Аннотация к рабочей программе дисциплины «Защита информации в компьютерных системах и сетях» направление подготовки бакалавров «02.03.03 – Математическое обеспечение и администрирование информационных систем»

Цель преподавания дисциплины:

Целью преподавания дисциплины «Защита информации в компьютерных системах и сетях» 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 принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- 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 средств анализа защищенности и обнаружения сетевых атак;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение методов и программных средств анализа рисков;
- изучение принципов разработки и защиты Web-сайтов.

Индикаторы компетенций, формируемые в результате освоения дисциплины:

ПК-5.1 Определяет базовые элементы конфигурации информационной системы;

ПК-5.2 Присваивает версии базовым элементам конфигурации информационной системы;

ПК-5.3 Устанавливает базовые версий конфигурации информационной системы;

ПК-6.1 Анализирует возможность реализации требований к программному обеспечению;

ПК-6.2 Проводит оценку времени и трудоемкости реализации требований к программному обеспечению;

ПК-6.3 Согласовывает требования к программному обеспечению с заинтересованными сторонами;

ПК-6.4 Осуществляет оценку и согласование сроков выполнения поставленных задач.

Разделы дисциплины:

1. Проблемы информационной безопасности сетей
2. Политика безопасности
3. Технологии аутентификации
4. Технологии межсетевых экранов
5. Технологии защиты от вирусов
6. Технологии анализа защищенности и обнаружения сетевых атак
7. Требования к системам защиты информации
8. Аудит безопасности информационных систем
9. Разработка и защита Web-сайтов

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

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

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

«30» 08 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в компьютерных системах и сетях
(наименование дисциплины)

ОПОП ВО 02.03.03
(шифр и наименование направления

Математическое обеспечение и администрирование информационных систем
подготовки (специальности)

Математическое и информационное обеспечение экономической деятельности
наименование направленности (профиля, специализации)

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

Курск – 2019

Рабочая программа дисциплины Защита информации в компьютерных системах и сетях составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 02.03.03. Математическое обеспечение и администрирование информационных систем на основании учебного плана ОПОП ВО 02.03.03. Математическое обеспечение и администрирование информационных систем, направленность Математическое и информационное обеспечение экономической деятельности, одобренного Ученым советом университета (протокол № 7 «29» 03 2019г.).

Рабочая программа дисциплины Защита информации в компьютерных системах и сетях обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 02.03.03. Математическое обеспечение и администрирование информационных систем, направленность Математическое и информационное обеспечение экономической деятельности на заседании кафедры информационной безопасности Протокол № 11
«27» 06 2019 г.

Зав. кафедрой Таныгин М.О.
Разработчик программы
к.в.н., доцент Ханис А.Л.
Согласовано: на заседании кафедры ИСиЗИ
№ 1 «29» 08 2019 г.
Зав. кафедрой Сазонов С.Ю.
Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Защита информации в компьютерных системах и сетях пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 02.03.03. Математическое обеспечение и администрирование информационных систем, направленность Математическое и информационное обеспечение экономической деятельности, одобренного Ученым советом университета протокол №7«29»03 2020г., на заседании кафедры ИБ, протокол № 1 от 31.04.2020 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 02.03.03 Математическое обеспечение и администрирование информационных систем, направленность (профиль, специализация) «Математическое и информационное обеспечение экономической деятельности», одобренного Ученым советом университета протокол №7«25» 02 2020 г., на заседании кафедры ИБ, протокол № 11 от 28.06.2021

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ М.О. Тынянкин

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 02.03.03 Математическое обеспечение и администрирование информационных систем, направленность (профиль, специализация) «Математическое и информационное обеспечение экономической деятельности», одобренного Ученым советом университета протокол №6«26» 02 2021 г., на заседании кафедры ИБ, протокол № 11 от 30.06.2022 г

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ М.О. Тынянкин

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 02.03.03 Математическое обеспечение и администрирование информационных систем, направленность (профиль, специализация) «Математическое и информационное обеспечение экономической деятельности», одобренного Ученым советом университета протокол №9«25» 06 2021 г., на заседании кафедры ИБ, протокол №1 от 30.08.2023 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ А.А. Марусенко

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 02.03.03 Математическое обеспечение и администрирование информационных систем, направленность (профиль, специализация) «Математическое и информационное обеспечение экономической деятельности», одобренного Ученым советом университета протокол №_«__»___20__г., на заседании кафедры _____

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1 Цель дисциплины

Целью преподавания дисциплины «Защита информации в компьютерных системах и сетях» 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 принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- 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 средств анализа защищенности и обнаружения сетевых атак;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение методов и программных средств анализа рисков;
- изучение принципов разработки и защиты Web-сайтов.

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*		
ПК-5	Способен выбирать архитектуру и комплексирование современных компь-	ПК-5.1 Определяет базовые элементы кон-	***Знать:*** методы защиты информации, способы защиты информационных систем, методы анализа

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*		
	ютеров, систем, комплексов и сетей системного администрирования.	фигурации информационной системы.	угроз и оценки рисков информационной безопасности информационных систем. ***Уметь:*** применять средства защиты информации для решения практических задач в области защиты компьютерных систем и сетей, разрабатывать защищенные сайты, проводить анализ информационных рисков. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
		ПК-5.2 Присваивает версии базовым элементам конфигурации информационной системы.	***Знать:*** виды угроз и каналы утечки информации, принципы построения политики безопасности, основные виды сетевых атак. ***Уметь:*** проводить анализ угроз, рисков, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть:*** навыками защиты информации в компьютерных системах, навыками анализа защищенности локальной вычислительной сети.
		ПК-5.3 Устанавливает базовые версии конфигурации информационной системы.	***Знать:*** классификацию компьютерных вирусов, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, классификацию и архитектуру систем обнаружения атак, основные этапы аудита безопасности информационных систем, методы анализа и управления рисками, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники

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*		
			от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь:*** 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 защищенных сайтов.
ПК-6	Способен использовать современные системные программные средства: операционные системы, операционные и сетевые оболочки, сервисные программы.	ПК-6.1 Анализирует возможность реализации требований к программному обеспечению.	***Знать:*** методы защиты информации, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности информационных систем. ***Уметь:*** применять средства защиты информации для решения практических задач в области защиты компьютерных систем и сетей, разрабатывать защищенные сайты, проводить анализ информационных рисков. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
		ПК-6.2 Проводит оценку времени и трудоемкости реализации требований к программному обеспечению.	***Знать:*** виды угроз и каналы утечки информации, принципы построения политики безопасности, основные виды сетевых атак. ***Уметь:*** проводить анализ угроз, рисков, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть:*** навыками защиты ин-

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*		
			формации в компьютерных системах, навыками анализа защищенности локальной вычислительной сети.
		ПК-6.3 Согласовывает требования к программному обеспечению с заинтересованными сторонами.	***Знать:*** классификацию компьютерных вирусов, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, классификацию и архитектуру систем обнаружения атак, основные этапы аудита безопасности информационных систем, методы анализа и управления рисками, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь:*** 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 защищенных сайтов.
		ПК-6.4 Осуществляет оценку и согласование сроков выполнения поставленных задач	***Знать:*** нормативные документы в области защиты информационных ресурсов, в области разработки программных средств защиты информации, в области разработки аппаратных средств защиты информации, классификацию, состав, ТТХ и принципы работы аппаратно-программных средств для обеспечения информационной безопасности компьютерных си-

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*		
			стем и сетей, основные этапы аудита безопасности информационных систем, методы анализа и управления рисками, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь:*** применять требования нормативных документов в профессиональной деятельности, проводить анализ защищенности локальной вычислительной сети, разрабатывать защищенные сайты, проводить анализ информационных рисков. ***Владеть:*** навыками применения требований нормативных документов в области защиты информационных систем, навыками эксплуатации программных и аппаратных средств защиты информации, анализа и управления рисками, навыками разработки защищенных сайтов, программных средств обеспечения безопасности функционирования информационных систем и сетей.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Элективная дисциплина «Защита информации в компьютерных системах и сетях»» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы бакалавриата (специалитета, магистратуры) 02.03.03. Математическое обеспечение и администрирование информационных систем, направленность Математическое и информационное обеспечение экономической деятельности. Дисциплина изучается на 4 курсе в 7 семестре.

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

Общая трудоемкость (объем) дисциплины составляет 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	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.
2	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.
3	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно – программные системы идентификации и аутентификации.

4	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.
5	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.
6	Технологии анализа защищенности и обнаружения сетевых атак	Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования. Обзор современных средств обнаружения атак.
7	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.

8	Аудит безопасности информационных систем	Понятие аудита безопасности и цели его проведения. Стандарты, используемые при проведении аудита. Инициирование и планирование процедуры аудита. Сбор информации для аудита. Анализ данных аудита. Разработка рекомендаций. Подготовка отчетных документов. Анализ рисков и управление рисками. Оценка по верхним и нижним значениям. Оценка на основе выявления слабого звена. Оценка риска на основе рассмотрения этапов вторжения. Обзор программных продуктов для анализа и управления рисками: GRAMM, RiskWath, COBRA, ПО компании MethodWare, ПО "Аван Гард".
9	Разработка и защита Web-сайтов	Основы языка разметки документов HTML. Структура HTML -документа. Форматирование текста в HTML. Использование графики в HTML. Использование таблиц в HTML. Гиперссылки в HTML. Фреймы в HTML. Каскадные таблицы стилей CSS. Основы языка программирования JavaScript. Методы ввода и вывода информации в языке программирования JavaScript. Операторы в языке программирования JavaScript. Функции в языке программирования JavaScript. Обработчики событий в языке программирования JavaScript. Создание меню в языке программирования JavaScript. Окна в в языке программирования JavaScript. Формы в в языке программирования JavaScript.Защита информации с помощью аутентификации в языке программирования JavaScript. Защита контента от несанкционированного копирования информации в языке программирования JavaScript. Защита Web-сайта от DDoS – атак. Антивирусная защита Web-сайта.

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	Проблемы информационной безопасности сетей	2	-	-	У-1- 5, У-7, У-10, МУ-7	УО- 2	ПК-5

2	Политика безопасности	2	-	-	У-1- 5, У-7, У-10, МУ-7	УО - 4	ПК-5
3	Технологии аутентификации	2	-	-	У-1- 5, У-6, У-7, У-10, МУ-7	УО-6	ПК-5, ПК-6
4	Технологии межсетевых экранов	2	-	-	У-1-5,У-6, У-9, У-10, МУ-7	УО-8	ПК-5, ПК-6
5	Технологии защиты от вирусов	2	-	1	У-1- 5, У-8, У-9, У-10, МУ-4	УО-10, ЗПР - 6	ПК-6, ПК-5
6	Технологии анализа защищенности и обнаружения сетевых атак	2	-	2	У-1- 5, У-7, МУ-5	УО-12, ЗПР - 12	ПК-5, ПК-6
7	Требования к системам защиты информации	2	-	-	У-1- 5, У-6, У-9, У-10, МУ-7	УО - 14	ПК-5, ПК-6
8	Аудит безопасности информационных систем	2	1	-	У-1- 5, У-7, МУ-1	УО-16, ЗЛР - 6	ПК-5, ПК-6
9	Разработка и защита Web-сайтов	2	2, 3	3	У-1- 5, У-9-10, МУ-2, МУ-3, МУ-6	УО-18, ЗЛР – 16, 18, ЗПР-18	ПК-5, ПК-6
	Всего	18	18	18			

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

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Разработка обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	3
2	Создание сайтов на языке JavaScript и обеспечение их информаци-	3
3	Разработка и защита Web - приложений с серверными сценариями на языке PHP.	3
Итого		18

4.2.2 Практические занятия

Таблица 4.2.2 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
1	Менеджер паролей: программа Password Commander.	3
2	Фаервол Comodo Firewall.	3
3	Антивирусная программа: Kaspersky Internet Security	3
Итого		18

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Проблемы информационной безопасности сетей	2 неделя	4,9
2	Политика безопасности	4 неделя	5
3	Технологии аутентификации	6 неделя	6
4	Технологии межсетевых экранов	8 неделя	6
5	Технологии защиты от вирусов	10 неделя	6
6	Технологии анализа защищенности и обнаружения сетевых атак	12 неделя	6
7	Требования к системам защиты информации	14 неделя	6
8	Аудит безопасности информационных систем	16 неделя	7
9	Разработка и защита Web-сайтов	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	Практическая работа №1. Менеджер паролей: программа Password Commander	Анализ конкретных ситуаций	2
2	Практическая работа №2. Фаервол Comodo Firewall.	Анализ конкретных ситуаций	2
3	Практическая работа № 3. Антивирусная программа: Kaspersky Internet Security.Разработка и защита Web - приложений с клиентскими сцена-	Анализ конкретных ситуаций	2
Итого			6

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
ПК-5. Способность выбирать архитектуру и комплексирование современных компьютеров, систем, комплексов и сетей системного администрирования.	Проектирование информационных систем.	Операционные системы и оболочки. Инфокоммуникационные системы и сети. Администрирование информационных систем.	Защита информации в компьютерных системах и сетях. Сетевые технологии. Корпоративные информационные системы. Информационные системы предприятий. Администрирование информационных систем.
ПК-6. Способность использовать современные системные программные средства: операционные системы, операционные и сетевые оболочки, сервисные программы.	Операционные системы и оболочки	Программирование офисных приложений. Web-программирование.	Защита информации в компьютерных системах и сетях. Программирование офисных приложений. Сетевые технологии. Информационные системы предприятий. Администрирование информационных систем. Информационные системы менеджмента. Информационные системы маркетинга.

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
ПК-5, завершающий.	ПК-5.1 Определение базовых элементов конфигурации информационной системы.	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.
	ПК-5.2 Присвоение	Знать: методы защиты ин-	Знать: методы защиты	Знать: методы защиты

	версий базовым элементам конфигурации информационной системы.	формации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты.	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,
			Владеть: навыками применения программных	проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ПК-5.3 Установка базовых версий конфигурации информационной системы.	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 при-	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-

			менения 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.
ПК-6, завершающий.	ПК-6.1 Анализ возможности реализации требований к программному обеспечению.	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.
	ПК-6.2 Проведение оценки времени и трудоемкости реализации требований	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практи-	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять сред-	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной без-

	к программному обеспечению.	ческих задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	ства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	опасности. 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.
	ПК-6.3 Согласование требований к программному обеспечению с заинтересованными сторонами.	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.

	ПК-6.4 Осуществление оценки и согласования сроков выполнения поставленных задач.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

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	Проблемы информационной безопасности сетей	ПК-5	Лекция, СРС	Вопросы для устного опроса	1-12	Согласно таблице 7.2
2	Политика безопасности	ПК-5	Лекция, СРС	Вопросы для устного опроса	13-15	Согласно таблице 7.2
3	Технологии аутентификации	ПК-5, ПК-6	Лекция, СРС	Вопросы для устного опроса	16-21	Согласно таблице 7.2
4	Технологии межсетевых экранов	ПК-5, ПК-6	Лекция, СРС	Вопросы для устного опроса	22-24	Согласно таблице 7.2
5	Технологии защиты от вирусов	ПК-5, ПК-6	Лекция, практическая работа №, 1СРС	Вопросы для устного опроса	25-32	Согласно таблице 7.2
				КВЗПР №1	1-5	
6	Технологии анализа защищенности и обнаружения сетевых атак	ПК-5, ПК-6	Лекция, практическая работа №2, СРС	Вопросы для устного опроса	33-36	Согласно таблице 7.2
				КВЗПР №2	1-4	
7	Требования к системам защиты информации	ПК-5, ПК-6	Лекция, СРС	Вопросы для устного опроса	37-41	Согласно таблице 7.2

8	Аудит безопасности информационных систем	ПК-5, ПК-6	Лекция, лабораторная работа №1, СРС	Вопросы для устного опроса	42-45	Согласно таблице 7.2
				КВЗЛР №1	1-4	
9	Разработка и защита Web-сайтов	ПК-5, ПК-6	Лекция, лабораторные работы №2, №3, СРС	Вопросы для устного опроса	46-48	Согласно таблице 7.2
				КВЗЛР №2	1-4	
				КВЗЛР №3	1-4	

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

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Проблемы информационной безопасности сетей».

1. Классификация угроз информационной безопасности автоматизированных систем.

2. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.

3. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: подслушивание (sniffing), подмена доверенного субъекта (IP – spoofing), посредничество в обмене незашифрованными ключами (Man-in-the-Middle).

4. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: перехват сеанса (Session hijacking), отказ в обслуживании (Denial of Service, DoS), парольная атака полного перебора (brute force attack).

5. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.

6. Основные характеристики спама и методы борьбы с ним.

7. Виды интернет - мошенничества: фишинг и фарминг и методы борьбы с ними.

8. Угрозы и уязвимости проводных корпоративных сетей.

9. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: вещание радиомаяка, обнаружение WLAN, подслушивание, ложные точки доступа в сеть.

10. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: отказ в обслуживании, атаки типа " человек в середине", атака подмены ARP-записей, анонимный доступ в Интернет.

11. Способы обеспечения информационной безопасности компьютерных сетей. Фрагментарный и комплексный подходы.

12. Пути решения проблем защиты информации в сети Интернет. Информационная безопасность электронного бизнеса.

Контрольные вопросы для защиты практической работы №1:

1. Типы паролей, создаваемые с помощью генератора паролей
2. Пасскарта в программе Password Commander
3. Программы, предназначенные для хранения паролей
4. Аккаунт в программе Password Commander

Контрольные вопросы для защиты лабораторной работы №1

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

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 зачета. Зачет 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 сетевая атака связана с превышением допустимых пределов функционирования сети:

А) Отказ в обслуживании (DoS –атака).
Б) Подслушивание (Sniffing).
В) Атака Man in – the – Middle (человек в середине).
Г) Угадывание ключа.

Задание в открытой форме:

1. Для беспроводных сетей характерной сетевой атакой является ……..

2. Основной защитой от фишинга являются ……..

3. К видам систем идентификации и аутентификации относятся …….

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:

Для кодирования последовательности, состоящей из букв А, Б, В, Г и Д, используется неравномерный двоичный код.

Для букв А, Б, В и Г использованы кодовые слова:

А-111

Б-110

В-101

Г-100

Укажите, каким кодовым словом может быть закодирована буква Д.

(Код должен удовлетворять свойству однозначного декодирования. Если можно использовать более одного кодового слова, указать кратчайшее).

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 «Менеджер паролей: программа Password Commander»	3	Выполнил, доля правильных ответов от 50% до 90%	7	Выполнил, доля правильных ответов более 90%
Практическая работа №2 «Настройка межсетевого экрана Comodo Firewall.»	3	Выполнил, доля правильных ответов от 50% до 90%	7	Выполнил, доля правильных ответов более 90%
Практическая работа №3 «Антивирусная программа: Kaspersky Internet Security.»	3	Выполнил, доля правильных ответов от 50% до 90%	7	Выполнил, доля правильных ответов более 90%
Лабораторная работа №1 «Разработка обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	4	Выполнил, доля правильных ответов от 50% до 90%	7	Выполнил, доля правильных ответов более 90%
Лабораторная работа №2 «Создание сайтов на языке JavaScript и обеспечение их информационной безопасности»	4	Выполнил, доля правильных ответов от 50% до 90%	7	Выполнил, доля правильных ответов более 90%
Лабораторная работа №3 «Разработка и защита Web - приложений с серверными сценариями на языке PHP.»	4	Выполнил, доля правильных ответов от 50% до 90%	7	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. Сети и телекоммуникации [Текст]: учебник / К. Е. Самуйлов [и др.] - М : Юрайт, 2019. -363 с.
2. Информационная безопасность [Текст]: учебное пособие / А. Г. Спеваков [и др.] – Курск : ЮЗГУ, 2017. - 196 с.
3. 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
4. Разработка защищённых корпоративных систем на базе клиент-серверной технологии [Текст] : учебное пособие / А. Л. Марухленко [и др.]- Курск : Университетская книга, 2018. - 176 с.
5. Безопасность сетей [Электронный ресурс] / Э.В. Мэйволд, М : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.

8.2 Дополнительная учебная литература

6. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.
7. Заика А. Компьютерная безопасность [Электронный ресурс] / А. Заика. - М. : РИПОЛ классик, 2013. - 160 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=227317
8. Пархимович М.Н. Основы интернет-технологий [Электронный ресурс]: учебное пособие / М.Н. Пархимович, А.А. Липницкий, В.А. Некрасова - Архангельск : ИПЦ САФУ, 2013. - 366 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=436379

9. Громов Ю.Ю. Основы Web-инжиниринга: разработка клиентских приложений [Электронный ресурс]: учебное пособие / Ю.Ю. Громов, О.Г. Иванова, С.В. Данилкин . - Тамбов : Изд -во ФГБОУ ВПО «ТГТУ», 2012. - 240 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=277648

10. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. - 2-е изд., стереотип. - М. : ФЛИНТА, 2011. - 269 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=93245

8.3 Перечень методических указаний

1. Разработка обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс]: методические указания по выполнению лабораторных работ для студентов направления подготовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост. А.Л. Ханис. - Курск : ЮЗГУ, 2021. - 6 с.
2. Создание сайтов на языке JAVASCRIPT и обеспечение их информационной безопасности : методические указания по выполнению лабораторных работ для студентов направления подготовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост. А.Л. Ханис. - Курск : ЮЗГУ, 2021. - 41 с.
3. Разработка и защита web-приложений с серверными сценариями на языке PHP : методические указания по выполнению лабораторных работ для студентов направления подготовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост. А.Л. Ханис. - Курск : ЮЗГУ, 2021. - 32 с.
4. Менеджер паролей: программа Password Commander : [Электронный ресурс] : методические указания по выполнению практических занятий по дисциплинам «Защита информационных процессов в компьютерных системах» для студентов направления подготовки бакалавров 10.03.01, специальности 38.05.01, «Информационная безопасность» для студентов направлений подготовки бакалавров 09.03.02, 09.03.03и лабораторных работ по дисциплине «Информационная безопасность» для студентов направлений подготовки бакалавров 45.03.03, «Методы и средства защиты компьютерной информации», для студентов направления подготовки бакалавров 09.03.04. / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2017. - 18 с.
5. 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. - Курск : ЮЗГУ, 2021. - 15 с.
6. Антивирусная программа: Kaspersky Internet Security: методические указания по выполнению практических работ для студентов направления под-

готовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост. А.Л. Ханис. - Курск : ЮЗГУ, 2021. - 14 с.

7. Защита информации в компьютерных системах и сетях: методические указания для самостоятельной работы по изучению дисциплины для направления подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем» / Юго-Зап. гос. ун-т ; сост. А.Л. Ханис. - Курск : ЮЗГУ, 2019. - 17 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].

Основными видами аудиторной работы студента при изучении дисциплины «Защита информационных процессов в компьютерных системах» 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 «Защита информационных процессов в компьютерных системах» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Защита информационных процессов в компьютерных системах» - 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 хранения паролей Password Commander http://pascom.ru/ download, бесплатная версия).

Фаервол Comodo Firewall (http://personalfirewall.comodo.com/, бесплатная версия).

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

Apache (https://httpd.apache.org/, бесплатная, GNU General Public License)

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: ноут-6yKASUSX50VLPMD-T2330/14'71024Mb/160Gb/cyMKa/npoeKTop 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
	Измененных	Заменённых	Аннулированных	новых			