Аннотация к рабочей программе дисциплины «Защита информационных процессов в компьютерных системах»

Цель преподавания дисциплины

Целью преподавания дисциплины «Защита информационных процессов в компьютерных системах» 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-1.1 Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности.

ПК-1.2 Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности.

ПК-1.3 Выполняет регламентные работы по эксплуатации средств защиты информации.

ПК-1.4 Устраняет неисправности при эксплуатации средств защиты информации

ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах.

ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности.

ПК-2.3 Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД.

ПК-2.4 Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД

ПК-2.5 Устанавливает программное обеспечение в соответствии с требованиями по защите информации

Разделы дисциплины

Проблемы информационной безопасности сетей. Политика безопасности. Технологии аутентификации. Технологии межсетевых экранов

Технологии защиты от вирусов. Технологии анализа защищенности и обнаружения сетевых атак. Требования к системам защиты информации. Аудит безопасности информационных систем. Разработка и защита Web-сайтов.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» августа 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информационных процессов в компьютерных системах

(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность

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

направленность (профиль, специализация) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»

наименование направленности (профиля, специализации)

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Защита информационных процессов в компьютерных системах составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 10.03.01. Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01. Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины Защита информационных процессов в компьютерных системах обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01. Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий на заседании кафедры информационной безопасности Протокол № 1
«30» 08 2021 г.

Зав. кафедрой Таныгин М.О.
Разработчик программы
к.воен.н., доцент Ханис А.Л.
Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Защита информационных процессов в компьютерных системах пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01. Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета протокол №6 «26» 02 2021 г., на заседании кафедры ИБ №11 от 30.06.22 г.
(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 информационных процессов в компьютерных системах» 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

Таблица 1.3 – Результаты обучения по дисциплине

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

ПК-1	Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем.	ПК-1.1 Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности.	***Знать:*** классификацию угроз информационной безопасности (ИБ) в автоматизированных системах (АС); причины, виды и каналы утечки информации в АС; способы защиты операционных систем, классификацию систем защиты программного обеспечения (ПО); методы идентификации и установления подлинности пользователей и объектов, типы аутентификации и межсетевых экранов, способы их реализации; классификацию компьютерных вирусов, виды антивирусных программ; средства анализа защищённости АС; перечень мероприятий по защите информации от вирусов; этапы внедрения и отладки программно-аппаратных средств защиты информации в АС. ***Уметь:*** реализовывать контроль доступа средствами АС и аудит потоков данных; использовать средства аутентификации АС; применять одноразовые пароли, шифрование паролей и данных, определять уязвимые места в прикладном ПО, устанавливать программы защиты приложений, контролировать ресурсы оборудования АС; использовать антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); использовать средства анализа защищённости АС (сканеры безопасности); системы обнаружения сетевых атак; применять средства защиты информации в АС, проводить анализ информационных рисков. ***Владеть:*** навыками внедрения и отладки программных средств защиты АС; установки и эксплуатации средств анализа защищённости АС (сканеров безопасности); систем обнаружения сетевых атак;

			реализации контроля доступа и аудита, использования антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов); определения уязвимых мест в прикладном ПО, контроля ресурсов оборудования АС.
		ПК-1.2 Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности.	***Знать***: технические характеристики и особенности функционирования программно-аппаратных средств ЗИ в АС; перечень и объём мероприятий по обеспечению безопасности и защищённости АС, виды угроз АС, типы, виды, назначение средств защиты информации в АС; состав, характеристики, назначение, функции оборудования АС; классификацию антивирусного ПО, способы настройки сетевых экранов. ***Уметь:*** проводить анализ угроз, рисков АС, осуществлять выбор оборудования и средств защиты АС в соответствии с решаемыми АС задачами, классифицировать средства защиты исходя из функционала АС, определять состав средств защиты для обеспечения выполнения задач АС; применять программные средства защиты сетевого оборудования, антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть:*** навыками анализа функциональных возможностей оборудования и средств защиты АС, технических характеристик сетевого оборудования и программно-аппаратных средств ЗИ в АС; выбора и эксплуатации средств ЗИ в АС в соответствии с функциональными задачами АС, настройки сетевых экранов, установки ПО, разработки защищённых сайтов.

		ПК-1.3 Выполняет регламентные работы по эксплуатации средств защиты информации.	***Знать:*** типы регламентных работ, классификацию программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств защиты информации (СЗИ); эксплуатационную документацию, возможные угрозы и методики определения рисков, порядок настройки сетевого и программного оборудования и режимы функционирования. ***Уметь:*** проводить анализ защищенности АС; использовать программные и аппаратные средств анализа защищённости АС, системы обнаружения сетевых атак, антивирусное ПО, настраивать межсетевое оборудование. ***Владеть:*** навыками эксплуатации программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; программных средств анализа и управления рисками, навыками настройки сетевых экранов, разработки защищенных сайтов.
		ПК-1.4 Устраняет неисправности при эксплуатации средств защиты информации	***Знать:*** назначение и классификацию программно-аппаратных средств АС; особенности функционирования ПО АС; классификацию программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств защиты информации (СЗИ); эксплуатационную документацию. ***Уметь:*** проводить мониторинг

			безопасности АС; обнаруживать уязвимые места в функционировании ПО и аппаратного оборудования АС; провести настройку ПО и оборудования АС. ***Владеть:*** навыками настройки программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; программных средств анализа и управления рисками, навыками разработки защищенных сайтов.
ПК-2	Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности.	ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах.	***Знать:*** требования действующих стандартов и рекомендаций, определяющих критерии оценки безопасности АС и этапы анализа рисков и угроз безопасности и уязвимости АС; классификацию общих критериев, пути организации общих критериев; требования к разработке должностных инструкций; порядок эксплуатации программно-аппаратных средств защиты АС; основные принципы построения политики безопасности; методы и способы защиты информации в АС, методы анализа угроз и оценки рисков информационной безопасности АС. ***Уметь:*** применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в АС; разрабатывать служебную и техническую документацию; применять средства защиты информации в соответствии с заданными требованиями к АС; проводить анализ информационных рисков. ***Владеть:*** навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности

			обработки информации в АС; разработки служебной и технической документации; программных средств защиты информации, разработки архитектуры сетевой защиты.
		ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности.	***Знать:*** виды угроз и каналы утечки информации, состав, структуру, требования и принципы построения политики безопасности; модели и типы политик безопасности; состав, технические характеристики и правила эксплуатации программно-аппаратных средств АС; основные элементы политики безопасности, методы управления доступом, средства идентификация и аутентификация, анализа регистрационной информации; требования к технической, должностной и эксплуатационной документации; требования к уровням надёжности (безопасности); основные виды сетевых атак. ***Уметь:*** проводить анализ угроз, рисков, разрабатывать документацию пользователя, администратора сети, применять тестовые программы, разрабатывать архитектуры АС, разрабатывать политики безопасности; применять средства защиты информации в АС, проводить анализ защищенности АС, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть:*** навыками разработки документации пользователя, администратора сети, разработки и применения тестовых программ, описания архитектуры, описания политики безопасности; защиты информации в компьютерных системах, навыками анализа

			защищенности АС, применения антивирусных программных комплексов, настройки режимов работы межсетевых экранов.
		ПК-2.3 Определяет состав средств, необходимый для управления автоматизированным и системами и средствами их защиты от НСД.	***Знать:*** требования руководящих документов по защите АС от НСД; классификацию средств и АС по уровню защищённости от НСД; требования к защищённости АС; показатели и классы защищённости межсетевых экранов от НСД к информации; классификацию ПО СЗИ, требования руководящих документов к составу и содержанию документаций и испытаний ПО СЗИ; механизмы управления ключами, шифрованием, администрирования управления доступом, аутентификацией, маршрутизацией; задачи и методы управления системой защиты АС; типы, состав, назначение, способы применения современных систем управления защитой АС; принципы организации управления безопасностью АС; функции управления правами доступа пользователей АС, информационным каталогом, правилами политики безопасности; цели, задачи и порядок проведения аудита безопасности АС; программные средства мониторинга безопасности АС; состав, характеристики серверного, пользовательского и сетевого оборудования АС; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь:*** проводить анализ защищенности локальной вычислительной сети, определять текущее состояние оборудования АС; применять

			программно-аппаратные средства ЗИ в АС; классифицировать программные продукты управления в соответствии с задачами АС, подбирать конфигурацию ситемы управления безопасности АС; проводить анализ информационных рисков. ***Владеть:*** навыками определения задач АС, классификации оборудования АС (серверов, АРМ, рабочих станций, сетевое оборудование), установки ПО серверной и клиентской части, настройки систем управления доступом, эксплуатации программных средств мониторинга и управления средствами безопасности АС, определения уязвимых мест АС и выбора средств защиты от НСД.
		ПК-2.4 Определяет порядок настройки технических средств для управления автоматизированным и системами и средствами их защиты от НСД	***Знать:*** классификацию, состав, ТТХ и принципы работы аппаратно-программных средств и систем для обеспечения защиты АС от НСД, основные требования к системам управления СЗИ от НСД; показатели защищенности средств вычислительной техники АС от несанкционированного доступа, классы защищенности АС. ***Уметь:*** выполнять требования руководящих документов, эксплуатационной документации, проводить анализ защищенности АС, применять средства и системы управления средствами защиты АС от НСД; определять уязвимые узлы АС; разрабатывать защищенные сайты, проводить анализ информационных рисков. ***Владеть:*** навыками настройки и эксплуатации программных и аппаратных средств и систем управления средствами защиты АС от НСД.

		ПК-2.5 Устанавливает программное обеспечение в соответствии с требованиями по защите информации	***Знать:*** причины, виды и каналы утечки информации в АС; способы защиты операционных систем, классификацию систем защиты программного обеспечения (ПО); типы аутентификации и межсетевых экранов, способы их реализации; виды антивирусных программ; средства анализа защищённости АС; алгоритм установки и отладки ПО защиты информации в АС. ***Уметь:*** устанавливать программы защиты приложений, антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); средства анализа защищённости АС (сканеры безопасности); системы обнаружения сетевых атак; применять средства защиты информации в АС. ***Владеть:*** навыками внедрения и отладки программных средств защиты АС; установки и эксплуатации средств анализа защищённости АС (сканеров безопасности); систем обнаружения сетевых атак; реализации контроля доступа и аудита, установки антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов), контроля ресурсов оборудования АС.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита информационных процессов в компьютерных системах» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы бакалавриата (специалитета, магистратуры) 10.03.01. Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и

коммуникационных технологий». 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 5 зачетных единиц (з.е.), 180 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	90
в том числе:	
лекции	36
лабораторные занятия	54, из них практическая подготовка 4
практические занятия	0
Самостоятельная работа обучающихся (всего)	61,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

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

4.1 Содержание дисциплины

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

№ п/п	Раздел, (тема) дисциплины	Содержание

1	2	3
1	Проблемы информационной безопасности автоматизированных 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	Классификация компьютерных вирусов. Загрузочные

	вирусов	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	4	-	-	У-1- 6 МУ-6	УО- 2	ПК-1, ПК-2
2	Политика безопасности	4	-	-	У-1- 6 МУ-6	УО - 4	ПК-2
3	Технологии аутентификации	4	-	-	У-1- 6 МУ-6	УО-6	ПК-1, ПК-2
4	Технологии межсетевых экранов	4	-	-	У-1- 6 МУ-6	УО-8	ПК-1, ПК-2

5	Технологии защиты от вирусов	4	3	-	У-1- 6, МУ-3,6	Ситуационная задача УО-10, ЗЛР - 10	ПК-1, ПК-2
6	Технологии анализа защищенности и обнаружения сетевых атак	4	4	-	У-1- 6, МУ-4,6	Ситуационная задача УО-12, ЗЛР - 12	ПК-1, ПК-2
7	Требования к системам защиты информации	4	5	-	У-1- 6, МУ-5,6	Ситуационная задача УО – 14, ЗЛР - 14	ПК-1, ПК-2
8	Аудит безопасности информационных систем	4	1	-	У-1- 6 МУ-1,6	Ситуационная задача УО-16, ЗЛР - 16	ПК-1, ПК-2
9	Разработка и защита Web-сайтов	4	2		У-1- 6 МУ-2,6	Ситуационная задача УО-18, ЗЛР – 18	ПК-1, ПК-2
	Всего	36					

УО – устный опрос, ЗЛР – лабораторная работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Создание сайтов на языке JavaScript и обеспечение их информационной безопасности	12
2	Разработка и защита Web - приложений с серверными сценариями на языке PHP.	12, из них практическая подготовка 4
3	Менеджер паролей: программа Password Commander.	10
4	Фаервол Comodo Firewall.	10
5	Антивирусная программа: Kaspersky Internet Security.	10
Итого		54

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	5,85
2	Политика безопасности	4 неделя	7
3	Технологии аутентификации	6 неделя	7
4	Технологии межсетевых экранов	8 неделя	7
5	Технологии защиты от вирусов	10 неделя	7
6	Технологии анализа защищенности и обнаружения сетевых атак	12 неделя	7
7	Требования к системам защиты информации	14 неделя	7
8	Аудит безопасности информационных систем	16 неделя	7
9	Разработка и защита Web-сайтов	18 неделя	7
Итого			61,85

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

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

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

библиотекой университета:

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

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

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

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

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к экзамену;

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

типографией университета:

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

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

6. Образовательные технологии. Практическая подготовка обучающихся. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования 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	Создание сайтов на языке JavaScript и обеспечение их информационной безопасности	Анализ конкретных ситуаций	4
2	Разработка и защита Web - приложений с серверными сценариями на языке PHP.	Анализ конкретных ситуаций	4
3	Менеджер паролей: программа Password Commander.	Анализ конкретных ситуаций	4
4	Фаервол Comodo Firewall.	Анализ конкретных ситуаций	4
5	Антивирусная программа: Kaspersky Internet Security.	Анализ конкретных ситуаций	2
Итого			18

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю, специализации) программы бакалавриата.

Практическая подготовка обучающихся при реализации дисциплины организуется в реальных производственных условиях в профильных организациях.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181 (в РПД по ОПОП ВО медицинского образования следует указать положение П 02.189).

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 профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

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

– 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
ПК-1. Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем.	Специализированные вычислительные устройства защиты информации. Организация автоматизированных систем.	Специализированные вычислительные устройства защиты информации. Организация автоматизированных систем.	Защита информационных процессов в компьютерных системах Специализированные вычислительные устройства защиты информации. Организация автоматизированных систем. Производственная технологическая практика.
ПК-2. Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности.	Системы охраны и инженерной защиты информации.	Системы охраны и инженерной защиты информации.	Защита информационных процессов в компьютерных системах Производственная технологическая практика.

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции / этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ПК-1, завершающий.	ПК-1.1 Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности.	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	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

			защищенных сайтов.	защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ПК-1.2 Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности.	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	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-1.3 Выполняет регламентные работы по эксплуатации средств защиты 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. 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-1.4 Устраняет неисправности при эксплуатации средств защиты информации.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности.

		задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	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-2, завершающий.	ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты	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 защищенные сайты,

		информации.	Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности.	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-2.3 Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД.	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-2.4 Определяет порядок настройки технических средств для	Знать: методы защиты информации. Уметь: применять	Знать: методы защиты информации, способы защиты сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков

	управления автоматизированными системами и средствами их защиты от НСД.	средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	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.	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-2.5 Устанавливает программное обеспечение в соответствии с требованиями по защите информации.	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать	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

		применения программных средств защиты информации.	защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	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-1, ПК-2	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
2	Политика безопасности	ПК-2	Лекция, СРС	Вопросы для устного опроса	11-20	Согласно таблице 7.2

3	Технологии аутентификации	ПК-1, ПК-2	Лекция, СРС	Вопросы для устного опроса	21-30	Согласно таблице 7.2
4	Технологии межсетевых экранов	ПК-1, ПК-2	Лекция, СРС	Вопросы для устного опроса	31-40	Согласно таблице 7.2
5	Технологии защиты от вирусов	ПК-1, ПК-2	Лекция, лабораторная работа №3, СРС	Вопросы для устного опроса	41-50	Согласно таблице 7.2
				КВЗЛР №3 Ситуационная задача	1-10 1-15	
6	Технологии анализа защищенности и обнаружения сетевых атак	ПК-1, ПК-2	Лекция, лабораторная работа №4, СРС	Вопросы для устного опроса Ситуационная задача	51-60 1-15	Согласно таблице 7.2
				КВЗЛР №4	1-10	
7	Требования к системам защиты информации	ПК-1, ПК-2	Лекция, лабораторная работа №5, СРС	Вопросы для устного опроса	61-70	Согласно таблице 7.2
				КВЗЛР №5 Ситуационная задача	1-10 1-15	
8	Аудит безопасности информационных систем	ПК-1, ПК-2	Лекция, лабораторная работа№1 СРС	Вопросы для устного опроса	71-80	Согласно таблице 7.2
				КВЗЛР №1 Ситуационная задача	1-10 1-15	
9	Разработка и защита Web-сайтов	ПК-1, ПК-2	Лекция, лабораторные работы №2, СРС	Вопросы для устного опроса	81-90	Согласно таблице 7.2
				КВЗЛР №2 Ситуационная задача в т.ч. для контроля результатов практической подготовки	1-10 1-15	

СРС – самостоятельная работа студента,
КВЗЛР – контрольные вопросы для защиты лабораторных 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.

Контрольные вопросы для защиты лабораторной работы №4:

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

Производственная задача для контроля результатов практической подготовки обучающихся на лабораторном занятии №2

Создайте тест, состоящий из пяти вопросов (файл test.htm). После выбора правильных ответов, данные передаются в новый файл analyse_test.php, где вычисляется количество правильных ответов и выводится соответствующее сообщение. Обратите внимание, при ответе пользователь мог специально или случайно пропустить вопрос, поэтому перед проверкой каждого ответа на правильность нужно проверить, а передана ли соответствующая переменная в php-файл.

Ситуационная задача

Компания X разрабатывает приложение для хранения и обработки конфиденциальных данных своих клиентов. Какие меры безопасности должны быть предприняты для защиты этих данных? Какие риски могут возникнуть при неправильной реализации мер безопасности?

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 экзамена. Экзамен проводится в виде компьютерного 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.

Результаты практической подготовки *(умения, навыки (или опыт деятельности) и компетенции)* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

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.

Расположите в правильном порядке уровни модели ISO взаимодействия открытых систем (Open System Interconnect), пронумеровав уровни от нижнего до верхнего от 1 до 7:

транспортный =

физический =

канальный =

сетевой =

представления данных =

прикладной =

сеансовый =

Задание на установление соответствия:

Установите соответствие между указанными в списке названиями и определениями режимов передачи данных:

а) полнодуплексный (Full Duplex)

б) полудуплексный (Half Duplex)

в) симплексный (Simplex)

Компетентностно-ориентированная задача:

Создайте PHP-страницу, в которой пользователь вводит в форму количество строк и количество столбцов. В результате по введенным значениям строится таблица.

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	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 4-6	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 7-9	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Решение ситуационных задач	8	Выполнил, доля правильных ответов от 50% до 90%	16	Выполнил, доля правильных ответов от 50% до 90%

Лабораторная работа №1 «Создание сайтов на языке JavaScript и обеспечение их информационной безопасности»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №2 «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%
Лабораторная работа №3 «Менеджер паролей: программа Password Commander»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4 «Настройка межсетевого экрана Comodo Firewall»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Лабораторная работа №5 «Антивирусная программа: Kaspersky Internet Security»	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. Сети и телекоммуникации : учебник и практикум для академического бакалавриата : [для студентов вузов, обучающихся по специальности 10.05.02 "Информационная безопасность телекоммуникационных систем"] / под ред.: К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва : Юрайт, 2019. - 363 с. - Текст : непосредственный.

8.2 Дополнительная учебная литература

2. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

3. Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие / А. Щербаков. – Москва : Книжный мир, 2009. – 352 с. – (Высшая школа). –. – URL: https://biblioclub.ru/index.php?page=book&id=89798 (дата обращения: 24.08.2021). – Режим доступа: по подписке. – Текст : электронный.

4. 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

5. 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

6. 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. Создание сайтов на языке JavaScript и обеспечение их информационной безопасности : методические указания по выполнению лаборатор-ных работ для студентов укрупненной группы специальностей и направ-лений подготовки 10.00.00 / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 70 с.: ил. 12, табл. 1. – Библиогр.: с. 70.

2. Разработка и защита Web-приложений с серверными сценария-ми на языке PHP : методические указания по выполнению лабораторных работ для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 33 с.: ил. 2, табл. 1. – Библиогр.: с. 33.

3. Менеджер паролей: программа Password Commander : методиче-ские указания по выполнению лабораторных работ для студентов укруп-ненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 16 с.: ил. 8, Библиогр.: с. 16.

4. Фаервол Comodo Firewall : методические указания по выполне-нию лабораторных работ для студентов укрупненной группы специально-стей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 15 с.: ил. 8, Библиогр.: с. 15.

5. Антивирусная программа: Kaspersky Internet Security : методиче-ские указания по выполнению лабораторных работ для студентов укруп-ненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 14 с.: ил. 8, Библиогр.: с. 14.

6. Защита информационных процессов в компьютерных системах: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 20с.: Библиогр.: с. 20.

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 «Защита информационных процессов в компьютерных системах» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

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

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

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

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

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-букASUSX50VLPMD-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
	Изме-нённых	Заменённых	Аннулированных	новых			