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

Цель преподавания дисциплины

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.

Компетенции, формируемые в результате освоения дисциплины

способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

- способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

- способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

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

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

«2» 02 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информационных процессов в компьютерных системах
(наименование дисциплины)

направление подготовки (специальность) 10.03.01
(шифр согласно ФГОС

Информационная безопасность
и наименование направления подготовки (специальности))

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

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

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 «Информационная безопасность» и на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол № 5 от «30» 01 2017г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» на заседании кафедры информационной безопасности, протокол № 9 «1» 02 2017г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ М. О. Таныгин

Разработчик программы
к.т.н., доцент _____ К. А. Тезик
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ В.Г. Макаровская

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол № 1 «28» 08 2017г. на заседании кафедры ИБ
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры ИБ, 29.03.2018, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол № _ «__» _____ 20_ г. на заседании кафедры ИБ, 27.06.2019, протокол №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения 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

Основными обобщенными задачами дисциплины являются:

- 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 образовательной программы

Обучающиеся должны **знать**:

- виды угроз и возможные каналы утечки конфиденциальной информации;
- основные принципы построения политики информационной безопасности;
- основные виды сетевых атак и методы противодействия им;
- методы аутентификации и принципы работы аппаратно – программных систем идентификации и аутентификации;
- функции и классификацию межсетевых экранов;
- 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 возможных угроз, потенциальных рисков и в связи с этим обоснованно предлагать оптимальный вариант архитектуры сетевой защиты;
- правильно эксплуатировать антивирусные программные комплексы;
- предлагать конкретные меры по усилению парольной защиты;
- настраивать режимы работы межсетевых экранов;
- проводить анализ защищенности локальной вычислительной сети;
- разрабатывать защищенные сайты с использованием языков HTML, JavaScript, PHP;
- проводить анализ информационных рисков.

владеть:

- высокой мотивацией к выполнению профессиональной деятельности;
- навыками защиты информации в компьютерных системах;
- навыками анализа защищенности локальной вычислительной сети;

- навыками эксплуатации программных средств анализа и управления рисками;
- навыками разработки защищенных сайтов;

В процессе изучения дисциплины «Защита информационных процессов в компьютерных системах» происходит формирование следующих профессиональных компетенций:

- способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
- способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);
- способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

2. Указание места дисциплины в структуре образовательной программы

«Защита информационных процессов в компьютерных системах» представляет дисциплину с индексом Б1. Б. 36 базовой части учебного плана направления подготовки 10.03.01 Информационная безопасность, изучаемую на 4 курсе в 7 семестре.

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

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (з.е.), 144 академических часа.

Таблица 3 –Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54
в том числе:	
лекции	18
лабораторные занятия	36
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 - 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: фи-

		зическая 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 4.2 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- 6 МУ-6	УО- 2	ПК-4, ПК-6, ОПК-7
2	Политика безопасности	2	-	-	У-1- 6 МУ-6	УО - 4	ПК-4, ПК-6, ОПК-7
3	Технологии аутентификации	2	-	-	У-1- 6 МУ-6	УО-6	ПК-4, ПК-6, ОПК-7
4	Технологии межсетевых экранов	2	-	-	У-1- 6 МУ-6	УО-8	ПК-4, ПК-6, ОПК-7
5	Технологии защиты от вирусов	2	3	-	У-1- 6, МУ-3,6	УО-10, ЗЛР - 10	ПК-4, ПК-6, ОПК-7
6	Технологии анализа защищенности и обнаружения сетевых атак	2	4	-	У-1- 6, МУ-4,6	УО-12, ЗЛР - 12	ПК-4, ПК-6, ОПК-7
7	Требования к системам защиты информации	2	5	-	У-1- 6, МУ-5,6	УО – 14, ЗЛР - 14	ПК-4, ПК-6, ОПК-7
8	Аудит безопасности информационных систем	2	1	-	У-1- 6 МУ-1,6	УО-16, ЗЛР - 16	ПК-4, ПК-6, ОПК-7
9	Разработка и защита Web-сайтов	2	2		У-1- 6 МУ-2,6	УО-18, ЗЛР – 18	ПК-4, ПК-6, ОПК-7
	Всего	18					

УО – устный опрос, ЗЛР – лабораторная работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.3 - Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Создание сайтов на языке JavaScript и обеспечение их информационной безопасности	6
2	Разработка и защита Web - приложений с серверными сценариями на языке PHP.	6
3	Менеджер паролей: программа Password Commander.	8
4	Фаервол Comodo Firewall.	8
5	Антивирусная программа: Kaspersky Internet Security.	8
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.5 - 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 УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– вопросов 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

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 19 декабря 2013 г. № 1367 по направлению подготовки 10.03.01 «Информационная безопасность», реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 25 % от аудиторных занятий согласно УП.

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	**Лабораторная работа №1**. Анализ и управление информационными рисками в программе “Гриф”.	Анализ конкретных ситуаций	4
2	**Лабораторная работа №2**. Разработка Web - приложений на языке HTML.	Анализ конкретных ситуаций	4
3	**Лабораторная работа № 3**. Разработка и защита Web - приложений с клиентскими сценариями на языке JavaScript.	Анализ конкретных ситуаций	4
4	**Лабораторная работа № 4**. Разработка и защита Web - приложений с серверными сценариями на языке PHP.	Анализ конкретных ситуаций	6
Итого			18

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 − Этапы формирования компетенций

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	Введение в направление подготовки и планирование профессиональной карьеры	Основы управления информационной безопасностью	Защита информационных процессов в компьютерных системах; Защита и обработка конфиденциальных документов;

объекта защиты (ПК-4).			Сети и системы передачи информации (специальные разделы); Беспроводные сети связи; Эксплуатационная практика;
Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6).	Методы защиты программного обеспечения; Основы риверсинжиниринга программных средств		Программно-аппаратные средства защиты информации; Техническая защита информации; Защита информационных процессов в компьютерных системах; Эксплуатационная практика;
Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).	Методы защиты информации, способы защиты сайтов, угрозы безопасности информации, пути их реализации.		Программно-аппаратные средства защиты информации; Техническая защита информации; Защита информационных процессов в компьютерных системах; Эксплуатационная практика;

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	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)

1	2	3	4	5
ПК-4/ завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	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/ завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в обла-	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в обла-	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

	знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	сти информационной безопасности. Владеть: навыками применения программных средств защиты информации.	сти информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов	области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты
ОПК-7/ завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	Знать: угрозы безопасности 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, угрозы безопасности информации, пути их реализации. 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 образовательной программы**

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля

№ 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-4, ПК-6, ОПК-7	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
2	Политика безопасности	ПК-4, ПК-6, ОПК-7	Лекция, СРС	Вопросы для устного опроса	11-20	Согласно таблице 7.2
3	Технологии аутентификации	ПК-4, ПК-6, ОПК-7	Лекция, СРС	Вопросы для устного опроса	21-30	Согласно таблице 7.2
4	Технологии межсетевых	ПК-4, ПК-6, ОПК-7	Лекция, СРС	Вопросы для устного опроса	31-40	Согласно таблице 7.2

	экранов					
5	Технологии защиты от вирусов	ПК-4, ПК-6, ОПК-7	Лекция, лабораторная работа №3, СРС	Вопросы для устного опроса	41-50	Согласно таблице 7.2
				КВЗЛР №3	1-10	
6	Технологии анализа защищенности и обнаружения сетевых атак	ПК-4, ПК-6, ОПК-7	Лекция, лабораторная работа №4, СРС	Вопросы для устного опроса	51-60	Согласно таблице 7.2
				КВЗЛР №4	1-10	
7	Требования к системам защиты информации	ПК-4, ПК-6, ОПК-7	Лекция, лабораторная работа №5, СРС	Вопросы для устного опроса	61-70	Согласно таблице 7.2
				КВЗЛР №5	1-10	
8	Аудит безопасности информационных систем	ПК-4, ПК-6, ОПК-7	Лекция, лабораторная работа№1 СРС	Вопросы для устного опроса	71-80	Согласно таблице 7.2
				КВЗЛР №1	1-10	
9	Разработка и защита Web-сайтов	ПК-4, ПК-6, ОПК-7	Лекция, лабораторные работы №2, СРС	Вопросы для устного опроса	81-90	Согласно таблице 7.2
				КВЗЛР №2	1-10	

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

Ситуационная задача

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.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. кзамен 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.

Умения, навыки 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:

Под политикой безопасности организации понимают:

1. Совокупность документированных управленческих решений, направленных на защиту информации.
2. Совокупность юридических законов в области защиты информации.

3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание в открытой форме:

Основные угрозы безопасности при работе с распределенными системами включают атаки на …

Задание на установление правильной последовательности,

Установите правильную последовательность этапов реализации контроля доступа в распределенных системах:

a) Идентификация пользователей и ресурсов;

b) Аутентификация пользователей и авторизация доступа к ресурсам;

c) Установка прав доступа;

d) Мониторинг доступа;

e) Аудит доступа.

Задание на установление соответствия:

Установить соответствие:

1.Косвенные каналы	a. связанные с доступом к элементам АСОД, но не требующие изменения компонентов системы.
2.Прямые каналы	b. не связанные с физическим доступом к элементам АСОД.
3.Полудуплексный канал	c. связанные с доступом к элементам АСОД и изменением структуры компонентов АСОД.
	d. позволяет передавать данные в обоих направлениях, но только в одном направлении за раз.

Компетентностно-ориентированная задача:

Компания А использует распределенную систему для обработки своих данных. Однако, некоторые сотрудники компании заметили, что их персональные данные также обрабатываются в этой системе. Какие законодательные нормы необходимо учитывать при обработке персональных данных в распределенных системах?.

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 «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	3	Доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Устный опрос по темам 4-6	3	Доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Устный опрос по темам 7-9	3	Доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Лабораторная работа №1 «Создание сайтов на языке JavaScript и обеспечение их информационной безопасности»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%

Лабораторная работа №2 «Разработка и защита Web - приложений с серверными сценариями на языке PHP»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №3 «Менеджер паролей: программа Password Commander»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4 «Настройка межсетевого экрана Comodo Firewall»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №5 «Антивирусная программа: Kaspersky Internet Security»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

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

Каждый верный ответ оценивается следующим образом:

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

Максимальное количество баллов за тестирование - 36 баллов.

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

8.1 Основная учебная литература

1. 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 лабораторных работ для студентов укрупненной группы специальностей и направлений 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 сценариями 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 : 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. - 16 с.: ил. 8, Библиогр.: с. 16.

4. Фаервол Comodo Firewall : 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. - 15 с.: ил. 8, Библиогр.: с. 15.

5. Антивирусная программа: Kaspersky Internet Security : 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. - 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, 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 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» - за-

крепить 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: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/ 160Gb/сумка/проектор inFocusIN24+

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

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

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

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

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

14 Лист дополнений и изменений, внесенных в рабочую программу

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изме-нённых	Заме-нённых	Анну-лиро-ванных	новых			