Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ
И.о. декана радиотехнического факультета
_____ / В.А. Баженов /
27. апреля 2018 г.

Рабочая программа дисциплины
Информационная безопасность распределенных информационных систем
(наименование дисциплины)
базовой части образовательной программы
по специальности

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы
«Обеспечение информационной безопасности распределенных информационных систем»

Факультет: Радиотехнический (РТФ)
Кафедра «Информационная безопасность»

Калининград 2018 г.

Визирование РПД для исполнения в очередном учебном году

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«27» июня 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2018 – 2019 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «14» июня 2018 г. № 9

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«____» _____ 2019 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2019 – 2020 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «___» _____2019 г. №

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

1. Цель освоения дисциплины.

1.1. Цель изучения дисциплины.

Цель изучения дисциплины обучить студентов выявлять и противодействовать атакам вредоносных программ и злоумышленников в распределенных системах обработки информации.

1.2. Задачи изучения дисциплины.

- дать основы:
- построения комплексов программно-аппаратных средств обеспечения информационной безопасности различной архитектуры;
- направлений обеспечения защиты ресурсов вычислительных сетей и СУБД от атак вредоносных программ и злоумышленников;
- принципов функционирования современных систем аудита ресурсов ВС;
- построения систем адаптивной безопасности в вычислительных сетях передачи данных;
- способов защиты трафика от изучения, разрушающих программных действий и изменений.

1.3 Предметом изучения дисциплины являются:

- сетевые атаки в распределенных системах, методы, способы и средства защиты от сетевых атак.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.
ОПК-8.	способностью к освоению новых образцов программных, технических средств и информационных технологий	знать: принципы построения современных программных, технических средств и информационных технологий; принципы эксплуатации и ограничения современных программных, технических средств и информационных технологий уметь: уметь определять особенности современных программных, технических средств и информационных технологий при их изучении; эксплуатировать современные программных, технических средств и информационных технологий владеть: методикой эксплуатации современные программных, технических средств и информационных технологий.

ПК-1.	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	знать: методики поиска, изучения, обобщения и систематизации научно-технической информации, виды нормативных и методических материалов в сфере профессиональной деятельности уметь: осуществлять поиск и обобщать, систематизировать научно-техническую информацию в области информационной защиты, использовать нормативные и методические материалы в сфере профессиональной деятельности владеть: методикой поиска, изучения, обобщения и систематизации научно-технической информации
ПК-3.	способностью проводить анализ защищенности автоматизированных систем	знать: методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера уметь: определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники; оценивать уязвимость информации; анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ); создавать модель нарушителя, проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем владеть: методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ

ПК-14.	способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	знать: принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для проверки проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; методы определения стойкости парольной защиты; механизмы активного и пассивного анализа уязвимостей; определять эффективность применяемых программно-аппаратных, криптографических и технических средств защиты информации в зависимости степень риска и вероятность осуществления НСД; принципы контроля данных при передачи информации по прободным и беспроводным каналам связи при использовании криптографических протоколов; языки описания уязвимостей и проверок; теоретико-графовые модели комплексной оценки защищенности распределенных ресурсов уметь: применять сканеры безопасности в пассивном и активном режиме; производить аудит распределенных систем; анализировать результаты сканирования; использовать снифферы для анализа потока передаваемой информации; рассчитывать степень защищенности передаваемой информации; определять степень стойкости паролей; применять системы анализа защищенности; системы анализа рисков владеть: программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; владеть методами сканирования: проверка заголовков, активные зондирующие проверки, имитация атак; методами и средствами проверки стойкости парольной защиты; программным обеспечением и методиками анализа защищенности распределенных ресурсов; программным обеспечением и методи-

		ками анализа рисков
ПК-15.	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	знать: принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения уметь: применять принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; производить аудит распределенных систем; анализировать результаты сканирования владеть: методиками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем, аудита распределенных систем; анализа результатов сканирования

ПК-17.	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	знать: принципы мониторинга защищенности информации в автоматизированной системе, выявления каналов утечки информации; механизмы анализа уязвимостей; определять степень риска и вероятность осуществления НСД уметь: проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; применять сканеры безопасности в пассивном и активном режиме; производить аудит информационных систем; анализировать результаты сканирования владеть: инструментами мониторинга защищенности информации в автоматизированной системе, средствами выявления каналов утечки информации; сканерами безопасности информационных систем; средствами аудит информационных систем
ПК-24.	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	знать: методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности уметь: обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности владеть: методами обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

ПСК-7.1.	способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	знать: методы разработки и исследования модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах уметь: разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах владеть: методами исследования информационно-технологических ресурсов, методами разработки моделей угроз и модели нарушителя информационной безопасности в распределенных информационных системах
ПСК-7.4.	способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	знать: модели политик безопасности; протоколы и сетевые службы, используемые при организации политики безопасности и отладке удаленного соединения: архитектуры распределенных систем; методы доступа операционных систем уметь: применять модели политик безопасности в соответствии с предъявляемыми требованиями; использовать протоколы и сетевые службы при организации политики безопасности и отладке удаленного соединения; определять и выстраивать архитектуры распределенных систем; использовать методы доступа операционных систем владеть: инструментами настройки политик безопасности; инструментами управления протоколами и сетевыми службами, используемыми при организации политики безопасности, средствами отладки удаленного соединения
ПСК-7.5.	способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	знать: особенности, методы и способы координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов уметь: осуществлять отбор и применять методы и способы координирования деятельности подразделений и специалистов по защите информации в ор-

		ганизациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов владеть: методами и способами координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов

Таблица 2 - Этапы формирования компетенций

Коды компетенций	Этапы формирования компетенций (разделы программы)
ОПК-8 ПК-1 ПК-3 ПК-14 ПК-15 ПК-17 ПК-24	Тема 1. Ошибки в программном обеспечении. Уязвимости системных утилит, команд и сетевых служб. Перехват паролей. Перехват незащищенного трафика. Конфигурация системы. Тема 2 Типичные сценарии и уровни атак. Методы, используемые нападающими для проникновения в интернет-сети. Тема 3. Сканирование карты сети. Атаки на основе telnet и rlogin. Соответствие портов. Нападения с использованием сетевых протоколов. SYN-бомбардировка. Спуффинг. Тема 4. Распределенные атаки "отказ в обслуживании". ARP-spoofing или ложный ARP- сервер. IP Hijacking. Нападения на основе протокола ICMP. Тема 5. Эволюция методов отражения вторжений. Тема 6. Классификация методов отражения вторжений. Предотвращение вторжения. Противодействие вторжению. Сдерживание вторжения. Отклонение вторжения. Обнаружение вторжений. Прерывание вторжения.
ПК-1 ПК-3 ПК-14 ПК-15 ПК-17 ПК-24 ПСК-7.1 ПСК-7.4 ПСК-7.5	Тема 7. Политика безопасности интернет-сети. Сетевой аудит. Место систем обнаружения вторжений в защите интернет-сети и интрасетей. / Тема 8. Системы обнаружения вторжений и межсетевые экраны. Порядок развертывания систем обнаружения вторжений. Тема 9 Классификация систем обнаружения вторжений. Эволюция систем обнаружения вторжения. Тема 10 Размещение сетевых систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений. Системное и сетевое обнаружение вторжений. Тема 11 Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы. Сохранение доказательств вторжения

Таблица 3 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	- концепцию диспетчера доступа; - методы и средства ограничения доступа к ресурсам распределенной ВС;

	- методы и средства обнаружения уязвимостей распределенной ВС; - методы и средства обнаружения атак на ресурсы распределенной ВС; - методы и средства противодействия атакам на ресурсы распределенной ВС.
уметь	- организовывать защиту распределенной ВС; - производить защиту от атак на ресурсы распределенной ВС; - производить защиту программ от изменений в распределенной ВС; - осуществлять контроль трафика в рамках распределенной ВС.
владеть	- средствами защиты в распределенной ВС от несанкционированного доступа и нарушения функциональности ее подсистем; - средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных. - методикой контроля информационной целостности в распределенной ВС;

3. Место дисциплины в структуре образовательной программы

Место дисциплины в структуре ООП специалитета:

С3.Б1.18 Базовая часть. Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

Требования к предварительной подготовке обучающегося:

Перечень дисциплин, усвоение которых необходимо для изучения дисциплины «Информационная безопасность распределенных информационных систем»: «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Безопасность операционных систем», «Правовое обеспечение информационной безопасности».

Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

"Комплексное обеспечение информационной безопасности автоматизированных систем".

4. Содержание дисциплины:

Тема 1. Ошибки в программном обеспечении. Уязвимости системных утилит, команд и сетевых служб. Перехват паролей. Перехват незащищенного трафика. Конфигурация системы.

Тема 2 Типичные сценарии и уровни атак. Методы, используемые нападающими для проникновения в интернет-сети.

Тема 3. Сканирование карты сети. Атаки на основе telnet и rlogin. Соответствие портов. Нападения с использованием сетевых протоколов. SYN-бомбардировка. Спуффинг.

Тема 4. Распределенные атаки "отказ в обслуживании". ARP-spoofing или ложный ARP-сервер. IP Hijacking. Нападения на основе протокола ICMP.

Тема 5. Эволюция методов отражения вторжений.

Тема 6. Классификация методов отражения вторжений. Предотвращение вторжения. Противодействие вторжению. Сдерживание вторжения. Отклонение вторжения. Обнаружение вторжений. Прерывание вторжения.

Тема 7. Политика безопасности интернет-сети. Сетевой аудит. Место систем обнаружения вторжений в защите интернет-сети и интрасетей. /

Тема 8. Системы обнаружения вторжений и межсетевые экраны. Порядок развертывания систем обнаружения вторжений.

Тема 9 Классификация систем обнаружения вторжений. Эволюция систем обнаружения вторжения.

Тема 10 Размещение сетевых систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений. Системное и сетевое обнаружение вторжений.

Тема 11 Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы. Сохранение доказательств вторжения

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации

Таблица 1 - Объем (трудоемкость освоения) и структура дисциплины, формы аттестации для очной формы обучения

Номер и наименование тем	Объем учебной работы (час.)					
	Лек-	ЛЗ	ПЗ	СРС	Контроль	Всего
Семестр - 8 (216 час; 6 ЗЕТ)						
Тема 1. Ошибки в программном обеспечении. Уязвимости системных утилит, команд и сетевых служб. Перехват паролей. Перехват незащищенного трафика. Конфигурация системы.	4					4
Тема 2 Типичные сценарии и уровни атак. Методы, используемые нападающими для проникновения в интернет-сети.	4	4		14	10	32
Тема 3. Сканирование карты сети. Атаки на основе telnet и rlogin. Соответствие портов. Нападения с использованием сетевых протоколов. SYN-бомбардировка. Спуффинг.	4	12		14		30
Тема 4. Распределенные атаки "отказ в обслуживании". ARP-spoofing или ложный ARP- сервер IP Hijacking. Нападения на основе протокола ICMP.	4	16		16		36
Тема 5. Эволюция методов отражения вторжений.	4	4				8
Тема 6. Классификация методов отражения вторжений. Предотвращение вторжения. Противодействие вторжению. Сдерживание вторжения. Отклонение вторжения. Обнаружение вторжений. Прерывание вторжения.	4	4		16		24
Тема 7. Политика безопасности интернет-сети. Сетевой аудит. Место систем обнаружения вторжений в защите интернет-сети и интрасетей. /	2	8			10	20

Тема 8. Системы обнаружения вторжений и межсетевые экраны. Порядок развертывания систем обнаружения вторжений.	2	4				6
Тема 9 Классификация систем обнаружения вторжений. Эволюция систем обнаружения вторжения.	4	4				8
Тема 10 Размещение сетевых систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений. Системное и сетевое обнаружение вторжений.	2	8		18		28
Тема 11 Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы. Сохранение доказательств вторжения	2	4			16	22
Подготовка к сдаче и сдача экзамена						
Всего в семестре	34	68		78	36	216
Итого по дисциплине	34	68		78	36	216

ЛЗ – лабораторные занятия,
ПЗ – практические занятия,
СРС – самостоятельная работа студента,
КР – курсовая работа,
КП – курсовой проект.

6. Лабораторные занятия (работы)

Таблица 2 - Лабораторные по очной форме обучения

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов ЛЗ
Семестр – 8 (68 час.)			
1.	Тема 2	Построение графа атаки.	4
2.	Тема 3	Определение уязвимостей сетевых служб протоколов.	4
3.	Тема 3	Противодействие SYN-бомбардировка.	4
4.	Тема 3	Противодействие спуффинг.	4
5.	Тема 4	Распределенные атаки "отказ в обслуживании". ARP-spoofing или ложный ARP- сервер	4
6.	Тема 4	IP Hijacking. Нападения на основе протокола ICMP	4
7.	Тема 4	Распределенные атаки "отказ в обслуживании". ARP-spoofing или ложный ARP- сервер	4
8.	Тема 4	Выявления возможных каналов НСД	4
9.	Тема 5	Противодействие атакам DOS.	4

10.	Тема 6	Противодействие атакам XSS.	4
11.	Тема 7	Обнаружение вторжений в компьютерную систему	4
12.	Тема 7	Методики противодействия сетевым вторжениям	4
13.	Тема 8	Применение системы определения вторжений.	4
14.	Тема 9	Исследование защитных механизмов браузера internet explorer.	4
15.	Тема 10	Создание и применение правил Snort.	4
16.	Тема 10	Защита сервера.	2
17.	Тема 10	Методика аутентификации пользователей в распределенных системах обработки информации.	2
18.	Тема 11	Тестирования сетевой защищенности Эшелон	4
Итого по дисциплине			68

7. Практические занятия

Практические занятия по дисциплине учебным планом не предусмотрены.

8. Самостоятельная работа студента

Таблица 3 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
Семестр – 8 (78 час.)			
1.	Угрозы безопасности автоматизированных систем обработки данных. Характеристика программно-технических изделий защиты информации в ПК.	14	Текущий контроль: опрос, тест
2.	Состав и структура методов и систем обеспечения информационной безопасности. Методы идентификации и установления подлинности субъектов и различных объектов. Способы разграничения доступа. Методы и средства нейтрализации угроз.	14	
3.	Состав и структура методов и систем обеспечения информационной безопасности. Методы идентификации и установления подлинности субъектов и различных объектов.	16	
4.	Способы разграничения доступа. Методы и средства нейтрализации угроз.	16	
5.	Система управления доступом и организация автоматизированной системы контроля доступом (АСКД). Способы аутентификации пользователей. Характеристика программной защиты ПК – Ad-Aware.	18	
Всего за семестр:		78	
Итого по дисциплине		78	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

Таблица 4 – Основная учебная литература

Авторы, составители	Заглавие	Издательство, год	Колич-во

Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: учебное пособие	М. : ИД "Форум" ; М. : ИНФРА-М, 2013. -	20

Таблица 5 – Дополнительная учебная литература

Авторы, составители	Заглавие	Издательство,	Колич-во
Запечников С.В., Милославская Н.Г.	Информационная безопасность открытых систем в 2-х томах. Т.1: учебник для вузов	М.: Горячая линия-Телеком, 2006	15
Запечников С.В., Милославская Н.Г.	Информационная безопасность открытых систем в 2-х томах. Т.2: учебник для вузов	М.: Горячая линия-Телеком, 2006	15

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Программное обеспечение

1.СЗИ Блокхост-сеть 2.0. Договор о сотрудничестве №012 ООО "Газинформсервис" артикул БХС2.0-АВ-10-49 "Блокхост-сеть 2.0" /лицензии:26 шт./ Дата: 14.06.2018 г. (срок действия: три года)

2.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

3.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);
– Ethereal (Программы перехвата и анализа сетевых пакетов);
– NMAP(Программа сканирование сетевых ресурсов);
– MySQL (Система управления базами данных).

Интернет-ресурсы

Интернет-ресурсы, применяемые при изучении:

1. http://www.intuit.ru/
2. http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/
3. http://eLIBRARY.RU (Научная лицензионная библиотека eLIBRARY.RU договор №673-03/2017К от 23. 03.207г., бессрочно)

11. Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебная аудитория № 441.

Состав оборудования: столы учебные – 15 шт., стол преподавательский – 1 шт., стулья учебные – 30 шт., стул преподавательский – 1 шт., трибуна – 1 шт., экран раздвижной PROJECTA – 1 шт.; доска магнитно-маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды: «Комплекс средств автоматизации деятельности оперативного персонала пункта централизованной охраны», «Требования и нормы проектирования по защите объектов от преступных посягательств». Специализированные стенды: СКУД «Стилпост»; «СИНЕРГЕТ» (цифровая система видеонаблюдения и аудиорегистрации).

Используется лицензионное программное обеспечение Microsoft Desktop Education, Microsoft Office 2016, Kaspersky Total Space Security Russian Edition.

11.1.2. Материально-техническое обеспечение для лабораторных занятий

Для проведения лабораторных занятий используется лаборатория технической защиты информации № 439.

Состав оборудования: столы учебные – 12 шт., стол преподавательский – 1 шт., стулья учебные – 17 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.

Компьютеры (системный блок, монитор, мышка, клавиатура), с установленным лицензионным программным обеспечением:

1.СЗИ Блокхост-сеть 2.0. Договор о сотрудничестве №012 ООО "Газинформсервис"

артикул БХС2.0-АВ-10-49 "Блокхост-сеть 2.0" /лицензии:26 шт./ Дата: 14.06.2018 г. (срок действия: три года)

2.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

3.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);
– Ethereal (Программы перехвата и анализа сетевых пакетов);
– NMAP(Программа сканирование сетевых ресурсов);
– MySQL (Система управления базами данных).

Для проведения лабораторных занятий используются компьютерный класс № 248.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютеры (системный блок, монитор ASUS, мышка, клавиатура), с установленным лицензионным программным обеспечением: Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

11.1.3. Материально-техническое обеспечение для самостоятельной работы

Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной си-

стемы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12. Фонд оценочных средств для проведения аттестации по дисциплине.

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств для аттестации по дисциплине «Языки программирования».

13. Особенности преподавания и освоения дисциплины

13.1 Под образовательными технологиями будем понимать пути и способы формирования компетенций. В рамках дисциплины предусмотрены:

- лекции;
- лабораторные занятия, во время которых отрабатываются практические навыки, обсуждаются вопросы лекций, домашних заданий, проводятся контрольные и самостоятельные работы и т.д.;
- самостоятельная работа студентов, включающая усвоение теоретического материала, подготовку к практическим занятиям, выполнение индивидуальных заданий, курсовой работы, работа с учебниками, иной учебной и учебно-методической литературой, подготовка к текущему контролю успеваемости, к экзамену;
- тестирование по отдельным темам дисциплины;
- консультирование студентов по вопросам учебного материала.

13.2 Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

14. Методические указания по освоению дисциплины

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая *(*повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):

• исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

• индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
• конспектирование лекций;
• получение консультаций для разъяснений по вопросам изучаемой дисциплины;
• подготовка ответов на вопросы тестов;
• подготовка к экзамену;
• выполнение контрольных, курсовых и дипломных работ;
• подготовка научных докладов, рефератов, эссе;
• анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

• чтение текста (учебника, первоисточника, дополнительной литературы);
• составление плана текста;
• конспектирование текста;

• выписки из текста;
• работа со словарями и справочниками;
• исследовательская работа;
• использование аудио- и видеозаписи;
• работа с электронными информационными ресурсами и ресурсами Internet:
Для закрепления и систематизации знании:
• работа с конспектом лекции (обработка текста);
• повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей):
• составление плана и тезисов ответа;
• выполнение тестовых заданий;
• ответы на контрольные вопросы;
• аннотирование, реферирование, рецензирование текста;
• подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
• работа с компьютерными программами;
• подготовка к сдаче экзамена;
Для формирования умений:
• решение задач и упражнений по образцу;
• решение вариативных задач и упражнений:
• выполнение расчетно-графических работ;
• решение ситуационных производственных (профессиональных) задач;
• участие в научных и практических конференциях;
• проектирование и моделирование разных видов и компонентов профессиональной деятельности;
• создание проспектов, проектов, моделей;
• экспериментальная работа, участие в НИР;
• рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
• подготовка курсовых и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

15. Сведения о рабочей программе и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и соответствует учебному плану, утвержденному «31» января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор(ы) программы:
ст. преподаватель кафедры информационной безопасности _____ /В.В.Подтопельный/

Программа дисциплины рассмотрена и одобрена на заседании кафедры «Информационная безопасность» (протокол № 9 от 14 июня 2018 г.)

Зав. кафедрой информационной безопасности _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета (протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ / Жестовский А.Г.