МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.
«31» августа 2021 г.

Рабочая программа дисциплины
Основы построения защищенных компьютерных сетей

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Бондарев Н. Н.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления			31.08.2021 г.

1. Цели освоения дисциплины

Целями освоения дисциплины являются овладение основными знаниями и навыками в области защиты информации в компьютерных сетях.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Аппаратные средства вычислительной техники», «Компьютерные сети», «Операционные системы», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Сети и системы передачи информации».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Модели безопасности компьютерных систем», «Защита информации от утечки по техническим каналам».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Программно-аппаратные средства обеспечения информационной безопасности».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.1.1 знает источники и классификацию угроз информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; ОПК-5.2.3 умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; ОПК-5.3.1 владеет навыками применения нормативных	Знать источники и классификацию угроз информационной безопасности. Уметь анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации. Владеть навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации; методами и средствами технической защиты информации.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации; ОПК-5.3.2 владеет методами и средствами технической защиты информации.	
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	ОПК-6.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем; ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного	Знать систему нормативных правовых актов и стандартов по лицензированию в области технической защиты конфиденциальной информации. Уметь разрабатывать модели угроз и модели нарушителя компьютерных систем;; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы. Владеть навыками при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; ОПК-6.3 владеет навыками при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	
ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	ОПК-16.1.1 знает основные задачи мониторинга средств защиты информации в компьютерных системах; ОПК-16.1.2 знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы	Знать основные задачи мониторинга средств защиты информации в компьютерных системах; средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	предотвращения и обнаружения вторжений; ОПК-16.2.1 умеет проводить мониторинг работоспособности средств защиты информации в компьютерных системах; ОПК-16.2.2 умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; ОПК-16.3.1 владеет навыками проведения анализа эффективности средств защиты информации в компьютерных системах и сетях; ОПК-16.3.2 владеет навыками настройки межсетевых экранов; методиками анализа сетевого трафика.	предотвращения и обнаружения вторжений. Уметь проводить мониторинг работоспособности средств защиты информации в компьютерных системах; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеть навыками настройки межсетевых экранов; методиками анализа сетевого трафика.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8		9
1	Теоретические основы защиты компьютерных сетей	7	1-9	17	17	0	1	19	Контрольная работа на 17 неделе
2	Средства защиты компьютерных сетей		9-17	17	17	0	1	19	
	Промежуточная аттестация								Зачет
	ИТОГО в 7-м семестре			**34**	**34**	**0**	**2**	**38**	–

Содержание дисциплины

Теоретические основы защиты компьютерных сетей. Угрозы информации в компьютерных сетях. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях. Протоколы аутентификации при удаленном доступе. Средства и методы обеспечения целостности и конфиденциальности. Математические методы борьбы со спамом. Защита от вредоносных программ, работающих через компьютерную сеть.

Средства защиты компьютерных сетей. Защита серверов и рабочих станций. Средства защиты локальных сетей при подключении к Интернет. HoneyPot и HoneyNet. Защитные экраны (firewall). Системы обнаружения вторжений (IDS). Защита виртуальных частных сетей (VPN). Защита беспроводных сетей. Защита от атак «отказ в обслуживании». Защита от снифферов. Защита систем дистанционного банковского обслуживания.

План лабораторных занятий

На лабораторных занятиях студенты выполняют задания, связанные с закреплением полученного теоретического материала, с использованием рекомендованного программного обеспечения.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1–9	Теоретические основы защиты компьютерных сетей	1-3
9–17	Средства защиты компьютерных сетей	4-6

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как интерактивный опрос, эвристическая беседа, диалог, выступления экспертов и специалистов перед студентами.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешанных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

В рамках самостоятельной работы студенты изучают источники, в которых более детально рассматривается материал. Каждому студенту выдается задание, связанное с практическим изучением методов и средств защиты компьютерной информации в компьютерных сетях, которое выполняется студентом самостоятельно. Контроль текущей успеваемости осуществляется в процессе проведения лабораторных занятий.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачет). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Основы построения защищённых компьютерных сетей».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	30	20	0	5	0	5	40	100

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 30 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий в течение одного семестра – от 0 до 20 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Оценивается качество выполнения заданий в рамках самостоятельной работы, грамотность оформления, глубина проработки материала. Выполнение домашних работ в течении семестра – от 0 до 5 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Выполнение контрольной работы – от 0 до 5 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой зачет, проводимый в устной форме с предварительной подготовкой студента к ответу.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 31 до 40 баллов;

ответ на «хорошо» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 7 семестр по дисциплине «Основы построения защищенных компьютерных сетей» составляет 100 баллов.

Таблица 2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Основы построения защищенных компьютерных сетей» в оценку (зачет)

55 баллов и более	«зачтено»
меньше 55 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины.

а) литература:

1) Корт, С. С. Теоретические основы защиты информации [Текст] : учеб. пособие / С. С. Корт. - Москва : Гелиос АРВ, 2004. - 233, [7] с. : ил. - Библиогр.: с. 226-229. - ISBN 5-85438-010-2.

2) Юрин, И. Ю. Теоретические и практические основы защиты информации [Электронный ресурс]: учеб. пособие / И. Ю. Юрин. Саратов, 2012. 32 с. URL: http://library.sgu.ru/uch_lit/620.pdf. Загл. с экрана. Яз. рус.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Microsoft Windows; Microsoft Visual Studio.

2) Аппаратные ключи «РуТокен».

3) Программно-аппаратный комплекс «SecretNet».

4) Программно-аппаратный комплекс «Аккорд».

5) Программно-аппаратный комплекс «Соболь».

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных занятий необходим компьютерный класс, оснащенный персональными компьютерами и необходимым программно-аппаратным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии Н. Н. Бондарев

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.