - 4	Согласно таблице 7.2
5	Технологии аутентификации	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №5	25-30 1-5	Согласно таблице 7.2
6	Технологии межсетевых экранов	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №6	31-33 1 - 4	Согласно таблице 7.2
7	Технологии защиты от вирусов	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №7	34-41 1-4	Согласно таблице 7.2
8	Требования к системам защиты информации	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №8	42-46 1-4	Согласно таблице 7.2
9	Основы правового обеспечения защиты информации	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №9	47-60 1-4	Согласно таблице 7.2

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

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

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

1. Основные понятия защиты информации и информационной безопасности.

2. Классификация угроз информационной безопасности автоматизированных систем.

3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.

Контрольные вопросы для защиты практических работ:

Разработка криптографической программы «Шифр Виженера»
1. Квадрат (таблица) Виженера
2. Алфавитный шифр
3. Количество символов в строке для русского алфавита

Анализ и управление информационными рисками в программе “Гриф”
1. Назначение системы Гриф
2. Модуль управления системы Гриф
3. Виды защищённости информации на ресурсе
4. Алгоритм задания контрмер

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

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

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

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

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

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),

- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

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

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

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Какая угроза информационной безопасности является пассивной:
А) Копирование секретных данных.
Б) Внедрение вредоносного программного обеспечения.
В) Кража носителей информации.
Г) Удаление файла.

Задание в открытой форме:

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

Задание на установление правильной последовательности.

Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

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

способов и видов информации

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

Компетентностно-ориентированная задача:

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

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

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

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

– положение П 02.016–2018 О балльно - рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по темам 1-3	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 4-6	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 7-9	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Практическая работа № 1 «Разработка криптографической программы «Шифр Виженера»»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 2 «Разработка криптографической программы «Алгоритм RSA»»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 3 «Менеджер паролей – программа Password Commander»»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Практическая работа № 4 «Настройка межсетевого экрана Comodo Firewall»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Практическая работа № 5 «Эксплуатация антивирусной программы Kaspersky Internet Security»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Практическая работа №6 « Анализ и управление информационными рисками в программе “Гриф”»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа №7 «Разработка Web - приложений на языке HTML.»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа №8 «Разработка и защита Web - приложений с клиентскими сценариями на языке	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%

JavaScript.»				
Практическая работа №9 «Разработка и защита Web - приложений с серверными сценариями на языке PHP.»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

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

Каждый верный ответ оценивается следующим образом:

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

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная учебная литература

1. А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 07.08.2022). – Библиогр. в кн. – ISBN 978-5-4499-1676-1. – DOI 10.23681/599050. – Текст : электронный.

2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения:

07.08.2022). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

3. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. - Москва ; Берлин : Директ-Медиа, 2021. - 201 с. : ил., табл. - URL: http://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 28.08.2022) . - Режим доступа: по подписке. - ISBN 978-5-4499-1674-7. - Текст : электронный.

8.2 Дополнительная учебная литература

4. Информационная безопасность [Текст]: учебное пособие / А. Г. Спеваков [и др.] – Курск : ЮЗГУ, 2017. - 196 с.

5. Информационные системы в экономике [Текст] : учебное пособие / Д. В. Чистов [и др.]. - М. : Инфра-М, 2019. - 234 с.

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации[Электронный ресурс] :учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=276557

8.3 Перечень методических указаний

1. Методические указания по организации самостоятельной работы студентов [Электронный ресурс] : по дисциплине «Основы информационной безопасности» для студентов специальности 02.03.03/ Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с.

2. Шифрование с помощью таблицы Виженера : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост.: А. Л. Марухленко, А. Л. Ханис. - Электрон. текстовые дан. (734 КБ). - Курск : ЮЗГУ, 2021. - 19 с. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

3. Алгоритм шифрования RSA : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 02.03.03 математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост.: А. Л. Марухленко, А. Л. Ханис. - Электрон. текстовые дан. (371 КБ). - Курск : ЮЗГУ, 2021. - 11 с. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

4. Фаервол Comodo Firewall : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 02.03.03 математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (663 КБ). - Курск : ЮЗГУ, 2021. - 15 с. : ил. - Загл. с титул. экрана. - Б. ц.

5. Разработка криптографических программ на языке Delphi [Электронный ресурс]: методические указания по выполнению лабораторных работ по дисциплине «Информационная безопасность» для студентов направлений под-

готовки бакалавров 02.03.03 / ЮЗГУ; сост.: К. А. Тезик, А. Л. Марухленко. – Курск : ЮЗГУ, 2015. – 50 с.

6. Менеджер паролей: программа Password Commander [Электронный ресурс] : методические указания по выполнению практических занятий по дисциплине «Информационная безопасность» для студентов направлений подготовки бакалавров 02.03.03 / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2017. - 16 с.

8.4 Другие учебно-методические материалы

Периодические издания:

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

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

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

10. Методические указания для обучающихся по освоению дисциплины

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

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

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

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

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

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

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

ру по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность» с целью усвоения и закрепления компетенций.

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

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

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

Программа хранения паролей Password Commander (свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFI LANguard Network Security Scanner.

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

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

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

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

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

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

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

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

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

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

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Измененных	Заменённых	Аннулированных	новых			

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декана факультета
Экономики и менеджмента
(наименование ф-та полностью)
_____ Т.Ю. Ткачева
(подпись, инициалы, фамилия)

«31» августа 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность
(наименование дисциплины)

ОПОП ВО 38.05.01Экономическая безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (специализация) «Экономико-правовое обеспечение экономической безопасности»
наименование направленности (профиля, специализации)

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

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по специальности 38.05.01 Экономическая безопасность на основании учебного плана ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», одобренного Ученым советом университета (протокол № 7 от 28.02.2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности»на заседании кафедры информационной безопасности, протокол № 11 «30» 06 2022 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доц. _____ Марухленко А.Л.
(ученая степень и ученое звание, Ф.И.О.)

Согласовано: на заседании кафедры экономической безопасности налогообложения протокол № 1 «31» 08 2022 г.

Зав. кафедрой _____ Афанасьева Л.В.

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ, протокол № 12 от 29.06.2023г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Марухленко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 38.05.01Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», одобренного Ученым советом университета протокол № ___ «__» _____ 20___ г., на заседании кафедры ИБ, протокол № 11 от 27.06.2024г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Марухленко А.Л.

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

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность» является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации.

1.2 Задачи дисциплины

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

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

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	ОПК-6.1 Применяет современные инструментальные средства для обработки экономической информации	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им. ***Уметь:*** правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
		ОПК-6.2 Выполняет профессиональные задачи с использованием современных информационных технологий	***Знать:*** алгоритмы работы криптографических систем, методы аутентификации и принципы работы аппаратно-программных систем идентификации и аутентификации, функции, классификацию и схемы подключения межсетевых экранов. ***Уметь:*** правильно эксплуатировать и разрабатывать криптографические программы, предлагать конкретные меры по усилению парольной защиты,

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*		
			применять антивирусные программные комплексы. ***Владеть:*** навыками защиты информации в компьютерных системах, навыками анализа защищенности локальной вычислительной сети.
		ОПК-6.3 Интерпретирует и критически оценивает решения профессиональных задач с помощью современных информационных технологий и программных средств	***Знать:*** классификацию компьютерных вирусов, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, основные требования к системам защиты информации, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем, основные юридические законы в области защиты информации. ***Уметь:*** настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети, разрабатывать защищенные сайты с использованием языков HTML, JavaScript, PHP, проводить анализ информационных рисков. ***Владеть:*** навыками эксплуатации программных средств анализа и управления рисками, навыками разработки криптографических программ, навыками разработки защищенных сайтов.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность», входит в обязательную часть блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы специалитета 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности». Дисциплина изучается на 3 курсе.

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)	10
в том числе:	
лекции	4
лабораторные занятия	
практические занятия	6
Самостоятельная работа обучающихся (всего)	93,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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

4.1 Содержание дисциплины

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

№ п/п	Раздел, (тема) дисциплины	Содержание

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

		идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	0,25	-	1	У-1-6 МУ-1-6	УО, ЗПР - 2	ОПК-6
2	Проблемы информационной безопасности сетей	0,25	-		У-1-6 МУ-1-6	УО – 4	ОПК-6
3	Политика безопасности	0,5	-	2	У-1-6 МУ-1-6	УО, ЗПР - 6	ОПК-6
4	Криптографическая защита информации	0,5	-		У-1-6 МУ-1-6	УО – 8	ОПК-6
5	Технологии аутентификации	0,5	-	3	У-1-6 МУ-1-6	УО, ЗПР - 10	ОПК-6
6	Технологии межсетевых экранов	0,5	-		У-1-6 МУ-1-6	УО –12	ОПК-6
7	Технологии защиты от вирусов	0,5	-	4	У-1-6 МУ-1-6	УО, ЗПР - 14	ОПК-6
8	Требования к системам защиты информации	0,5	-		У-1-6 МУ-1-6	УО –16	ОПК-6
9	Основы правового обеспечения защиты информации	0,5	-	5	У-1-6 МУ-1-6	УО, ЗПР - 18	ОПК-6
	Всего	4					

УО – устный опрос, ЗПР – практическая работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
1	Разработка криптографической программы «Шифр Виженера»	1,5
2	Разработка криптографической программы «Алгоритм RSA»	1,5
3	Менеджер паролей – программа Password Commander.	1
4	Настройка межсетевого экрана Comodo Firewall	1

5	Эксплуатация антивирусной программы Kaspersky Internet Security	1
Итого		6

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и анализ угроз информационной безопасности	2 неделя	9,9
2	Проблемы информационной безопасности сетей	4 неделя	10
3	Политика безопасности	6 неделя	10
4	Криптографическая защита информации	8 неделя	10
5	Технологии аутентификации	10 неделя	12
6	Технологии межсетевых экранов	12 неделя	10
7	Технологии защиты от вирусов	14 неделя	10
8	Требования к системам защиты информации	16 неделя	10
9	Основы правового обеспечения защиты информации	18 неделя	12
Итого			93,9

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

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

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

библиотекой университета:

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

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

кафедрой:

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

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

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

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

типографией университета:

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

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

6. Образовательные технологии

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

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

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Практическое занятие №1. Разработка криптографической программы «Шифр Виженера»	Анализ конкретных ситуаций	1
2	Практическое занятие №2. Разработка криптографической программы «Алгоритм RSA»	Анализ конкретных ситуаций	1
3	Лекция №3	Анализ конкретных ситуаций	0,5
4	Лекция №4	Анализ конкретных ситуаций	0,5
5	Лекция №5	Анализ конкретных ситуаций	0,5
6	Лекция №6	Анализ конкретных ситуаций	0,5
Итого			4

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован 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 общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– 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 средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	Статистика Информатика	Информационная безопасность Деньги, кредит, банки Учебная ознакомительная практика	Деньги, кредит, банки

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ОПК-6, основной.	ОПК-6.1 Применяет современные инструментальные средства для обработки экономической информации	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать за-

			Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	щищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-6.2 Выполняет профессиональные задачи с использованием современных информационных технологий	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-6.3 Интерпретирует и критически оценивает решения профессиональных задач с помо-	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь:

	щью современных информационных технологий и программных средств	безопасности. Владеть: навыками применения программных средств защиты информации.	решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №1	1-3 1 – 3	Согласно таблице 7.2

2	Проблемы информационной безопасности сетей	ОПК-6	Лекция, СРС	Вопросы для устного опроса	4-14	Согласно таблице 7.2
3	Политика безопасности	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №2	15-17 1-3	Согласно таблице 7.2
4	Криптографическая защита информации	ОПК-6	Лекция, СРС	Вопросы для устного опроса	18-24	Согласно таблице 7.2
5	Технологии аутентификации	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №3	25-30 1-4	Согласно таблице 7.2
6	Технологии межсетевых экранов	ОПК-6	Лекция, СРС	Вопросы для устного опроса	31-33	Согласно таблице 7.2
7	Технологии защиты от вирусов	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №4	34-41 1-4	Согласно таблице 7.2
8	Требования к системам защиты информации	ОПК-6	Лекция, СРС	Вопросы для устного опроса	42-46	Согласно таблице 7.2
9	Основы правового обеспечения защиты информации	ОПК-6	Лекция, практическая работа СРС	Вопросы для устного опроса КВЗПР №5	47-60 1-5	Согласно таблице 7.2

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

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

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

1. Основные понятия защиты информации и информационной безопасности.

2. Классификация угроз информационной безопасности автоматизированных систем.

3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.

Контрольные вопросы для защиты практических работ:

Разработка криптографической программы «Шифр Виженера»
1. Квадрат (таблица) Виженера
2. Алфавитный шифр
3. Количество символов в строке для русского алфавита

Анализ и управление информационными рисками в программе “Гриф”
1. Назначение системы Гриф
2. Модуль управления системы Гриф
3. Виды защищённости информации на ресурсе
4. Алгоритм задания контрмер

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

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

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

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

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

Для проверки *знаний* используются вопросы и задания в различных формах:

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

– на установление соответствия.

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

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

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Какая угроза информационной безопасности является пассивной:
А) Копирование секретных данных.
Б) Внедрение вредоносного программного обеспечения.
В) Кража носителей информации.
Г) Удаление файла.

Задание в открытой форме:

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

Задание на установление правильной последовательности.

Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

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

способов и видов информации

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

Компетентностно-ориентированная задача:

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

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

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

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

– положение П 02.016–2018 О балльно - рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по темам 1-3	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 4-6	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 7-9	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Практическая работа № 1 «Разработка криптографической программы «Шифр Виженера»»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 2 «Разработка криптографической программы «Алгоритм RSA»»	3	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 3 «Менеджер паролей – программа Password Commander»»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 4 «Настройка межсетевого экрана Comodo Firewall»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Практическая работа № 5 «Эксплуатация антивирусной программы Kaspersky Internet Security»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Итого	14		26	
Посещаемость	0		14	
Зачёт	0		60	
Итого	14		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 –3 балла,
- задание в открытой форме – 3 балла,
- задание на установление правильной последовательности – 3 балла,
- задание на установление соответствия – 3 балла,
- решение компетентностно-ориентированной задачи – 15 баллов.

Максимальное количество баллов за тестирование – 60 баллов.

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

8.1 Основная учебная литература

1. А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 07.08.2022). – Библиогр. в кн. – ISBN 978-5-4499-1676-1. – DOI 10.23681/599050. – Текст : электронный.

2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.08.2022). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

3. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. - Москва ; Берлин : Директ-Медиа, 2021. - 201 с. : ил., табл. - URL: http://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 28.08.2022) . - Режим доступа: по подписке. - ISBN 978-5-4499-1674-7. - Текст : электронный.

8.2 Дополнительная учебная литература

4. Информационная безопасность [Текст]: учебное пособие / А. Г. Спеваков [и др.] – Курск : ЮЗГУ, 2017. - 196 с.

5. Информационные системы в экономике [Текст] : учебное пособие / Д. В. Чистов [и др.]. - М. : Инфра-М, 2019. - 234 с.

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации[Электронный ресурс] :учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=276557

8.3 Перечень методических указаний

1. Методические указания по организации самостоятельной работы студентов [Электронный ресурс] : по дисциплине «Основы информационной безопасности» для студентов специальности 02.03.03/ Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с.

2. Шифрование с помощью таблицы Виженера : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост.: А. Л. Марухленко, А. Л. Ханис. - Электрон. текстовые дан. (734 КБ). - Курск : ЮЗГУ, 2021. - 19 с. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

3. Алгоритм шифрования RSA : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 02.03.03 математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост.: А. Л. Марухленко, А. Л. Ханис. - Электрон. текстовые дан. (371 КБ). - Курск : ЮЗГУ, 2021. - 11 с. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

4. Фаервол Comodo Firewall : методические указания по выполнению практических работ для студентов направления подготовки (специальности) 02.03.03 математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Электрон. текстовые дан. (663 КБ). - Курск : ЮЗГУ, 2021. - 15 с. : ил. - Загл. с титул. экрана. - Б. ц.

5. Разработка криптографических программ на языке Delphi [Электронный ресурс]: методические указания по выполнению лабораторных работ по дисциплине «Информационная безопасность» для студентов направлений подготовки бакалавров 02.03.03 / ЮЗГУ; сост.: К. А. Тезик, А. Л. Марухленко. – Курск : ЮЗГУ, 2015. – 50 с.

6. Менеджер паролей: программа Password Commander [Электронный ресурс] : методические указания по выполнению практических занятий по дисциплине «Информационная безопасность» для студентов направлений подготовки бакалавров 02.03.03 / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2017. - 16 с.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца

2. Журнал «InformationSecurity/Информационная безопасность.» - http://window.edu.ru/

3. Журнал «Проблемы информационной безопасности. Компью терные системы» - http://window.edu.ru/

4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

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

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

10. Методические указания для обучающихся по освоению дисциплины

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

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

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

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

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

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

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого 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 «Информационная безопасность» с целью усвоения и закрепления компетенций.

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

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

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

Программа хранения паролей Password Commander (свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFI LANguard Network Security Scanner.

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

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

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

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

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

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

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

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях

ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

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

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

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изменённых	Заменённых	Аннулированных	новых			
