

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 13.10.2023 13:56:09
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»



Утверждаю:

Руководитель ООП:

Смирнов Н.А. Семькина

« 9 » 06 2023 г.

Рабочая программа дисциплины (с аннотацией)

Криптографические протоколы

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 5 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составитель: Желтая

ст. преподаватель С.А. Желтая.

Тверь 2023

І. Аннотация

1. Наименование дисциплины (модуля) в соответствии с учебным планом
Криптографические протоколы.

2. Цель и задачи дисциплины (модуля)

Целью освоения дисциплины (модуля) является:

формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических протоколов, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

- получение базовых знаний и умений, связанных с основными понятиями криптографических протоколов;
- получение теоретических знаний о роли и назначении различных криптографических протоколов;
- обучения студентов общим принципам и методам построения криптографических протоколов;
- получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью криптопротоколов;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в базовую часть профессионального цикла.

Для освоения дисциплины студент должен владеть основными понятиями криптографии, информационной безопасности. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам Организационное и правовое обеспечение информационной безопасности, информатика, криптографические методы защиты информации, теоретико-числовые методы в криптографии. Знания и практические навыки, полученные из курса, используются студентами при прохождении производственной и преддипломной практики, а также при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):

___3___ зачетных единиц, ___108___ академических часов, **в том числе контактная работа:** лекции ___36___ часов, практические занятия ___18___ часов, **самостоятельная работа:** ___54___ часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| | |
|--|---|
| Планируемые результаты освоения образовательной программы | Планируемые результаты обучения по дисциплине (модулю) |
|--|---|

| | |
|--|--|
| (формируемые компетенции) | |
| <p>ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации</p> | <p>Владеть: навыками освоения большого объема информации и решения задач (в том числе, сложных). Уметь: самостоятельно находить информацию по алгоритмам решения задач, в том числе и нестандартных, и проводить их анализ. Знать: основы Интернет-технологий, современные проблемы соответствующих разделов криптографии.</p> |
| <p>Базовый ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.</p> | <p>Владеть: криптографической терминологией; простейшими подходами к анализу безопасности криптографических протоколов. Уметь: использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов; формулировать свойства безопасности криптографических протоколов; проводить сравнительный анализ криптографических протоколов, решающих сходные задачи. Знать: криптографические протоколы, применяемые в компьютерных сетях; формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям; криптографические стандарты; основные схемы цифровой подписи.</p> |

6. Форма промежуточной аттестации:
экзамен.

7. Язык преподавания русский.

II. Содержание дисциплины (или модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Для студентов очной формы обучения

| Учебная программа – наименование разделов и тем | Всего (час.) | Контактная работа (час.) | | Самостоятельная работа (час.) |
|--|--------------|--------------------------|-------------------------------------|-------------------------------|
| | | Лекции | Практические (лабораторные) занятия | |
| Раздел 1. Основные понятия криптопротоколов | | | | |
| Тема 1.1. Криптографические протоколы: основные понятия и основные требования к ним. | 7 | 2 | 2 | 3 |
| Тема 1.2. Классификация криптографических протоколов | 7 | 2 | 2 | 3 |
| Тема 1.3. Протоколы аутентификации и идентификации. | 9 | 4 | 2 | 3 |
| Тема 1.4. Парольные схемы разграничения доступа. | 11 | 6 | 2 | 3 |
| Тема 1.5. Протоколы генерации и распространения ключей | 9 | 4 | 2 | 3 |
| Тема 1.6. Рекомендации X.509 | 9 | 4 | 2 | 3 |
| Тема 1.7. Протоколы разделения секретов | 11 | 6 | 2 | 3 |
| Тема 1.8. Протоколы с нулевым разглашением, д-во нулевого разглашения | 9 | 4 | 2 | 3 |
| Тема 1.9. Протоколы «игры в покер» | 9 | 4 | 2 | 3 |
| ИТОГО | 81 | 34 | 18 | 27 |

Учебная программа

Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОПРОТОКОЛОВ

Тема 1.1. Криптографические протоколы: основные понятия и основные требования к ним.

Определение криптографического протокола. Задачи, решаемые с помощью криптографических протоколов. Требования и функции криптографических протоколов.

Тема 1.2. Классификация криптографических протоколов

Виды протоколов и их классификация.

Тема 1.3. Протоколы аутентификации и идентификации

Протоколы аутентификации и идентификации. Слабая и сильная идентификация.

Тема 1.4. Парольные схемы разграничения доступа.

Парольные схемы разграничения доступа.

Тема 1.5. Протоколы генерации и распространения ключей

Протокол Диффи-Хелмана и его модификации. Схемы управления ключами: централизованное и децентрализованное.

Тема 1.6. Рекомендации X.509

Рекомендации X.509.

Тема 1.7. Протоколы разделения секретов

Протоколы разделения секретов, основные виды. (n,k) пороговая схема разделения секрета. Разделение секрета с подтверждением.

Тема 1.8. Протоколы с нулевым разглашением, д-во нулевого разглашения

Протокол на основе задачи об изоморфизме графов. Протокол -Фиата-Шамира

Тема 1.9. Протоколы «игры в покер»

. Протоколы «игры в покер».

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Самостоятельная работа обучающихся направлена на освоение учебного материала и развитие практических умений. Самостоятельная работа включает следующие виды самостоятельной работы студентов: работа с рекомендованной литературой и документацией; выполнение практических заданий; подготовка к контрольным .

Тематика рефератов и методические рекомендации по их написанию.

1. Протоколы аутентификации с использованием eToken.
2. Обзор современных программных средств ЭЦП.
3. Неоспоримые цифровые подписи.
4. Перехват паролей пользователей ИС программными средствами.
5. Перехват паролей пользователей ИС аппаратными средствами.
6. Генерация паролей и их проверка их стойкости.

Вопросы для контрольных тестов и самоконтроля.

1. Что такое криптографический протокол?
2. Назовите основные виды криптографических протоколов
3. Приведите классификацию криптографических протоколов.
4. Сформулируйте требования к паролю.

5. Какую задачу решает протокол Диффи Хелмана.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

Типовые контрольные задания для проверки уровня сформированности компетенций ОПК -3, ПК-3 .

Рассматривается трехкомпонентной структура компетенции: знать, уметь, владеть.

При этом под указанными категориями понимается:

- «знать» – воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;
- «уметь» – решать типичные задачи на основе воспроизведения стандартных алгоритмов решения;
- «владеть» – решать усложненные задачи на основе приобретенных знаний, умений и навыков, в нетипичных ситуациях

| Этап формирования компетенции, в котором участвует дисциплина | Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера) | Показатели и критерии оценивания компетенции, шкала оценивания |
|---|--|---|
| Базовый | | |
| владеть | Основными понятиями криптографических протоколов | <ul style="list-style-type: none"> • Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части описания из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов |
| | Алгоритмами реализующими вычислительные операции | <ul style="list-style-type: none"> • Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ |

| | | |
|--------------|---|--|
| | | дано неверное решение – 0 баллов |
| уметь | Описывать схемы и алгоритмы реализующие криптографические протоколы | <ul style="list-style-type: none"> • Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов |
| | Определить Тип протокола по решаемой задаче. | <ul style="list-style-type: none"> • Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов |
| знать | Основные криптографические протоколы. | <ul style="list-style-type: none"> • Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов |
| | Параметры криптографических протоколов | <ul style="list-style-type: none"> • Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов |
| | навыками | <ul style="list-style-type: none"> • Факты и примеры в полном |

| | | |
|----------------|---|---|
| владеть | доказательств утверждений и теорем | <p>объеме обосновывают выводы – 2 балла</p> <ul style="list-style-type: none"> • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов |
| уметь | Формулировать (описывать) алгоритмы схемы реализующие криптографические протоколы | <ul style="list-style-type: none"> • Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за алгоритмической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов |
| знать | Стандарты использования криптографических протоколов | <ul style="list-style-type: none"> • Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов |
| | Требования (рекомендации) к криптографическим протоколам | <ul style="list-style-type: none"> • Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов |

При оценивании результатов освоения дисциплины применяется «рейтинговая» технология (балльно-накопительная) система. Оценка уровня сформированности компетенций осуществляется в процессе следующих форм контроля:

1) **слеящего** (проводится оценка выполнения студентами заданий в ходе аудиторных занятий). Дает возможность квалифицировать степень сформированности знаний, умений, навыков, а также их глубину и прочность. Его задача - регулярное управление учебной деятельности студентов и ее корректировка. Он позволяет получать первичную информацию о ходе и качестве усвоения учебного материала, а также стимулировать регулярную, напряженную и целенаправленную работу студентов. Данный контроль позволяет вовремя выявить пробелы в знаниях и оказать им помощь в усвоении программного материала. Данными формами контроля являются: ответы с места и у доски, проверка работ выполненных в тетради.

2) **текущего** (оценивается работа студентов вне аудиторных занятий). Текущими формами контроля являются: проверка выполнения практических работ, ответы у доски, рефераты, доклады, проверка самостоятельной работы студентов.

3) **промежуточного** (рейтинговые точки) позволяет определять качество изучения студентами учебного материала по разделам и темам. Контроль проводится два раз в семестр. С помощью периодического контроля обобщаются и усваиваются целые темы и разделы, выявляются взаимосвязями с другими разделами, предметами. Контроль охватывает студентов и всей группы и проводится в виде теста, письменных практических работ.

4) **итогового** (зачёт). Максимальная сумма рейтинговых баллов по дисциплине составляет 100 баллов. Студенту, набравшему 50 баллов и выше по итогам работе в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший от 20 до 49 баллов включительно, сдаёт зачет в последнюю неделю семестра по данной дисциплине. Баллы, полученные на зачете проставляются в ведомости. Студенту, набравшему меньше 20 баллов, в экзаменационной ведомости выставляется оценка «незачтено». Данному студенту разрешается передача зачета по направлению деканата на последней неделе семестра.

Формы контроля

Занятия для студентов очной формы обучения проводятся в 1-м семестре 5 курса и заканчиваются зачетом. Период времени, отведенный на обучение по данной дисциплине, планируется разделить на 2 модуля, каждый из которых заканчивается контрольной точкой. Количество баллов за текущую работу выставляется в соответствии со сложностью темы и количеством заданий, выносимых для практических работ в аудитории и самостоятельных занятий.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы.

Для оценки уровня теоретических и практических знаний используется тест или контрольная работа письменный опрос. Перечень некоторых вопросов теста и практических заданий представлен ниже.

Приводится два варианта из имеющихся двадцати различных вариантов по каждой из рассматриваемых тем.

Вариант 1

1. Опишите схему протокола генерации ключей Диффи Хелмана
2. Опишите общую схему разделения секрета

Вариант 2

1. Приведите пример протокола сильной идентификации
2. Приведите классификацию протоколов

ВОПРОСЫ К ЗАЧЕТУ 9 СЕМЕСТРА

Вопросы по дисциплине «криптографические протоколы» (зачет).

1. Понятие и назначение криптографических протоколов.
2. Классификация протоколов (по видам, по выполняемой задаче, по способу генерации ключевой информации)
3. Атаки на протоколы
4. Протоколы идентификации
5. Протоколы аутентификации
6. Парольные схемы разграничения доступа.
7. Протоколы генерации и распределения ключей
8. Рекомендации X.509
9. Протоколы разделения секрета (общая схема)
10. (n, k) пороговые схемы разделения секрета (идеальные СРС, способы их математического описания)
11. Схема Шамира разделения секрета
12. Протоколы с нулевым разглашением*
13. Д-во нулевого разглашения*
14. Протоколы игры в покер.*
15. Однонаправленные функции
16. Хеш-функции
17. Неоспоримые цифровые подписи
18. Управление ключами

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература

Лапони́на, О.Р. Криптографические основы безопасности / О.Р. Лапони́на. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429092>.

Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1716-6>. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1899016>

б) Дополнительная литература:

Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469758>

Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие для СПО / Б. А. Фороузан ; под редакцией А. Н. Берлина. — Саратов : Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102192.html>

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (или модуля)

1. ЭБС Лань <https://e.lanbook.com/> Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com <https://znanium.com/> Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online <https://biblioclub.ru> Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ <https://urait.ru/> Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART <https://www.iprbookshop.ru/> Договор № 3-е/23К от 02.08.2023 г.
6. <https://cyberleninka.ru/> научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозиторий ТвГУ <http://eprints.tversu.ru>
9. [Информационная безопасность на Report.ru](http://Report.ru)
10. [Информационная безопасность / Блог / Хабрахабр](#)
11. [Библиотека информационной безопасности](#)
12. [Библиотека сетевой безопасности](#)
13. [Компьютерная безопасность: уязвимости, ошибки и эксплоиты](#)
14. [Построение безопасности в сетях](#)
15. [openPGP в России](#)
16. [Защита информации](#)

VII. Методические указания для обучающихся по освоению дисциплины (или модуля)

Материал дисциплины распределен по главным разделам (темам). В результате изучения дисциплины у студентов должно сформироваться научное представление о криптографических системах на базе эллиптических кривых. Необходимо выработать системный подход к пониманию процессов преобразования входных данных в приложениях защиты информации. В процессе обучения студенты, наряду с текстами лекций и учебными пособиями, должны пользоваться дополнительными научными изданиями, академическими периодическими изданиями. После каждой лекционной темы рекомендуется проработать вопросы для повторения и самоконтроля. В аспекте самостоятельной работы рекомендуется составлять конспект. Рекомендуется использовать справочники и руководства.

Для успешного освоения дисциплины важно соблюсти следующие рекомендации: На первой лекции важно обратить внимание на конкретные требования к прохождению и сдаче курса. Активная работа на занятиях, выполнение творческих заданий сформирует о Вас дополнительное положительное представление как об активном участнике познавательного процесса. На данном курсе практические занятия являются самым важным компонентом обучающего процесса. На занятиях будет представлен необходимый теоретический материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, настоятельно рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам в библиотеках и системе «Интернет». Самостоятельная работа является необходимой на всех стадиях и при всех формах изучения предмета. Важно помнить: без самостоятельной работы невозможно серьезное освоение любого курса. Надо быть готовым к тому, что по времени, затраченному на дисциплину, самостоятельная работа будет превалировать над иными видами работы. Важно продумать стиль фиксации нового и важного материала. Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (или модулю), включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Процесс изучения дисциплины включает лекции, практические занятия и самостоятельную работу студента. Во время обучения применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении занятий применяется имитационный подход (метод деловой игры, анализ конкретных ситуаций), когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания. Так же при проведении занятий применяется частично-поисковый метод: студенты осуществляют поиск решения поставленной проблемы (задачи). При этом постановочные задачи опираются на уже имеющиеся у студентов знания и умения, полученные в предшествующих темах. На занятиях практикуется выполнение заданий в малых группах, письменные работы, работа с раздаточным материалом, привлекаются ресурсы сети Интернет. Курс предусматривает выполнение тестов, контрольных и самостоятельных работ, письменных домашних заданий. В качестве форм контроля используются различные варианты взаимопроверки и взаимоконтроля.

Программное обеспечение

| | |
|--|--|
| Adobe Acrobat Reader DC - Russian | бесплатно Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009 |
| Cadence SPB/OrCAD 16.6 | бесплатно |
| Git version 2.5.2.2 | бесплатно |
| Google Chrome | бесплатно |
| Kaspersky Endpoint Security 10 для Windows | Акт на передачу прав ПК545 от 16.12.2022 |
| Lazarus 1.4.0 | бесплатно |
| Mathcad 15 M010 | Акт предоставления прав ИС00000027 от 16.09.2011; Акт предоставления прав № Us000311 от 25.09.2012; |
| MATLAB R2012b | |
| Многофункциональный редактор ONLYOFFICE | бесплатно |
| ОС Linux Ubuntu бесплатное ПО | бесплатно |
| Microsoft Web Deploy 3.5 | бесплатно |
| MiKTeX 2.9 | бесплатно |
| MSXML 4.0 SP2 Parser and SDK | бесплатно |
| MySQL Workbench 6.3 CE | бесплатно |
| NetBeans IDE 8.0.2 | бесплатно |
| Notepad++ | бесплатно |
| Origin 8.1 Sr2 | договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»; |
| PostgreSQL 9.6 | бесплатно |
| Python 3.4.3 | бесплатно |
| Visual Studio 2010 Prerequisites - English | Акт на передачу прав №785 от 06.08.2021 г. |
| WCF RIA Services V1.0 SP2 | бесплатно |
| WinDjView 2.1 | бесплатно |
| WinPcap 4.1.3 | бесплатно |
| Wireshark 2.0.0 (64-bit) | бесплатно |
| R studio | бесплатно |

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (или модулю)

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

| №п.п. | Обновленный раздел рабочей программы дисциплины (или модуля) | Описание внесенных изменений | Дата и протокол заседания кафедры, утвердившего изменения |
|-------|--|--|---|
| 1. | I - X | 14.05.2017 Корректировка всех разделов в соответствии | |

| | | | |
|----|--|---------------------------|--|
| | | с новым стандартом | |
| 2. | | | |
| 3. | | | |