МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины **Б1.В.ДВ.05.01 Техническая защита объектов критической информационной инфраструктуры**
Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки направленность (профиль) N 7 "Техническая защита информации"

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

стр.

1. Цели и задачи дисциплины

Целью курса «Техническая защита объектов критической информационной инфраструктуры» является формирование у студентов системных знаний по обеспечению информационной безопасности критической информационной инфраструктуры, а также практических навыков по разработке и реализации планов реагирования на компьютерные инциденты.

В состав задач изучения дисциплины входят:

- Формирование системных знаний о значимых объектах критической информационной инфраструктуры, а также методах и средствах обеспечения их безопасности.
- Изучение нормативно-правовых актов по безопасности критической информационной инфраструктуры.
- Изучение методов оценки уровня защищенности (аудита) систем и сетей и содержащейся в них информации.
- Освоение необходимых знаний по проведению категорирования объектов критической информационной инфраструктуры.
- Формирование умений и знаний по проведению оценки угроз безопасности информации на объектах критической информационной инфраструктуры.
- Изучения механизма проведения инвентаризации систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств.
- Освоение методов организации и планирования мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Техническая защита объектов критической информационной инфраструктуры» входит в вариативную часть дисциплин.

В структуре ОПОП дисциплина входит в вариативную часть программы и является продолжением курсов «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации от несанкционированного доступа» связанным с освоением продвинутых основ по обеспечению информационной безопасности критической информационной инфраструктуры.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты. В результате изучения дисциплины студент должен:

Знать: нормативно правовые акты и методические документы по обеспечению информационной безопасности критической информационной инфраструктуры.

Уметь: администрировать системы информационной безопасности объектов критической информационной инфраструктуры.

Владеть: навыками контроля деятельности по выполнению требований к

функционированию системы защиты информации на объектах критической информационной инфраструктуры.

ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате изучения дисциплины студент должен:

Знать: нормативно правовые и методические документы по созданию систем защиты информации объектов критической информационной инфраструктуры.

Уметь: определять требования к созданию и функционированию систем защиты информации объектов критической информационной инфраструктуры.

Владеть: навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ Российской Федерации, ФСТЭК.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		8			
Аудиторные занятия (всего)	78/2.1	78/2.1			
В том числе:	-	-	-	-	-
Лекции	44/1,2	44/1,2			
Практические занятия (ПЗ)	22/0.6	22/0.6			
Семинары (С)					
Лабораторные работы (ЛР)	-	-			
КСР	12/0.3	12/0.3			
Самостоятельная работа (всего)	30/0.8	30/0.8			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	30/0.8	30/0.8			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	78/2.1	78/2.1			
Общая трудоемкость часы	108	108			

зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

Т 1. Правовые основы обеспечения безопасности КИИ Российской Федерации

Т 2. Угрозы безопасности информации, обрабатываемой на объектах КИИ

Т3. Категорирование объектов КИИ

Т4. Требования по обеспечению безопасности значимых объектов КИИ

Т5. Система безопасности значимого объекта КИИ

Т6. Стадии (этапы) работ по созданию системы безопасности

Т7. Контроль за обеспечением безопасности значимого объекта КИИ

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Б2.В.04(П) Преддипломная практика	1-7
2	Б3.Б.01(Д) Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	1-7

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	4	2			2	8
2.	***Раздел 2***	Тема 2	4	2			2	8
3.	***Раздел 3***	Тема 3	6	2			4	12
4.	***Раздел 4***	Тема 4	10	4			6	20
5.	***Раздел 5***	Тема 5	12	8			8	28
6.	***Раздел 6***	Тема 6	6	2			4	12
7.	***Раздел 7***	Тема 7	2	2			4	8

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1***	Практическая работа №1	2	Тестовый контроль по теме	ПК-3; ПК-15
2.	***Раздел 2***	Практическая работа №2	2	Тестовый контроль по теме	ПК-3; ПК-15
3.	***Раздел 3***	Практическая работа №3	2	Тестовый контроль по теме	ПК-3; ПК-15
4.	***Раздел 4***	Практическая работа №4	4	Тестовый контроль по теме	ПК-3; ПК-15
5.	***Раздел 5***	Практическая работа №5	8	Тестовый контроль по теме	ПК-3; ПК-15
6.	***Раздел 6***	Практическая работа №6	2	Тестовый контроль по теме	ПК-3; ПК-15
7.	***Раздел 7***	Практическая работа №7	2	Тестовый контроль по теме	ПК-3; ПК-15

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-3**	Подготовка к контрольной работе	№1	Учебный сайт	8
8		Контрольная работа		Учебный сайт	
9		Подведение итогов по контрольной работе. Работа над ошибками по контрольной работе.		Учебный сайт	
10	**4-7**	Подготовка итоговой зачетной работы	№2	Учебный сайт	22
11		Подготовка доклада с		Учебный сайт	

		презентацией			

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой студент активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

В процессе проведения самостоятельной работы формируется компетенция ОПК-5; ПК-7. Контроль самостоятельной работы на лабораторных занятиях и на КСР, по окончании соответствующих тем.

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1. Технические средства и методы защиты информации. Технические средства и методы защиты информации. Учебно-практическое пособие. Москва: Евразийский открытый ин-т, 2011 100% онлайн. https://search.rsl.ru/ru/record/01006553324С.А.

б) базы данных, информационно-справочные и поисковые системы:

1. Учебный сайт Лаборатории ТЗИ Физического факультета ИГУ - – Режим доступа: https://sites.google.com/view/ltzi/, свободный.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория и лекционная аудитория, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

Программное обеспечение:

1. 1. M Microsoft Access 2019, Microsoft SQL Server, Oracle Server

10. Образовательные технологии

Для достижения планируемых результатов обучения, при изучении дисциплины «Основы информационной безопасности» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем

проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль (6 вариантов, 8-й семестр), представляет собой перечень из 10 вопросов и заданий. Входной контроль проводится в письменном виде на первом лабораторном занятии в течение 15 минут. Проверяется уровень входных знаний.

11.2. Оценочные средства текущего контроля

Текущий контроль осуществляется за счет контроля решенных задач на лабораторных занятиях, а также решения задач на лекционных занятиях, в том числе у доски.

В конце каждой темы, на последнем лабораторном занятии студенты выполняют специальное задание, с написанием отчета. Данное задание предназначено для проверки усвоения теоретического материала, а также навыков выполнения практических и творческих задач, связанных с разработкой программного обеспечения и работы с различными БД и СУБД. Таким образом, в течение курса студенты должны выполнить 10 спецзаданий, и получить оценку за задание и отчет по нему.

За выполнение каждого специального задания студент может набрать максимум 10 баллов. Баллы, за каждое из выполненных спецзаданий заносятся в индивидуальный семестровый рейтинг студента, и используются при проведении промежуточной аттестации по дисциплине. При наборе менее 5 баллов спецзадание считается не выполненным.

Кол-во баллов	Критерии оценивания	Оценка за спецзадание
5-6	Цели задания усвоены полностью, формулировки корректны и точны. Практическое задание выполнено, но допущены ошибки, не носящие	«удовлетворительно»

	критический характер. В отчете присутствуют серьезные ошибки, структура отчета недостаточно проработана, не все факторы отражены. При этом цели и задачи в общем достигнуты и отражены в отчете.	
7-8	Цели задания усвоены полностью, формулировки корректны и точны. Практическая часть выполнена полностью, без серьезных ошибок и замечаний, все цели и задачи выполнены и реализованы. В отчете отражены все основные моменты выполнения спецзадания, но могут присутствовать небольшие неточности и ошибки в изложении фактов.	«хорошо»
9-10	Цели задания усвоены полностью, формулировки корректны и точны. Практическая часть выполнена полностью, без ошибок и замечаний, все цели и задачи выполнены и реализованы. В отчете отражены все основные моменты выполнения спецзадания, структура отчета логична и последовательна, отсутствуют ошибки оформления и изложения всех аспектов выполненной работы.	«отлично»

ТЕСТОВЫЕ ВОПРОСЫ ПО ДИСЦИПЛИНЕ

Б1.В.ДВ.05.01 Техническая защита объектов критической информационной инфраструктуры

КОМПЕТЕНЦИИ ПК-3; ПК-15

Вариант 1

1. Безопасность критической информационной инфраструктуры:

а) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак:
б) обеспечение безопасного уровня защиты информации для обеспечения устойчивого функционирования критической информационной инфраструктуры
в) состояние защиты информации критической информационной инфраструктуры обеспечивающее её устойчивое функционирование.

2. Значимый объект критической информационной инфраструктуры:
а), объект критической информационной инфраструктуры который включен в реестр значимых объектов критической информационной инфраструктуры;
б). объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;
в). объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости

3. Объекты критической информационной инфраструктуры:
а). объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия с автоматизированными системами управления;
б). объекты информационной инфраструктуры, прошедшие процедуру категорирования;
в). информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

4. Принципами обеспечения безопасности критической информационной инфраструктуры являются:
а). законность, непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;
б). приоритет предотвращения компьютерных атак, законность;
в). законность, непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры, приоритет предотвращения компьютерных атак.

5. Категорирование объекта критической информационной инфраструктуры:
а). процедура установления объекту критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения;
б). установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений;
в). установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

6. **Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:**
а). предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
б). недопущение воздействия на технические средства обработки информации, обеспечение функционирования значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры.

7. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение:

а). отсутствие доступа к государственной услуге в течении, которого государственная услуга может быть недоступна для получателей;

б). причинение ущерба жизни и здоровью людей;

в). прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны.

8. Максимальный срок категорирования не должен превышать;

а). одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений);

б). двух лет со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений);

в). 6 месяцев со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений).

9. Создание и функционирование систем безопасности должно быть направлено на;

а). обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак;

б). обеспечение защиты значимых объектов критической информационной инфраструктуры от компьютерных атак;

в). обеспечение функционирования значимых объектов критической информационной инфраструктуры при возникновении угроз информационной безопасности.

10. Системы безопасности должны обеспечивать:

а). восстановление функционирования системы безопасности значимых объектов критической информационной инфраструктуры;

б). недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов критической информационной инфраструктуры

в). устойчивое функционирование системы безопасности значимых объектов критической информационной инфраструктуры.

11. К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся:

а). подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры;

б). подразделения (работники), участвующие в подготовке плана безопасности значимого объекта критической информационной инфраструктуры.

в). подразделения (работники), эксплуатирующие значимые объекты критической информационной инфраструктуры.

12. Организационно-технические меры по обеспечению безопасности значимого объекта должны включать:

а). анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);

б) разработку технического задания на создание системы безопасности значимого объекта;

в) разработку рабочей (эксплуатационной) документации на систему защиты

13. Модель угроз безопасности информации должна содержать:

а). краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;

б). числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;
в). краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации.

14. Кем осуществляется государственный контроль за обеспечением уровня безопасности значимого объекта КИИ осуществляет;

а). ФСБ;
б). ФСТЭК;
в). Органами прокуратуры РФ.

15. Ответственность за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

а). дисциплинарная;
б). дисциплинарная и административная;
в). дисциплинарная, гражданско-правовая, административная и уголовная ответственность.

11.3. Оценочные средства для промежуточной аттестации

Промежуточная аттестация проводится в форме зачета.

Примерные вопросы к зачету

1. Объекты и субъекты. Права и обязанности субъектов КИИ.
2.Полномочия органов государственной власти Российской Федерации в обеспечения безопасности КИИ.
3.Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ.
5.Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ
6.Права и обязанности субъектов КИИ.
7.Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.
9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.
10. Правила и порядок категорирования объектов КИИ.
11. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.
12.Формирование комиссии по категорированию объектов КИИ Российской Федерации.
13.Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ.
14.Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управления, контроль и мониторинг критических процессов.
15. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение.
16. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

17. Формирования перечня объектов КИИ Российской Федерации, подлежащих категорированию.
18.Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации.
19.Формирование сведений о результатах категорирования объектов КИИ,
20.Устанеовление требований по обеспечению безопасности значимого объекта КИИ.
21. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.
22. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.
23. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.
24. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.
25. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности.
26. Требования к созданию систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.
27. Требования к силам обеспечения безопасности значимого объекта КИИ.
28.Требования к организационно-распорядительным документам по безопасности значимого объекта КИИ.
29. Перечень необходимых документов в рамках создания систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.
30. Этапы жизненного цикла системы безопасности значимого объекта КИИ.
31. Стадии (этапы) работ по созданию системы безопасности значимого объекта КИИ.
32.Внедрение системы безопасности значимого объекта КИИ.
33. Контроль за обеспечением уровня безопасности значимого объекта КИИ.
34.Мониторинг событий безопасности и контроль за действиями персонала значимого объекта КИИ.
35.Оценка соответствия значимых объектов КИИ требованиям безопасности.
36. Документирование процедур и результатов контроля за обеспечением безопасности значимого объекта КИИ.
37. Ответственность за нарушения законодательства о безопасности КИИ Российской Федерации.

Разработчик:

Доцент кафедры РФиРЭ  Серёдкин С.П.

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ОПОП по направлению и профилю подготовки **10.03.01 Информационная безопасность.**

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой  Колесник С.Н.