МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
Лениногорский филиал

УТВЕРЖДАЮ
Директор ЛФ КНИТУ-КАИ
_____ Р.А. Шамсутдинов

«25» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины (модуля)

Б1.В.ДВ.02.02 Обнаружение вторжений в компьютерные сети
(индекс и наименование дисциплины по учебному плану)

Квалификация: *магистр*

Форма обучения: *очная*

Направление подготовки: *09.04.02 Информационные системы и технологии*

Направленность (профиль): *Безопасность информационных систем*

Лениногорск 2022

Рабочая программа дисциплины (модуля) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования - магистратура по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017г. № 917.

Разработчик(и):
Сагдатуллин А.М., к.т.н., доцент кафедры МиИТ _____ (подпись)
(ФИО, ученая степень, ученое звание)

Денисов О.В., к.т.н., старший преподаватель кафедры МиИТ _____ (подпись)
(ФИО, ученая степень, ученое звание)

Рабочая программа утверждена на заседании кафедры МиИТ от «19» апреля 2022 г., протокол № 8.

/Заведующий кафедрой МиИТ
Думлер Е.Б., к.т.н. _____ (подпись)
(ФИО, ученая степень, ученое звание)

Рабочая программа дисциплины (модуля):	Наименование Подразделения	Дата	№ протокола	Подпись
ОДОБРЕНА	на заседании кафедры МиИТ	19.04.2022	№ 8	Руководитель ОП А.М. Сагдатуллин
ОДОБРЕНА	Учебно-методическая комиссия ЛФ КНИТУ-КАИ	21.04.2022	№ 8	Председатель УМК З.И.Аскарова
СОГЛАСОВАНА	Научно-техническая библиотека	21.04.2022		Библиотекарь А.Г. Страшнова

1 ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цель изучения дисциплины (модуля)

Основной целью изучения дисциплины является обучение технологиям, принципам, методам и средствам защиты данных в сети от различных угроз с применением программных и программно-аппаратных средств защиты.

1.2 Задачи дисциплины (модуля)

Основными задачами дисциплины являются:

1) изучение базовых методов защиты информации в компьютерных сетях;

2) знакомство с программными и программно-аппаратными средствами защиты от типовых угроз ИБ в компьютерных сетях;

3) знакомство с основными подходами к активному аудиту в компьютерных сетях.

1.3 Место дисциплины (модуля) в структуре ОП ВО

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы и является элективной дисциплиной, определяющей ее предметно-тематическое содержание – направленность.

1.4 Объем дисциплины (модуля) и виды учебной работы

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся представлены в таблице 1.1

Таблица 1.1

Объем дисциплины (модуля) для очной формы обучения

Семестр	Общая трудоемкость дисциплины (модуля), в ЗЕ/час	*Виды учебной работы, в т.ч., проводимые с использованием ЭО и ДОТ*											
		Контактная работа обучающихся с преподавателем по видам учебной работы (аудиторная работа)							***Самостоятельная работа обучающегося (внеаудиторная работа)***				
		Лекции/ в т.ч. в форме практической подготовки	Лабораторные работы/ в т.ч. в форме практической подготовки	Практические занятия/ в т.ч. в форме практической подготовки	Курсовая работа (консультация, защита)	Курсовой проект (консультации, защита)	Консультации перед экзаменом	Контактная работа на промежуточной аттестации	Курсовая работа (подготовка)/ в т.ч. в форме практической подготовки	Курсовой проект (подготовка)/ в т.ч. в форме практической подготовки	Проработка учебного материала (самоподготовка)/ в т.ч. в форме практической подготовки	Подготовка к промежуточной аттестации	Форма промежуточной аттестации
3	3 ЗЕ/108	16/8	16/16		-	-	-	0,3	-	-	75,7/50	-	Зачет
Итого	3 ЗЕ/108	16/8	16/16		-	-	-	0,3	-	-	75,7/50	-	Зачет

1.5 Перечень планируемых результатов обучения по дисциплине (модулю)

Процесс изучения дисциплины направлен на формирование компетенций, представленных в таблице 1.2.

Таблица 1.2

Формируемые компетенции

Код компетенции	Наименование компетенции	Индикаторы достижения компетенций	Планируемые результаты обучения
ПК-3	Способен выполнять работы по проектированию и созданию и сопровождению системного программного обеспечения и его компонент	ИД-1$_{ПК-3}$ – выполняет работы по проектированию архитектуры системного программного обеспечения; ИД-2$_{ПК-3}$ – разрабатывает программное обеспечение на основе выбранной архитектуры; ИД-3$_{ПК-3}$ – проектирует и	**Знает** типы архитектур инфокоммуникационных систем **Умеет** проектировать архитектуру информационной системы для конкретных задач **Владеет** навыками

		разрабатывает компоненты программного обеспечения	развертывания, настройки, масштабирования и обслуживания инфокоммуникационных систем
ПК-4	Способен выполнять работы по анализу безопасности и мониторингу защищенности компьютерных систем и сетей	ИД-1$_{ПК-4}$ – анализирует степень обеспечения безопасности компьютерных систем и сетей; ИД-2$_{ПК-4}$ – применяет инструментальные средства инструментальные средства мониторинга безопасности компьютерных систем и сетей; ИД-3$_{ПК-4}$ – применяет инструментальные средства для противодействия нарушению безопасности компьютерных систем и сетей	**Знает** принципы и методы обеспечения безопасности компьютерных сетей **Умеет** проводить мониторинг безопасности компьютерных систем и сетей и выявлять вторжения в компьютерные сети **Владеет** навками использования инструментария для обнаружения вторжений в компьютерные сети

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1 Структура дисциплины (модуля)

Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебной работы приведены в таблице 2.1.

Таблица 2.1

Разделы дисциплины (модуля) и виды учебной работы

Наименование тем (разделов) дисциплины (модуля)	Всего (час)	Контактная работа обучающихся с преподавателем по видам учебных занятий (в час)				Самостоятельная работа (проработка учебного материала), выполнение курсовой работы /проекта, подготовка к ПА, самоподготовка.
		Лекции	Лабораторные работы	Практические занятия	КР, КП, ПА, консультация	
3 семестр						
1 Основные подходы к защите информации в компьютерных сетях	32,7	4	4			24,7
2 Программно-аппаратные средства защиты информации в компьютерных сетях	37	6	6			25
3 Системы анализа защищенности компьютерных сетей	38	6	6			26
Промежуточная аттестация (зачет)	0,3				0,3	
Итого за семестр	**108**	**16**	**16**		**0,3**	**75,7**

2.2 Содержание разделов дисциплины (модуля)

1 Основные подходы к защите информации в компьютерных сетях.

Основные угрозы ИБ в компьютерных сетях и подходы к защите от них. Основные уязвимости и их причины. Классификация типовых удаленных атак. Оценка степени серьезности атак.

2 Программно-аппаратные средства защиты информации в компьютерных сетях.

Межсетевые экраны и их классификация. Настройка правил доступа к сетевым ресурсам. Организация демилитаризованной зоны. Анализ журналов безопасности. Системы обнаружения и предотвращения атак. Размещение и конфигурирование сенсоров. Виртуальные частные сети. Основные протоколы. Удаленной аутентфикации пользователей в компьютерных сетях.

3 Системы анализа защищенности компьютерных сетей.

Классификация уязвимостей. Источники информации об уязвимостях. Оценка степени опасности уязвимостей. Сканеры безопасности, их классификация.

2.3 Курсовая работа (курсовой проект)

Не предусмотрено учебным планом.

3 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля).

Промежуточная аттестация обеспечивает оценивание промежуточных результатов обучения по дисциплине (модулю).

Комплект оценочных материалов представляет собой совокупность оценочных средств (комплекс заданий различного типа с ключами правильных ответов, включая критерии оценки), используемых при проведении оценочных процедур (текущего контроля, промежуточной аттестации) с целью оценивания достижения обучающимися результатов обучения по дисциплине (модулю).

Комплект оценочных материалов (текущего контроля и промежуточной аттестации), необходимых для оценивания результатов освоения дисциплины (модуля) представлен в виде отдельного документа по дисциплине (модулю) и хранится на кафедре-разработчике в бумажном или электронном виде.

3.1 Оценка успеваемости обучающихся

Текущий контроль успеваемости и промежуточная аттестация по дисциплине (модулю) осуществляется в соответствии с балльно-рейтинговой системой по 100-балльной шкале. Пересчет суммы баллов в традиционную оценку представлен в таблице 3.1.

Таблица 3.1

Шкала оценки на промежуточной аттестации

Выражение в баллах	Словесное выражение при форме промежуточной аттестации – зачет
от 86 до 100	Зачтено
от 71 до 85	Зачтено
от 51 до 70	Зачтено
до 51	Не зачтено

4 ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1 Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1.1 Основная литература

1. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова ; под редакцией О. И. Шелухина. — М.: Горячая линия-Телеком, 2018. — 220 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111119

2. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. — М.: ДМК Пресс, 2012. — 592 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032

4.1.2 Дополнительная литература

1. Пугин, В. В. Защита информации в компьютерных информационных системах [Электронный ресурс]: учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара: ПГУТИ, 2018. — 119 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299

2. Технологии защиты информации в компьютерных сетях [Электронный ресурс]: учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — М.: ИНТУИТ, 2016. — 368 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522

3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: учебное пособие / Е. В. Глинская, Н. В. Чичварин. – М.: ИНФРА-М, 2021. - 118 с. - (Высшее образование: Специалитет). - Текст: электронный. - URL: https://znanium.com/catalog/product/1178153

4. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — М.: Горячая линия-Телеком, 2017. — 338 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111049

5. Пушкарёв, В. В. Защита информационных процессов в компьютерных системах [Электронный ресурс]: учебное пособие / В. В. Пушкарёв, В. П. Пушкарёв. — М.: ТУСУР, 2012. — 131 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/4925

6. Басыня, Е. А. Системное администрирование и информационная безопасность [Электронный ресурс]: учебное пособие / Е. А. Басыня. —

Новосибирск: НГТУ, 2018. — 79 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/118259

4.1.3 Методические материалы

1.Методические указания к выполнению лабораторных работ по дисциплине.

4.1.4 Перечень информационных технологий и электронных ресурсов, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Организовано взаимодействие обучающегося и преподавателя с использованием электронной информационно-образовательной среды КНИТУ-КАИ.

1. Сайт электронного обучения КНИТУ-КАИ http://e.kai.ru

4.1.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине (модулю)

1 Электронно-библиотечная система учебной и научной литературы «Лань». URL: https://e.lanbook.com/.

2. Электронно-библиотечная система учебной и научной литературы «Znanium/com». URL: https://znanium.com/

3. Электронно-библиотечная система учебной и научной литературы «Юрайт». URL: https://urait.ru/catalog/full

4. Научно-техническая библиотека КНИТУ-КАИ им. Н.Г. Четаева. URL: http://elibs.kai.ru/

4.2 Материально-техническое обеспечение дисциплины (модуля) и требуемое программное обеспечение

Описание материально-технической базы и программного обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю) приведено соответственно в таблицах 4.1 и 4.2.

Таблица 4.1

Материально-техническое обеспечение дисциплины (модуля)

Наименование вида учебных занятий	Наименование учебной аудитории,	Перечень необходимого оборудования и технических средств

	специализированной лаборатории	обучения
Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа ауд.№302	- мультимедийный проектор; - ноутбук; - настенный экран; - акустические колонки; - учебные столы, стулья; - доска; - стол преподавателя; - учебно – наглядные пособия.
Лабораторные занятия	Учебная аудитория для проведения практических занятий, текущего контроля и промежуточной аттестации (Компьютерная аудитория) ауд.№201	- компьютерные столы, стулья; - персональные компьютеры, ЖК мониторы; - доска интерактивная, - мультимедиа-проектор; - пакет операционных и прикладных программ.
Самостоятельная работа	Помещение для самостоятельной работы студента ауд.№112	- персональный компьютер (9 шт.); - ЖК монитор 19” (9 шт.); - столы компьютерные (9 шт.); - учебные столы (8 шт.), - стулья (25шт.).

Таблица 4.2

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое при осуществлении образовательного процесса по дисциплине (модулю)

№ п/п	Наименование программного обеспечения	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1.	Microsoft Windows 7 Professional Russian	Microsoft, США	Лицензионное
2.	Microsoft Office Professional Plus 2010 Russian	Microsoft, США	Лицензионное
3.	Антивирусная программа Kaspersky Endpoint Security 8 for Windows	Лаборатория Касперского, Россия	Лицензионное
4.	Microsoft Visual Studio	Microsoft, США	Лицензионное
5.	Matlab	The MathWorks	Лицензионное
6.	Microsoft Visio	Microsoft, США	Лицензионное
7.	Microsoft SQL Server	Microsoft, США	Свободно распространяемое
8.	XAMPP	Apachefriends.org	Свободно распространяемое
9.	PyCharm	JetBrains	Свободно распространяемое

10.	CISCO Packet Tracer	CISCO Systems	Свободно распространяемое

5 ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Обучение по дисциплине (модулю) обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение лиц с ограниченными возможностями здоровья и инвалидов организуется как совместно с другими обучающимися, так и в отдельных группах.

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 5.1.

Таблица 5.1

Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, контрольные работы, письменные самостоятельные работы, вопросы к (зачету)	Преимущественно письменная проверка
С нарушениями зрения	Устный опрос по терминам, собеседование по вопросам к (зачету)	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к (зачету)	Преимущественно дистанционными методами

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, например:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Освоение дисциплины (модуля) лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изменения, вносимые в рабочую программу дисциплины (модуля)

№ п/п	№ раздела внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» заведующий кафедрой, реализующей дисциплину