Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О. И. Чуприс
«__» _____ 2018 г.

Регистрационный № УД-6266 /уч.

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И КОМПЬЮТЕРНЫХ СЕТЯХ

**Учебная программа учреждения высшего образования
по учебной дисциплине для специальности первой ступени высшего образования:**

**1-980101 Компьютерная безопасность (по направлениям)
направления специальности
1-980101-01 Компьютерная безопасность
(математические методы и программные системы)**

2018 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-9801 01-2013 и учебных планов Р98-138/уч., Р98и-141/уч. от 30.05.2013.

СОСТАВИТЕЛИ:

М.Ю. Деркач, ассистент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета.

В.В. Пьянов, ассистент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета (протокол № 13 от 29 марта 2018 г.);

Научно-методическим Советом Белорусского государственного университета (протокол № 7 от 13июля 2018 г.).

/ Бодягин И.А., зав. кафедрой ММАД /

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цель преподавания учебной дисциплины – ознакомление студентов с основами современной теории криптографических протоколов, задачами, решаемыми с помощью криптографических протоколов, изучение криптографических протоколов аутентификации, распределения ключей и голосования.

В рамках поставленной цели ***задачи*** учебной дисциплины состоят в следующем:

1) развить у студентов навыки построения, реализации, анализа стойкости и применения криптографических протоколов для обеспечения безопасности в современных информационных системах и компьютерных сетях;
2) изучить основ построения защищенных операционных систем;
3) изучить основы создания защищенных туннелей через открытые сети.
4) изучить существующие средства перехвата, фильтрации и исследования сетевого трафика (сетевые мониторы, брандмауэры), а также принципы их функционирования.

Учебная дисциплина «Криптографические протоколы. Защита информации в информационных системах и компьютерных сетях» относится к циклу дисциплин специализации.

Учебная программа составлена с учетом межпредметных связей с учебными дисциплинами. Так, основой для изучения дисциплины «Криптографические протоколы. Защита информации в информационных системах и компьютерных сетях» являются дисциплины «Операционные системы» и «Компьютерные сети». Знания, полученные в результате изучения дисциплины, будут использованы при изучении дисциплины «Системы связи и сети передачи информации», а также способствовать успешному прохождению преддипломной практики и подготовки дипломной работы.

В результате освоения учебной дисциплины студент магистратуры должен:

знать:

– типы ключей и их взаимосвязь, функции управления ключами, классификацию способов распределения ключевой информации;

– основные схемы криптографических протоколов аутентификации, распределения ключей и голосования;

– разновидности атак на криптографические протоколы аутентификации, распределения ключей и голосования;

– основные средства защиты на различных уровнях модели OSI;

– основные типы угроз безопасности операционных систем;

– основные виды вредоносного программного обеспечения;

– средства защиты операционных систем;

– основные угрозы безопасности в компьютерных сетях, методы защиты от них;

– основы создания защищенных туннелей через открытые сети;

– принципы функционирования сетевых служб, влияющих на безопасность;

– принципы функционирования сетевого стека ОС Windows, основы создания пакетных фильтров, средств перехвата сетевого трафика.

уметь:

– применять изложенный материал на практике при создании, применении и анализе стойкости криптографических протоколов аутентификации для обеспечения безопасности современных компьютерных систем;

– создавать и производить настройку политик доступа и аудита операционных систем;

– производить контроль целостности конфигурации операционной системы;

– создавать и производить настройку параметров защищенных виртуальных сетей и канала IPSec в туннельном и транспортном режиме средствами ОС Windows;

– производить настройку службы маршрутизации и удаленного доступа в ОС Windows;

– обеспечивать безопасность разделяемых сетевых ресурсов;

– настраивать безопасное подключение для веб-сервера IIS и Apache;

– анализировать трафик при помощи средства Wireshark;

– использовать персональные брандмауэры;

владеть:

– навыками настройки механизма SUDO в ОС семейства Linux;

– навыками настройки сетевых интерфейсов в ОС семейства Windows и Linux;

– навыками работы с утилитами управления безопасности IPTABLES в ОС Linux, встроенным брандмауэром и средствами управления службы маршрутизации и удаленного доступа, средствами управления политикой безопасности IP в ОС Windows;

– навыками работы с сетевым анализатором Wireshark.

Освоение учебной дисциплины «Криптографические протоколы. Защита информации в информационных системах и компьютерных сетях» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

академические компетенции**:**

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

социально-личностные компетенции:

СЛК-3. Обладать способностью к межличностным коммуникациям.

профессиональные компетенции:

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

ПК-13. Владеть современными средствами телекоммуникаций.

ПК-21. Эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

Структура содержания учебной дисциплины включает такие дидактические единицы, как темы (разделы), в соответствии с которыми разрабатываются и реализуются соответствующие лекционные и семинарские занятия. Примерная тематика занятий приведена в информационно-методической части.

Дисциплина изучается в 7 семестре. Всего на освоение учебной дисциплины «Криптографические протоколы. Защита информации в информационных системах и компьютерных сетях» отведено 159 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часа, лабораторные занятия – 30 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 4 зачетные единицы.

Форма текущей аттестации – зачет и экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел I. Введение

Тема 1.1. Введение в курс лекций. Предмет, цели и задачи курса. Актуальность задач построения, применение и анализ стойкости криптографических протоколов. Условные обозначения, принятые для схематичного отображения криптографических протоколов.

Тема 1.2. Криптографические протоколы: общие положения. Определение, назначение, область применения криптографических протоколов. Задачи, решаемые с помощью криптографических протоколов. Параметры, используемые для обеспечения подлинности сеанса связи: временные отметки, порядковые номера, случайные числа. Базовые схемы использования этих параметров.

Тема 1.3. Атаки на криптографические протоколы. Что понимается под атакой на криптографические протоколы. Модель угрозы Долева-Яо. Пассивная и активная атаки. Взаимодействие атакующего с каналом связи. Разновидности атак на криптографические протоколы.

Раздел II. Криптографические протоколы аутентификации

Тема 2.1. Введение в криптографические протоколы аутентификации. Определение понятий «идентификация», «аутентификация» и «авторизация». Разновидности протоколов аутентификации.

Тема 2.2. Протоколы простой аутентификации. Протоколы аутентификации, основанные на использовании одноразового пароля. Протоколы аутентификации, основанные на пароле пользователя.

Тема 2.3. Протоколы строгой аутентификации. Протоколы аутентификации Международных стандартов ISO/IEC 9798 части 2, 3, и 4, основанные на использовании симметричного алгоритма шифрования, цифровой подписи и кода аутентификации сообщений (MAC-коде); их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости.

Раздел III. Криптографические протоколы распределения ключей

Тема 3.1. Инфраструктура открытых ключей. Основные определения и понятия, связанные со структурой открытых ключей, структура сертификата и списка отозванных сертификатов X.509.

Тема 3.2. Управление ключами в криптографических системах и протоколах. Определение криптографического ключа и ключевой системы, основные функции по управлению ключами. Типы ключей в зависимости от

практического использования. Криптопериод ключа, типы ключей по криптопериоду. Способы распределения ключей. Классификация способов распределения ключей.

Тема 3.3. Криптографические протоколы распределения ключей, основанные на симметричной криптосистеме. Протоколы распределения ключей без использования третьей доверенной стороны, основанные на симметричной криптосистеме: протоколы, использующие необратимые функции; протоколы с использованием MAC-кода; протоколы Международных стандартов ISO/IEC 9798 части 2, 3, и 4, ISO/IEC 11770-2. Их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости.

Протоколы распределения ключей с участием третьей доверенной стороны, основанные на симметричной криптосистеме: протоколы Международных стандартов ISO/IEC 9798 части 2, 3, и 4, ISO/IEC 11770-2, протоколы Нидхема-Шредера, Деннинг-Сакко, Отвея-Риса. Их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости.

Тема 3.4. Криптографические протоколы распределения ключей, основанные на асимметричной криптосистеме. Протоколы формирования общего секретного ключа. Протоколы распределения ключей, основанные на асимметричной криптосистеме: протокол Нидхема-Шредера, Деннинг-Сакко и др. Их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости.

Раздел IV . Криптографические протоколы голосования

Тема 4.1. Криптографические протоколы голосования. Разновидности протоколов голосования. Протоколы голосования: протокол голосования с ЦИК и ЦУР, улучшенный протокол голосования, протокол голосования без ЦИК, протокол голосования с использование ЭЦП, числовой протокол голосования.

Раздел V. Практические криптографические протоколы

Тема 5.1. Практические криптографические протоколы. Обзор практических криптографических протоколов: OCSP, SSL/TLS, IPSEC, SSH, WEP, WPA2, WPA3.

Раздел VI. Защита информации в информационных системах и компьютерных сетях

Тема 6.1. Угрозы безопасности операционной системы. Подходы к построению защищенной операционной системы. Классификация угроз

безопасности операционной системы. Типичные атаки на операционную систему. Понятие защищенной операционной системы. Подходы к построению защищенных операционных систем. Административные меры защиты и политика безопасности. Стандарты защищенности операционных систем.

Тема 6.2. Аппаратное обеспечение средств защиты. Задачи аппаратного обеспечения защиты информации. Управление оперативной памятью. Планирование задач. Синхронизация параллельных задач. Обеспечение корректности совместного доступа к данным. Предотвращение тупиков. Аппаратная защита в процессорах x86. Адресация оперативной памяти, кольца защиты и уровни привилегий, селекторы и дескрипторы сегментов. Предотвращение выполнения данных.

Тема 6.3. Типовая архитектура подсистемы защиты операционной системы. Основные функции подсистемы защиты операционной системы. Разграничение доступа к объектам ОС. Избирательное, полномочное разграничение доступа, изолированная программная среда. Идентификация, аутентификация и авторизация субъектов доступа. Подсистема аудита операционной системы.

Тема 6.4. Защита в операционных системах Windows. Объекты, субъекты, методы, права доступа, привилегии. Разграничение доступа. Объекты доступа Windows. Субъекты доступа Windows: пользователи, псевдопользователи, обычные и специальные группы пользователей, относительные субъекты. Специфичные и стандартные методы доступа к объектам. Права доступа: специфичные, стандартные, отображаемые, виртуальные. Привилегии субъектов доступа. Элементы изолированной программной среды. Маркер доступа пользователя. Олицетворение пользователей. Дескриптор защиты объекта. Алгоритм проверки прав доступа субъекта к объекту. Назначение дескрипторов защиты новым объектам, наследование списков доступа. Мандатный контроль целостности и контроль учетных записей (UAC) в Windows 7/Windows 8/Windows 10. Изоляция привилегий пользовательского интерфейса (UIPI).

Идентификация, аутентификация, аудит. Архитектура подсистемы аутентификации Windows. Параметры аутентификации: ограничения на пароли, блокировка учетной записи, индивидуальные настройки параметров аутентификации отдельных пользователей, привилегии входа в систему. Средства защиты от перебора паролей. Усиленная аутентификация. Аудит в Windows: журнал аудита, политика аудита, категории событий аудита, порядок регистрации обращений пользователей к объектам операционной системы.

Встроенные средства криптографической защиты. Введение в инфраструктуру PKI. Криптографическая защита объектов файловой системы, EFS. Средство шифрования BitLocker.

Интеграция защищенных операционных систем в защищенную сеть. Доменная архитектура Windows. Плоская доменная архитектура. Понятие

домена. Контроллеры домена. Сквозная аутентификации, защита от перехвата и навязывания сетевого трафика при сквозной аутентификации. Порядок наделения пользователей домена правами и привилегиями, связь локальной политики безопасности компьютера с политикой безопасности домена. Отношения доверия между доменами. Лесная доменная архитектура. Понятие активного каталога. Структура активного каталога: объекты, атрибуты, их идентификация. Структура сети Windows: лес, дерево, организационная единица. Защита объектов активного каталога, наследование дескрипторов защиты, делегирование полномочий пользователей. Групповая политика. Интеграция активного каталога с почтовыми системами.

Тема 6.5. Защита в UNIX-системах. Объекты, субъекты, методы и права доступа в UNIX. Формат атрибутов защиты объекта доступа UNIX, порядок проверки прав доступа субъекта к объекту. Механизм SUID/SGID. Механизм SUDO. Аутентификация в UNIX, архитектура PAM. Интеграция UNIX в домены Windows. Аудит в UNIX.

Тема 6.6. Вредоносное программное обеспечение, программные закладки. Средства и методы защиты от программных закладок. Классификация вредоносного программного обеспечения. Разновидности программных закладок: вирусы, троянские программы, клавиатурные шпионы, мониторы информационных потоков. Модели взаимодействия программной закладки с атакуемой системой. Методы внедрения программных закладок. Сканирование системы на предмет наличия программных закладок. Контроль целостности программного обеспечения. Контроль целостности конфигурации системы. Антивирусный мониторинг информационных потоков. Программные ловушки.

Тема 6.7. Технологии резервного копирования и восстановления информации. Планирование и реализация резервного копирования. Встроенные средства ОС Windows. Средства сторонних производителей.

Тема 6.8. Принципы сетевого взаимодействия. Базовые принципы сетевого взаимодействия. Модель OSI. Стек протоколов TCP/IP. Сетевая архитектура операционной системы и модель OSI.

Тема 6.9. Безопасность физического и канального уровней. Безопасность физического и канального уровней. Сетевые анализаторы и «снифферы». Утилита Wireshark. Проблемы аутентификации на основе MAC-адреса. Проблемы безопасности протокола ARP. Варианты атак при помощи протокола ARP, ARP-Spoofing. Особенности работы механизма разрешения MAC-адресов в различных ОС. Утилита Cain. Обнаружение перехвата трафика и защита от атак на протокол ARP, утилита arpwatch. Безопасность беспроводных сетей Wi-Fi, основные направления атак в беспроводных сетях и методы защиты от них.

Тема 6.10. Безопасность сетевого и транспортного уровней. Безопасность сетевого уровня модели OSI. Протоколы IP и ICMP. Атака «Address spoofing». Атаки на протокол ICMP. Уязвимости механизма

фрагментации пакетов. Защита трафика на сетевом уровне. Протокол IPSec. Виртуальные частные сети. Протокол L2TP. Безопасность протокола IPv6. Безопасность транспортного уровня модели OSI. Протоколы TCP и UDP. Трансляция сетевых адресов NAT, служба маршрутизации и удаленного доступа Windows Server. Распределенные DoS-атаки, защита от них, «DoS-умножение». Методы сканирования портов, утилита nmap.

Тема 6.11. Безопасность прикладного уровня. Общие проблемы безопасности прикладного уровня модели OSI. Уязвимости протокола DHCP. Обнаружение ложного DHCP-сервера. Техника «обращенный-telnet». Утилита netcat. Механизм атаки DNS-Spoofing. Фреймворк Xerosploit, атаки «человек посередине», перехват HTTP трафика, атака SSLstrip. Обеспечение безопасности протоколов прикладного уровня (telnet, FTP, HTTP, IMAP, и др.).

Тема 6.12. Защита периметра сети. Межсетевые экраны. Защита периметра сети. Межсетевые экраны и их разновидности. Пакетные фильтры, технология SPI. Пакетный фильтр iptables в ОС Linux. Брандмауэр Windows. Обзор современных персональных брандмауэров. Защита от атаки «Address spoofing».

Тема 6.13. Анализ защищенности корпоративной сети. Обнаружение сетевых атак. Принципы анализа защищенности на сетевом уровне. Программа Internet Scanner. Обнаружение сетевых атак. Классификация систем обнаружения вторжений, архитектура систем обнаружения вторжений. Система Snort. «Honeynet» или сеть-приманка для изучения поведения нарушителей, утилита honeyd, проект HoneyNet. Анализ безопасности беспроводных сетей. Утилита CommView for WiFi. Проект WiFi pineapple.

Тема 6.14. Принципы функционирования средств захвата и фильтрации трафика. Сетевая архитектура ОС Windows. Программные интерфейсы сетевого взаимодействия: winsock, TDI, NDIS. Типы и структура NDIS-драйвера. Создание простейшего «сниффера». Создание простейшего пакетного фильтра (файервола) на основе примеров из WDK (passthru, netlwf).

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов			Количество часов в УСР	Форма контроля знаний
		Лекции	Семинарские Занятия	Лабораторные занятия		
1	**Введение**	**3**				
1.1	Введение в курс лекций.	1				Устный опрос
1.2	Криптографические протоколы: общие положения.	1				Устный опрос
1.3	Атаки на криптографические протоколы.	1				Устный опрос
2	**Криптографические протоколы аутентификации**	**7**				
2.1	Введение в криптографические протоколы аутентификации.	1				Устный опрос
2.2	Протоколы простой аутентификации.	2				Устный опрос
2.3	Протоколы строгой аутентификации.	4				Защита подготовленного реферата
3	**Криптографические протоколы распределения ключей**	**10**				
3.1	Инфраструктура открытых ключей.	1				Устный опрос
3.2	Управление ключами в криптографических системах и протоколах.	1				Устный опрос
3.3	Криптографические протоколы распределения ключей, основанные на	4				Устный опрос

	симметричной криптосистеме.					
3.4	Криптографические протоколы распределения ключей, основанные на асимметричной криптосистеме.	4				Устный опрос.
4	**Криптографические протоколы голосования**	**2**				
4.1	Криптографические протоколы голосования	2				Устный опрос, коллоквиум.
5	**Практические криптографические протоколы**	**12**				
5.1	Практические криптографические протоколы	12				Устный опрос
6	**Защита информации в информационных системах и компьютерных сетях**			**30**	**4**	
6.1	Угрозы безопасности операционной системы. Подходы к построению защищенной операционной системы			2		Защита лабораторной работы
6.2	Аппаратное обеспечение средств защиты			2		Защита лабораторной работы
6.3	Типовая архитектура подсистемы защиты операционной системы.			2	2	Защита лабораторной работы.
6.4	Защита в операционных системах Windows. Объекты, субъекты, методы, права доступа, привилегии.			2		Защита лабораторной работы
	Идентификация, аутентификация, аудит			2		Защита лабораторной работы
	Встроенные средства криптографической защиты			2		Защита лабораторной работы

	Интеграция защищенных операционных систем в защищенную сеть			2		Защита лабораторной работы. Контрольная работа №1.
6.5	Защита в UNIX-системах			2		Защита лабораторной работы.
6.6	Вредоносное программное обеспечение, программные закладки. Средства и методы защиты от программных закладок			2		Защита лабораторной работы
6.7	Технологии резервного копирования и восстановления информации				2	Устный опрос
6.8	Принципы сетевого взаимодействия			2		Защита лабораторной работы
6.9	Безопасность физического и канального уровней			2		Защита лабораторной работы. Контрольная работа №2
6.10	Безопасность сетевого и транспортного уровней			2		Защита лабораторной работы.
6.11	Безопасность прикладного уровня			2		Защита лабораторной работы.
6.12	Защита периметра сети. Межсетевые экраны			2		Защита лабораторной работы.
6.13	Анализ защищенности корпоративной сети. Обнаружение сетевых атак			2		Защита лабораторной работы. Контрольная работа №2
6.14	Принципы функционирования средств захвата и фильтрации трафика			2		Защита лабораторной работы.
ИТОГО		**34**		**30**	**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Харин Ю.С. [и др.] Криптология: учебник. – Минск: БГУ, 2013. – 511 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходный код на Си. – Москва: Вильямс, 2016.
3. Столлингс В. Криптография и защита сетей: принципы и практика. – Москва: Вильямс, 2001.
4. М. Руссинович, Д. Соломон. Внутреннее устройство Microsoft Windows, 6-е издание (Часть 1). Издательство: Питер, 2013. – 800 с.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2006. – 672 с.
6. В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков. Защита информации в компьютерных сетях Практический курс: учебное пособие. Екатеринбург: УГТУ-УПИ, 2007. - 246 с.
7. Норберт Польман, Тим Кразерс. Архитектура брандмауэров для сетей предприятия. Издательство: Вильямс, 2003 г. – 432 с.

Перечень дополнительной литературы

1. Сидни Фейт, пер.: М. Кузьмин. TCP/IP. Архитектура, протоколы, реализация (включая IPv6 и IP Security). Издательство: Лори, 2009 г.- 424 с
2. Роберта Брэгг, Марк Родс-Оусли, Кит Страссберг. Безопасность сетей. Полное руководство. – Издательство: Эком, 2006. – 912 с
3. Фленов М. Linux глазами хакера. – Издательство: БХВ-Петербург, 2006 г. – 544 с.
4. Брайан Хатч, Джеймс Ли, Джордж Курц. Секреты хакеров. Безопасность Linux - готовые решения. – Издательство: Вильямс, 2002 г. – 544 с.

Рекомендуемая тематика контрольных работ

1) Контрольная работа №1. Защита в операционных системах Windows.

2) Контрольная работа №2. Анализ защищенности корпоративной сети. Обнаружение сетевых атак

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине следует использовать современные информационные

технологии: разместить в сетевом доступе комплекс учебных и учебно-методических материалов (учебно-программные материалы, ссылки на учебные издания для теоретического изучения дисциплины, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, задания, тесты, вопросы для самоконтроля, тематика рефератов и др., список рекомендуемой литературы, информационных ресурсов и др.). Эффективность самостоятельной работы студентов проверяется в ходе текущего и итогового контроля знаний. Для общей оценки качества усвоения студентами учебного материала рекомендуется использование рейтинговой системы.

Перечень рекомендуемых средств диагностики

Для текущего контроля качества усвоения знаний студентами используется следующий диагностический инструментарий:

1. Устная форма: устные опросы; защиты отчетов по домашним заданиям, при выполнении студентами лабораторных работ; проведение коллоквиума; защита подготовленного студентом реферата (рефераты используются для обобщения и систематизации учебного материала; в процессе подготовки реферата студент мобилизует и актуализирует имеющиеся умения, приобретает самостоятельно новые знания, необходимые для раскрытия темы, сопоставляя разные позиции и точки зрения).
2. Письменная форма: письменные контрольные работы по отдельным темам учебной дисциплины.

Методика формирования итоговой оценки

Формой текущей аттестации по учебной дисциплине «Криптографические протоколы. Защита информации в информационных системах и компьютерных сетях» учебным планом предусмотрены зачет и экзамен.

Рекомендуется использовать рейтинговую оценку знаний студента магистратуры, дающую возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине. Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний в рейтинговую оценку:

- подготовка реферата – 15 %;
- работа на лабораторных занятиях – 35 %;

- контрольные работы – 30 %;
- коллоквиум – 20 %.

Итоговая оценка формируется на основе:

1) Правил проведения аттестации студентов (Постановление Министерства образования Республики Беларусь № 53 от 29 мая 2012г.);
2) Положение о рейтинговой системе оценки знаний по дисциплине в БГУ (Приказ ректора БГУ от 18.08.2015 № 382-ОД);
3) Критериев оценки знаний студентов (письмо Министерства образования от 22.12.2003).

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Системы связи и сети передачи информации	Телекоммуникаций и информационных технологий	нет	Оставить содержание учебной дисциплины без изменения, протокол № 13 от 29.03.2018 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры _____ (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой

_____ _____ _____

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____