Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Криптопротоколы**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к вариативной части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями по математическому анализу и линейной алгебре, теории вероятностей в объеме, соответствующем программе первого и второго года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ОПК-1.Б** Способность применять и адаптировать существующие математические и компьютерные методы для разработки и реализации алгоритмов решения актуальных задач в области фундаментальной и прикладной математики.
* **ПК-2.Б** Способность понимать и применять в научно-исследовательской деятельности современный математический аппарат.
* **ПК-5.Б** Способность определить совокупность математических методов и программных решений для отдельного этапа решения прикладной задачи в рамках заданной схемы.

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные свойства, характеризующие безопасность информации;
2. математические методы, используемые для построения основных криптографических протоколов;
3. схемы электронной цифровой подписи;
4. протоколы идентификации;
5. протоколы с нулевым разглашением;
6. игровые протоколы;
7. протоколы передачи и распределения ключей;
8. системы электронных платежей;
9. типовые уязвимости криптографических протоколов.

**Уметь:**

1. применять на практике основные методы построения и анализа криптографических протоколов;
2. применять на практике компьютерные технологии для решения различных задач реализации и изучения криптографических протоколов;
3. находить, анализировать и обрабатывать научно-техническую информацию;
4. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
5. демонстрировать способность к анализу и синтезу;
6. демонстрировать способность к письменному и устному общению на русском языке;
7. публично представить собственные и известные научные результаты;
8. представить математические знания в устной форме;

**Владеть:**

1. навыками использования криптографических протоколов;
2. терминологией, используемой в теории криптографических протоколов;
3. методами анализа криптографических протоколов, проблемно-задачной формой представления математических знаний;
4. проблемно-задачной формой представления естественнонаучных знаний;

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 4 з.е., в том числе 72 академических часов, отведенных на контактную работу обучающихся с преподавателем, 72 академических часов на самостоятельную работу обучающихся.

**6.** Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий.

|  |  |  |
| --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),****Форма промежуточной аттестации по дисциплине (модулю)** | **Всего****(часы**) | В том числе |
| **Контактная работа (работа во взаимодействии с преподавателем)****Виды контактной работы, часы** | **Самостоятельная работа обучающегося,** **часы**  |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |  |
| 1. Введение в криптографические протоколы. Понятие крип-тографического протокола. Свойства, характеризующие безопасность протоколов. Виды криптографических протоколов. Основные виды атак на безопасность криптографических протоколов. Формальные методы анализа протоколов.
 | **4** | 2 | 0 | **2** | **2** |
| 1. Игровые протоколы. Протокол игры в покер по телефону. Протокол подбрасывания монеты. Протокол подписания контракта. Сертифицированная электронная почта. Протоколы частичного разделения секрета. Протоколы скрытой (с забыванием) передачи информации.
 | **12** | 4 | 4 | **8** | **4** |
| 1. Введение в эллиптические кривые. Понятие эллиптической кривой. Дискриминант и инвариант эллиптической кривой. Изоморфизм эллиптических кривых. Группа точек эллиптической кривой. Операции сложения точек эллиптической кривой. Частные формулы и алгоритмы сложения и удвоения точек эллиптической кривой над некоторыми полями. Строение некоторых классов групп эллиптической кривой. Элементарные верхние и нижние оценки порядка группы точек эллиптической кривой. Теорема Постникова. Теорема Хассе. Теорема Хассе-Вейля. Эллиптические кривые над полем характеристики 2. Суперсингулярные и несуперсингулярные кривые. Алгоритм генерации эллиптических кривых с надежными криптографическим свойствами.
 | **24** | 8 | 8 | **16** | **8** |
| 1. Текущий контроль успеваемости: контрольная работа №1
 | **2** | 0 | 2 | **2** | **0** |
| 1. Схемы электронной цифровой подписи. Основные понятия и определения. Цифровые подписи на основе систем шифрования с от-крытым ключом: ЭЦП RSA. Цифровые подписи на основе алгоритмов шифрования с секретным ключом. Цифровые подписи на основе специ-ально разработанных алгоритмов – ЭЦП Фиата-Шамира, ЭЦП семей-ства Эль-Гамаля, ЭЦП Шнорра, ЭЦП DSA. Использование эллиптиче-ских кривых для построения цифровых подписей. Современный российский и американский стандарт электронной цифровой подписи.Схема Рабина. Стираемые электронные подписи. Подпись вслепую. Доказательство подделки подписи: протокол Хейста-Педерсона.
 | **12** | 4 | 4 | **8** | **4** |
| 1. Текущий контроль успеваемости: контрольная работа №2
 | **2** | 0 | 2 | **2** | **0** |
| 1. Протоколы идентификации. Виды протоколов идентификации. Протоколы идентификации, использующие пароли (слабая аутентификация). Протоколы идентификации, использующие технику «запрос-ответ» (сильная аутентификация): протоколы Нидхема-Шрёдера, атака Лоу на протоколы Нидхема-Шрёдера, протоколы ISO, ISO1, ISO2 и ISO3. Протоколы идентификации, использующие технику доказательства знания: протокол Фиата-Шамира, протокол Шнорра, протокол Окамото, протокол GQ и его модификации.
 | **6** | 2 | 2 | **4** | **2** |
| 1. Протоколы с нулевым разглашением. Понятие протокола с нулевым разглашением. Протоколы решения математических задач. Протокол привязки к биту.
 | **10** | 4 | 2 | **6** | **4** |
| 1. Протоколы передачи ключей. Передача ключей с исполь-зованием симметричного шифрования: протокол RPC Handshake и его уязвимость, протокол Шамира, протокол Wide-Mouth Frog, протоколы Yahalom и BAN-Yahalom, протокол Woo-Lam, протокол Нидхема-Шредера и его усиления, протокол Kerberos и протокол Otwa-Rees, протоколы Kryptoknight. Передача ключей с использованием ассиметричного шифрования: протокол Нидехема-Шредера, протокол Woo-Lam. Протокол EKE. Сертификаты открытых ключей. Инфраструктура открытых ключей. Протокол Мэсси-Омура. Протокол Менезеса-Кью-Венстоуна на эллиптических кривых.
 | **6** | 2 | 2 | **4** | **2** |
| 1. Протоколы открытого распределения ключей. Виды про-токолов открытого распределения ключей и их свойства. Протокол Диффи-Хеллмана и его усиление: протоколы MTI, протокол KEA и его модификации, самосертифицируемые ключи. Аутентифицированные протоколы: протокол STS и его модификации, протокол DHKE, одно-проходные протоколы.
 | **6** | 2 | 2 | **4** | **2** |
| 1. Протоколы предварительного распределения ключей. Схемы предварительного распределения ключей в сети связи. Свойства схем предварительного распределения ключей. Схема Блома, схемы на основе пересечения множеств. Схема установления конференц-связи.
 | **12** | 4 | 4 | **8** | **4** |
| 1. Протоколы разделения секрета. Определение схемы раз-деления секрета. Интерполяционная пороговая схема разделения секрета, матричная пороговая схема разделения секрета, модулярная схема разделения секрета, групповой протокол разделения секрета, непороговые схемы разделения секрета. Схема электронного голосования.
 | **8** | 2 | 4 | **6** | **2** |
| 1. Системы электронных платежей и электронные деньги. Общая схема централизованных электронных платежей, общая крипто-графическая модель банковских платежей без сдачи, модель Брэнда (электронные деньги).
 | **4** | 2 | 0 | **2** | **2** |
| Промежуточная аттестация: устный экзамен | **36** | 0 | 0 | **0** | **36** |
| **Итого** | **144** | 36  | 36 | **72** | **72** |

7. Фонд оценочных средств (ФОС)для оценивания результатов обучения по дисциплине (модулю)

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

|  |
| --- |
| Контрольная работа № 1 |
| Вариант 1 |  |
| **Задача 1.** Найти все точки эллиптической кривой над полем GF(31), заданной уравнением $y^{2}=x^{3}+2x+1$.**Задача 2***.* Найти порядок группы точек эллиптической кривой над полем GF($31^{5}$), заданной уравнением $y^{2}=x^{3}+2x+1$.**Задача 3**. Пусть эллиптическая кривая задана над полем GF(31) уравнением $y^{2}=x^{3}+2x+1$.Вычислить P(0,1)+P(0,1)+P(0,1). Найти порядок точки Q(0,-1).**Задача 4.** Пусть эллиптическая кривая задана над полем GF($2^{3}$) уравнением $y^{2}+xy=x^{3}+x^{2}+α$, где $α$ - примитивный элемент поля GF($2^{3}$).Найти все точки, лежащие на этой эллиптической кривой. Найти порядок точки P(1,$α^{2}+1$). |  |
| Контрольнаяработа № 2 |
| Вариант 1 |  |
| **Задача 1.** В системе для контроля входящих сообщений используется ЭЦП RSA. Имеются три абонента:1. secret\_key=(d=167), public\_key=(e=23,n=221);
2. secret\_key=(d=121), public\_key=(e=25,n=247);
3. secret\_key=( d=83), public\_key=(e=27, n=187);

Поступило три сообщения с электронной подписью под каждым.1. m1=3, sign1=185;
2. m2=5, sign2=112;
3. m3=7, sign3=156;

Определить какой абонент под каким сообщением поставил свою подпись.**Задача 2.** Дана хэш-функция h длины 10. Определить секретные параметры p и q, а также открытый параметр n, ЭЦП RSA таким образом, чтобы битовая длина ключей абонентов была минимально возможной, и при этом такой ЭЦП можно было бы подписывать h(m) для любого сообщения m.**Задача 3.** Дана хэш-функция h длины 4, которая задается следующим образом. Если M – сообщение, то$$M=M\_{1}M\_{2}…M\_{k}, |M\_{i}=4 bit|$$$h\_{0}=1100$, $h\_{i}=S\left(M\_{i}+h\_{i-1}\right)+S(h\_{i-1)}$, $i=1..k$, $h\left(M\right)=h\_{k}.$$$S\left(x\_{1},x\_{2},x\_{3},x\_{4}\right)=(x\_{2}x\_{3}x\_{4}+x\_{1},x\_{1}x\_{3}x\_{4}+x\_{2},x\_{1}x\_{2}x\_{4}+x\_{1},x\_{1}x\_{2}x\_{3}+x\_{4})$$m=1010 1110 1001 1011 0010 111от имени абонента A=(secret\_key=(S=(3,16,13,24)), public\_key=(n=77, V=(60, 37, 36, 25))), используя ЭЦП Фиата-Шамира с хэш-функцией h.**Задача 4.** Дана хэш-функция h длины 4, которая задается следующим образом. Если M - сообщение, то$$M=M\_{1}M\_{2}…M\_{k}, |M\_{i}=4 bit|$$$h\_{0}=1100$, $h\_{i}=S\left(M\_{i}+h\_{i-1}\right)+S(h\_{i-1)}$, $i=1..k$, $h\left(M\right)=h\_{k}.$$$S\left(x\_{1},x\_{2},x\_{3},x\_{4}\right)=(x\_{2}x\_{3}x\_{4}+x\_{1},x\_{1}x\_{3}x\_{4}+x\_{2},x\_{1}x\_{2}x\_{4}+x\_{1},x\_{1}x\_{2}x\_{3}+x\_{4})$$m=1010 1110 1001 1011 0010 111Проверить подпись s под сообщением m, если известно, что она сформирована от имени абонента A, используя ЭЦП Фиата-Шамира с хэш-функцией h.**Задача 5.** Хэш-функция h имеет битовую длину 4. Построить ЭЦП Эль-Гамаля на основе эллиптической кривой E(y^2=x^3+2x+3) над полем GF(17), то есть определить P – точку порядка p эллиптической кривой, такую, чтобы она позволяла подписывать значение h(m) для любого сообщения m. |  |

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Вопросы к экзамену.

1. Понятие эллиптической кривой. Дискриминант эллиптической кривой. Изоморфизм эллиптических кривых. Группа точек эллиптической кривой. Операция сложения в группе точек эллиптической кривой над полем характеристики большей 3.

2. Строение некоторых классов групп эллиптической кривой. Элементарные верхние и нижние оценки порядка группы точек эллиптической кривой. Теорема Постникова.

3. Теорема Хассе.

4. Эллиптические кривые над полем характеристики 2. Суперсингулярные и несуперсингулярные кривые.

5. Алгоритм генерации эллиптических кривых с надежными криптографическими свойствами.

6. Криптосистема Эль-Гамаля на эллиптической кривой. Проблема дискретного логарифмирования в группе точек эллиптической кривой. Размещение данных на эллиптических кривых. Выбор точки эллиптической кривой.

7. Понятие криптографического протокола. Свойства, характеризующие безопасность протоколов. Виды криптографических протоколов.

8. Основные виды атак на безопасность криптографических протоколов. Формальные методы анализа протоколов.

9. Определение и основные свойства. Ортогональные массивы.

10. Характеристика оптимальных кодов аутентификации. Коды аутентификации, определяемые кодами, исправляющими ошибки.

11. Определение электронной цифровой подписи. Свойства схемы электронной цифровой подписи. Сравнение электронной цифровой подписи и собственноручной подписи. Цифровые подписи на основе систем шифрования с открытым ключом: ЭЦП RSA.

12. Цифровые подписи на основе алгоритмов шифрования с секретным ключом. Цифровые подписи на основе специально разработанных алгоритмов – ЭЦП семейства Эль-Гамаля.

13. Проблема Диффи-Хеллмана в группе точек эллиптической кривой. Современный российский и американский стандарт электронной цифровой подписи.

14. Понятие протокола идентификации. Виды протоколов идентификации. Парольная аутентификация, одноразовые пароли.

15. Протоколы идентификации, использующие технику «запрос-ответ» (сильная аутентификация): протоколы Нидхема-Шрёдера, атака Лоу на протоколы Нидхема-Шрёдера, протоколы ISO, ISO1, ISO2 и ISO3, их уязвимости.

16. Протокол Фиата-Шамира и протокол Шнорра.

17. Протокол Окамото-Танаки.

18. Протокол GQ и его модификации.

19. Протокол Мэсси-Омура. Протокол Менезеса-Кью-Венстоуна на эллиптических кривых.

20. Протокол решения математических задач. Протокол привязки к биту.

21. Протокол RPC Handshake и его уязвимость, протокол аутентификации Шамира и его уязвимость.

22. Протокол аутентификации Wide-Mouth Frog, протоколы аутентификации Yahalom и BAN-Yahalom, протокол Woo-Lam.

23. Протокол аутентификации Нидхема-Шредера и его усиления, атака Лонга на усиленную версию протокола аутентификации Нидхема-Шредера. Протокол Otwa-Rees и его уязвимость.

24. Передача ключей с использованием ассиметричного шифрования: протокол Нидехема-Шредера, протокол Woo-Lam.

25. Протокол EKE и атака на него.

26. Протоколы передачи ключей с использованием электронной цифровой подписи. Сертификаты открытых ключей. Инфраструктура открытых ключей.

27. Протоколы частичного разделения секрета. Протоколы скрытой передачи с забыванием.

28. Понятие протокола открытого распределения ключей. Виды протоколов открытого распределения ключей и их свойства. Протокол Диффи-Хеллмана.

29. Статический протокол Диффи-Хеллмана. Протоколы MTI, самосертифицируемые ключи.

30. Протокол KEA и его модификации.

31. Протокол STS, протокол DHKE.

32. Протокол STS с использованием хэш-функций, однопроходные протоколы.

33. Определение схемы предварительного распределения ключей. Свойства схем предварительного распределения ключей.

34. Схема Блома.

35. Схема распределения ключей на основе пересечения множеств.

36. Определение схемы разделения секрета. Интерполяционная пороговая схема разделения секрета, матричная пороговая схема разделения секрета, модулярная схема разделения секрета.

37. Групповой протокол разделения секрета, непороговые схемы разделения секрета, протокол установления ключей для конференц-связи.

Типовые задачи для экзамена.

**Задача 1**. Найти все точки эллиптической кривой над полем GF(31), заданной уравнением,

1. $y^{2}=x^{3}+2x+1$
2. $y^{2}=x^{3}+3x+2$
3. $y^{2}=x^{3}+4x+3$
4. $y^{2}=x^{3}+5x+4$
5. $y^{2}=x^{3}+6x-1$

**Задача 2**. Найти порядок группы точек эллиптической кривой, заданной уравнением,

1. $y^{2}=x^{3}+2x+1$
2. $y^{2}=x^{3}+3x+2$
3. $y^{2}=x^{3}+4x+3$
4. $y^{2}=x^{3}+5x+4$
5. $y^{2}=x^{3}+6x-1$

над каждым из полей

1. $GF(31^{5})$
2. $GF(31^{6})$
3. $GF(31^{7})$
4. $GF(31^{8})$
5. $GF(31^{9})$

**Задача 3**. Пусть эллиптическая кривая задана над полем GF(31) уравнением

1. $y^{2}=x^{3}+2x+1$
2. $y^{2}=x^{3}+3x+1$
3. $y^{2}=x^{3}+4x+1$
4. $y^{2}=x^{3}+5x+1$
5. $y^{2}=x^{3}+6x+1$

Вычислить P(0,1)+P(0,1)+P(0,1). Найти порядок точки P(0,-1).

**Задача 4.** Пусть эллиптическая кривая задана над полем GF($2^{3}$) уравнением

$$y^{2}+xy=x^{3}+x^{2}+α$$

где $α$ - примитивный элемент поля GF($2^{3}$).

Найти все точки, лежащие на этой эллиптической кривой. Найти порядок точки P(1,$α^{2}+1$).

**Задача 5.** Пусть p и q простые числа. Построить ЭЦП RSA, то есть сгенерировать ключи для некоторого абонента A. Подписать сообщение m на ключах абонента A.

**Задача 6.** Дана хэш-функция h длины k. Построить ЭЦП RSA, то есть определить простые числа p и q и сформировать ключи для некоторого абонента A, так, чтобы она позволяла подписывать значение h(m) для любого сообщения m. Для сообщения m вычислить h(m) и подписать его от имени абонента A.

**Задача 7.** Пусть P - некоторая точка порядка p эллиптической кривой над полем GF(q) порядка n. Построить ЭЦП Эль-Гамаля, то есть найти параметры криптосистемы и сгенерировать ключи для некоторого абонента A. Подписать сообщение m от имени абонента A. Проверить подпись под сообщением m, сформированной с помощью ЭЦП Эль-Гамаля от имени абонента A.

**Задача 8.** Дана хэш-функция h длины k. Построить ЭЦП Эль-Гамаля на основе эллиптической кривой над полем GF(q) , то есть определить P - точку порядка p эллиптической кривой и сформировать ключи для некоторого абонента A, такую, чтобы она позволяла подписывать значение h(m) для любого сообщения m. Для сообщения m вычислить h(m) и подписать его от имени абонента A.

**Задача 9.** Дана хэш-функция h длины k. Построить ЭЦП Фиата-Шамира, то есть определить все параметры подписи и сформировать ключи для некоторого абонента A, так, чтобы она позволяла подписывать значение h(m) для любого сообщения m. Для сообщения m вычислить h(m) и подписать его от имени абонента A.

**Задача 10.** Для аутентификации клиента на сервере используется протокол односторонней аутентификации ISO на основе криптосистемы с секретным ключом E. Сформировать ответ клиента на запрос сервера (r, M1).

**Задача 11**. Для взаимной аутентификации клиента А и сервера B используется трехпроходной протокол взаимной аутентификации NSPK на основе криптосистемы с открытым ключом (E,D). Определены открытый и закрытый ключи сервера и клиента. Сформировать ответ-запрос сервера на запрос клиента res=E\_B(r\_A,A), а также ответ сервера на запрос клиента. Промоделировать атаку Лоу.

**Задача 12.** Привязать биты 0 и 1, используя схему Гольдвассера-Микали.

**Задача 13.** Пусть в колоде имеются следующие карты - (A,B,C, D). Произвести кодирование карт в протоколе «Игры в покер по телефону».

**Задача 14.** Пусть имеется кодировка карт для участника игры в покер. Используя протокол «Игры в покер по телефону», произвести сдачу i карт из колоды участнику.

**Задача 15.** Используя протокол электронного голосования, заполнить бюллетень за избирателя, который отдает голос a.

**Задача 16.** Используя «безключевой» протокол Шамира на основе односторонней функции f, передать секретный ключ k от абонента A к абоненту B. Промоделировать действия нарушителя в атаке повторения.

**Задача 17.** Построить схему Блома для n абонентов, стойкую к m-кратной компрометации.

|  |
| --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)**  |
| ОценкаРО исоответствующие виды оценочных средств  | 2 | 3 | 4 | 5 |
| **Знания***Экзамен* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения***Контрольная работа*  | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципи-ального характера) | Успешное и систематическое умение |
| **Навыки (владения, опыт деятельности)***Экзамен* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки (владения), применяемые при решении задач |

|  |
| --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**1. основные свойства, характеризующие безопасность информации;
2. схемы электронной цифровой подписи;
3. протоколы идентификации;
4. протоколы с нулевым разглашением;
5. игровые протоколы;
6. протоколы передачи и распределения ключей;
7. системы электронных платежей;
8. типовые уязвимости криптографических протоколов.

**Уметь:**1. применять на практике основные методы построения и анализа криптографических протоколов;
2. применять на практике компьютерные технологии для решения различных задач реализации и изучения криптографических протоколов;
3. находить, анализировать и обрабатывать научно-техническую информацию;
4. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
5. демонстрировать способность к письменному и устному общению на русском языке;

**Владеть:**1. навыками использования криптографических протоколов;
2. терминологией, используемой в теории криптографических протоколов;
 | ОПК-1.Б |
| **Знать:**1. математические методы, используемые для построения основных криптографических протоколов;

**Уметь:**1. демонстрировать способность к анализу и синтезу;
2. публично представить собственные и известные научные результаты;
 | ПК-2.Б |
| **Уметь:**1. представить математические знания в устной форме;

**Владеть:**1. методами анализа криптографических протоколов, проблемно-задачной формой представления математических знаний;
2. проблемно-задачной формой представления естественнонаучных знаний;
 | ПК-5.Б |

8. Ресурсное обеспечение:

Основная литература:

1. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости.  Москва: Академия, 2009.
2. Грушо А.А., Применко Э.А., Тимонина Е.Е. Криптографические протоколы. – Йошкар-Ола: МФ МОСУ, 2001.
3. Ван Тилборг Х.К.А. Основы криптологии. – Москва: Мир, 2006.
4. С.Б. Гашков, Э.А. Применко, М.А. Черепнев. Криптографические методы защиты информации. М: Академия, 2010 – 304 с.

Дополнительная литература:

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. - М.: Гелиос АРВ, 2005.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. M.:Связь, 1979.
3. Виноградов И.М. Основы теории чисел. М.: Наука, 1980.
4. Глухов М.М.. Елизаров В.П.. Нечаев А.А. Алгебра. Ч. 1, 2. М., 1990-1991.
5. Фомичев В.М. Дискретная математика и криптология. – М.: Диалог-МИФИ, 2003. – 400 с.
6. Э.А. Применко. Алгебраические основы криптографии. М: Либроком, 2013 – 288 с.
7. Шнайер Б. Прикладная криптография. – М.: Триумф, 2002. - 816 с.
8. Введение в криптографию. /Под ред. В.В.Ященко. – СПб.: Питер, 2001.- 288 с.
9. Нечаев В.И. Элементы криптографии: Основы теории защиты информации. - М., 1999.
10. Смарт Н. Криптография. М: Техносфера, 2005. - 528 с.

Информационные справочные системы: https://cryptography.ru/

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

9. Язык преподавания: русский.

10. Преподаватели: доцент факультета ВМК МГУ Э.А.Применко

11. Авторы программы: доцент факультета ВМК МГУ Э.А.Применко