ПРОБЛЕМЫ ОБРАЗОВАНИЯ

УДК 378.147

РЕАЛИЗАЦИЯ МЕЖПРЕДМЕТНЫХ СВЯЗЕЙ ДИСЦИПЛИН «АЛГЕБРА И ГЕОМЕТРИЯ» И «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ» В ВУЗАХ МВД РОССИИ

© 2018 О. Ю. Данилова, С. А. Телкова

Воронежский институт МВД России (г. Воронеж, Россия)

В статье рассматривается вопрос межпредметных связей дисциплин математического и естественнонаучного циклов с профессиональными дисциплинами и дисциплинами специализации, преподаваемых курсантам технических специальностей вузов МВД России.

Ключевые слова: межпредметные связи, преподавание, базовые дисциплины, дисциплины специализации, криптографический протокол, шифрующая матрица.

С введением новых ФГОС третьего поколения российское образование предъявляет более высокие требования к качеству профессиональной подготовки специалиста по защите информации – сотрудника органов внутренних дел. Фундаментальные знания и компетенции, которые получают обучающиеся технических специальностей и в дальнейшем применяют в профессиональных дисциплинах и дисциплинах специализации, приобретаются при изучении дисциплин математического и естественнонаучного циклов. Поэтому актуален вопрос определения межпредметных связей и рассмотрения их профессиональной направленности при выборе содержания учебных курсов.

В работе рассматривается взаимосвязь дисциплины «Алгебра и геометрия», относящейся к базовой части, и дисциплины «Математические основы криптографии», которая преподается для курсантов, впоследствии получающих диплом специалистов по обеспечению информационной безопасности, и способствует реализации связи между математическими дисциплинами и дисциплинами специализации. В ходе изучения математических основ криптографии решаются задачи:

– использования современных математических методов криптографии в практической деятельности;
– обучения курсантов математическим понятиям и методам, необходимым для дисциплин специализации;
– формирования у обучающихся умений и навыков построения математических моделей объектов и процессов, выбор метода их исследования и разработка алгоритма его реализации (в области криптографии);
– повышения уровня математической подготовки, необходимого для изучения профессиональных дисциплин, основанных на знаниях математики.

Сформулированные задачи имеют решение только при наличии базовых математических знаний и компетенций.

Мы определили темы алгебры и геометрии (понятия, методы, умения, навыки, компетенции), необходимые и достаточные курсантам для усваивания всех основных разделов дисциплины «Математические основы криптографии» согласно ФГОС третьего поколения и на этой основе сформулировали предложения для конкретизации методик преподавания обеих дисциплин.

Темы учебных курсов «Алгебра и геометрия» и «Математические основы криптографии» выбраны согласно основной профессиональной образовательной программе высшего образования для обучающихся по специальности «Информационная безопасность телекоммуникационных систем». Таб-

Данилова Ольга Юрьевна – Воронежский институт МВД России, доцент кафедры математики и моделирования систем, к. ф.-м. н., доцент, danilova_olga@hotmail.com.
Телкова Светлана Анатольевна – Воронежский институт МВД России, доцент кафедры математики и моделирования систем, к. п. н., доцент, tsa76@inbox.ru.

лица 1 показывает взаимосвязь между сходственными темами рассматриваемых курсов, что обозначено символом (+).

Числами от 1 до 10 в таблице отмечены следующие темы математических основ криптографии: 1. Аффинные криптопротоколы, 2. Матричные криптопротоколы, 3. Diffie-Hellman алгоритм, 4. Криптопротокол без передачи ключей, 5. Криптопротокол с открытым ключом, 6. Криптосистема Рабина, 7. Процедуры проверки подлинности, 8. Электронная цифровая подпись, 9. Криптопротоколы с использованием эллиптических кривых, 10. Построение электронной цифровой подписи с использованием эллиптических кривых.

Таблица 1

Взаимосвязь между темами учебных дисциплин «Алгебра и геометрия» (строки) и «Математические основы криптографии» (столбцы)

«Математические основы криптографии» / **«Алгебра и геометрия»**	1	2	3	4	5	6	7	8	9	10
Основные алгебраические структуры	+	+	+	+	+	+	+	+	+	+
Кольцо целых чисел	+	+	+	+	+	+	+	+	+	+
Матрицы и определители над полем		+								
Системы линейных уравнений над полем		+								
Элементы теории множеств										
Векторная алгебра	+	+	+							
Векторные пространства и линейные операторы	+	+		+						
Комплексные числа										
Многочлены над полем						+			+	+
Прямая на плоскости										
Кривые второго порядка									+	+
Прямая и плоскость в пространстве										
Поверхности второго порядка										

Мы видим, что в курсе «Математические основы криптографии» широко применяется сложный математический аппарат.

Из таблицы 1 следует, что при обучении курсу «Алгебра и геометрия» надо особо пристально рассматривать: основные алгебраические структуры; кольца целых чисел; матрицы и определители над полем; векторную алгебру; векторные пространства и линейные операторы; кривые второго порядка.

Все выше перечисленные темы применяют при построении различных криптографических протоколов [1, 2].

При проведении учебных занятий следует использовать активные и интерактивные методы обучения: бинарные лекции, лекции с проблемным изложением материала, занятия с элементами визуализации, «мозгового штурма», разбора практических ситуаций, реализующие межпредметные связи, позволяющие интегрировать знания из разных областей для решения одной проблемы, дающие возможность применить полученные знания в практической деятельности.

В качестве примера приведем фрагмент лабораторного занятия по решению задач шифрования дисциплины «Математические основы криптографии» с использованием знаний линейной и векторной алгебры.

Будем использовать следующую таблицу кодирования.

Таблица 2

Таблица кодирования

1	а	7	ж	13	н	19	у	25	щ
2	б	8	з	14	о	20	ф	26	ы
3	в	9	и	15	п	21	х	27	ь
4	г	10	к	16	р	22	ц	28	э
5	д	11	л	17	с	23	ч	29	ю
6	е	12	м	18	т	24	ш	30	я
								31=0	«-»

Для упрощения кодирования отождествим буквы «ь» и «ъ», «е» и «ё», «и» и «й», что никаким образом не исказит наше сообщение и мы сможем его понять при прочтении.

Задача 1. Зашифровать сообщение

$$X = \text{"математика"}$$

криптоключом

$$B = \text{"наука"},$$

используя шифр аббата Тритемиуса.

Решение. Из таблицы кодирования (табл. 2) каждой букве сообщения X поставим в соответствие код. Получим набор чисел

$$X = \text{"12,1,18,6,12,1,18,9,10,1"}.$$

Каждой букве ключа ставим код из таблицы кодирования (табл. 2). Получаем $B = \text{"13,1,19,10,1"}$.

Разбиваем текст на блоки, равные размеру ключа, то есть на блоки, состоящие из 5 символов. Таким образом, имеем

$$X = \text{"}\{12,1,18,6,12\},\{1,18,9,10,1\}\text{"}.$$

Складываем исходное сообщение с ключом поблочно.

$$Y \equiv X + B(\mathrm{mod}\,31)$$

$$\{12,1,18,6,12\} + \{13,1,19,10,1\} \equiv$$

$$\equiv \{25,2,37,16,13\} \equiv \{25,2,6,16,13\}(\mathrm{mod}\,31),$$

$$\{1,18,9,10,1\} + \{13,1,19,10,1\} \equiv$$

$$\equiv \{14,19,28,20,2\}(\mathrm{mod}\,31).$$

Получаем следующее зашифрованное сообщение

$$Y = \text{"25,2,6,16,13,14,19,28,20,2"}$$

или

$$Y = \text{"щ, б, е, р, н, о, у, э, ф, б"}.$$

Для того чтобы расшифровать данное сообщение, необходимо найти обратный ключ из выражения

$$B1 \equiv 31 - B(\mathrm{mod}\,31).$$

$$\begin{pmatrix}31\\31\\31\\31\\31\end{pmatrix} - \begin{pmatrix}13\\1\\19\\10\\1\end{pmatrix} \equiv \begin{pmatrix}18\\30\\12\\21\\30\end{pmatrix} (\mathrm{mod}\,31)$$

Складываем зашифрованное сообщение поблочно с обратным ключом. Получаем

$$\{25,2,6,16,13\} + \{18,30,12,21,30\} \equiv$$

$$\equiv \{43,32,18,37,43\} \equiv \{12,1,18,6,12\}(\mathrm{mod}\,31),$$

$$\{14,19,28,20,2\} + \{18,30,12,21,30\} \equiv$$

$$\equiv \{32,49,40,41,32\} \equiv \{1,18,9,10,11\}(\mathrm{mod}\,31),$$

или $X = \text{"12,1,18,6,12,1,18,9,10,1"}$.

Восстанавливаем сообщение по таблице кодирования (табл. 2). Получаем исходное сообщение $X = \text{"математика"}$.

Задача 2. Зашифруем сообщение

$$X = \text{"криптография"}$$

криптоключом

$$A = \text{"шифрование"},$$

используя матричный 3d криптопротокол

$$Y = AX \ (\mathrm{mod}\,31).$$

Решение. Кодируем сообщение X и криптоключ A при помощи цифр из таблицы кодирования (табл. 2). Имеем следующие последовательности чисел

$$X = \text{"10,16,9,15,18,14,4,16,1,20,9,30"},$$

$$A = \text{"24,9,20,16,14,3,1,13,9,6"}.$$

Поскольку у нас матричный 3d криптопротокол, то для формирования шифрующей матрицы нам достаточно первых 9 символов ключа. Получим следующую матрицу

$$A = \begin{pmatrix}24 & 9 & 20\\16 & 14 & 3\\1 & 13 & 9\end{pmatrix}.$$

Разобьем закодированное сообщение на блоки, состоящие из трех цифр. Получим:

$$X = \text{"}\{10,16,9\},\{15,18,14\},$$

$$\{4,16,1\},\{20,9,30\}\text{"}.$$

Зашифруем сообщение X ключевой матрицей A. Для этого умножим сообщение на ключевую матрицу поблочно. Имеем

$$\begin{pmatrix}24 & 9 & 20\\16 & 14 & 3\\1 & 13 & 9\end{pmatrix}\begin{pmatrix}10\\16\\9\end{pmatrix} \equiv \begin{pmatrix}564\\411\\299\end{pmatrix} \equiv \begin{pmatrix}6\\8\\20\end{pmatrix} (\mathrm{mod}\,31),$$

$$\begin{pmatrix}24 & 9 & 20\\16 & 14 & 3\\1 & 13 & 9\end{pmatrix}\begin{pmatrix}15\\18\\14\end{pmatrix} \equiv \begin{pmatrix}802\\534\\375\end{pmatrix} \equiv \begin{pmatrix}27\\7\\3\end{pmatrix} (\mathrm{mod}\,31),$$

$$\begin{pmatrix}24 & 9 & 20\\16 & 14 & 3\\1 & 13 & 9\end{pmatrix}\begin{pmatrix}4\\16\\1\end{pmatrix} \equiv \begin{pmatrix}260\\291\\221\end{pmatrix} \equiv \begin{pmatrix}12\\12\\4\end{pmatrix} (\mathrm{mod}\,31),$$

$$\begin{pmatrix}24 & 9 & 20\\16 & 14 & 3\\1 & 13 & 9\end{pmatrix}\begin{pmatrix}20\\9\\30\end{pmatrix} \equiv \begin{pmatrix}1161\\536\\407\end{pmatrix} \equiv \begin{pmatrix}14\\9\\4\end{pmatrix} (\mathrm{mod}\,31).$$

Получили зашифрованное сообщение

$$Y = \text{"6,8,20,27,7,3,12,12,4,14,9,4"}$$

или

$$Y = \text{"е, з, ф, ь, ж, в, м, м, г, о, и, г"}.$$

Для расшифровки сообщения ищем обратный ключ из выражения $A \cdot A_1 = I \pmod{31}$ или $A_1 = A^{-1} \pmod{31}$. То есть надо найти обратную матрицу к матрице A в $M_3(Z_{31})$. Вычисляем обратную матрицу обычным способом

$$A^{-1} = \frac{1}{|A|}\begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix}.$$

Находим определитель матрицы по правилу треугольников

$$|A| = 24 \cdot 14 \cdot 9 + 9 \cdot 3 \cdot 1 + 16 \cdot 13 \cdot 20 - $$
$$- 20 \cdot 14 \cdot 1 - 9 \cdot 16 \cdot 9 - 24 \cdot 3 \cdot 13 = 4699.$$

Находим все алгебраические дополнения

$$A_{11} = (-1)^2 \begin{vmatrix} 14 & 3 \\ 13 & 9 \end{vmatrix} = 87,$$

$$A_{12} = (-1)^3 \begin{vmatrix} 16 & 3 \\ 1 & 9 \end{vmatrix} = -141,$$

$$A_{13} = (-1)^4 \begin{vmatrix} 16 & 14 \\ 1 & 13 \end{vmatrix} = 194,$$

$$A_{21} = (-1)^3 \begin{vmatrix} 9 & 20 \\ 13 & 9 \end{vmatrix} = 179,$$

$$A_{22} = (-1)^4 \begin{vmatrix} 24 & 20 \\ 1 & 9 \end{vmatrix} = 196,$$

$$A_{23} = (-1)^5 \begin{vmatrix} 24 & 9 \\ 1 & 13 \end{vmatrix} = -303,$$

$$A_{31} = (-1)^4 \begin{vmatrix} 9 & 20 \\ 14 & 3 \end{vmatrix} = -253,$$

$$A_{32} = (-1)^5 \begin{vmatrix} 24 & 20 \\ 16 & 3 \end{vmatrix} = 248,$$

$$A_{33} = (-1)^6 \begin{vmatrix} 24 & 9 \\ 16 & 14 \end{vmatrix} = 192.$$

Получаем обратную матрицу в поле вещественных чисел

$$A^{-1} = \frac{1}{4699}\begin{pmatrix} 87 & 179 & -253 \\ -141 & 196 & 248 \\ 194 & -303 & 192 \end{pmatrix}.$$

Переводим все компоненты матрицы из поля R в кольцо целых чисел по модулю 31 Z_{31}. Получаем

$$A^{-1} \equiv \frac{1}{18}\begin{pmatrix} 25 & 24 & -5 \\ -17 & 10 & 0 \\ 8 & -24 & 6 \end{pmatrix} \pmod{31}.$$

Для нахождения

$$\frac{1}{18} \bmod (31)$$

надо решить сравнение

$$\frac{1}{18} \equiv x \pmod{31} \text{ или } 18x \equiv 1 \pmod{31}.$$

Будем решать полученное сравнение по методу Эйлера

$$x \equiv 18^{\varphi(31)-1} \pmod{31} \equiv 18^{29} \pmod{31} \equiv$$
$$\equiv (-13)^{29} \equiv (13^2)^{14} \cdot (-13) \equiv (-13) \cdot (169)^{14} \equiv$$
$$\equiv (-13) \cdot (14)^{14} \equiv (-13) \cdot (14^2)^7 \equiv$$
$$\equiv (-13) \cdot (196)^7 \equiv (-13) \cdot (10)^7 \equiv$$
$$\equiv (-13) \cdot (10^2)^3 \cdot 10 \equiv (-13) \cdot 10 \cdot (100)^3 \equiv$$
$$\equiv (-130) \cdot (7)^3 \equiv (-6) \cdot 49 \cdot 7 \equiv (-42) \cdot 49 \equiv$$
$$\equiv (-42) \cdot 49 \equiv (-11) \cdot 18 \equiv -198 \equiv$$
$$\equiv 12 \equiv 19 \pmod{31},$$

т. о.

$$\frac{1}{18} \equiv 19 \pmod{31}.$$

Значит

$$A^{-1} \equiv \frac{1}{18}\begin{pmatrix} 25 & 24 & -5 \\ -17 & 10 & 0 \\ 8 & -24 & 6 \end{pmatrix} \equiv 19\begin{pmatrix} 25 & 24 & -5 \\ -17 & 10 & 0 \\ 8 & -24 & 6 \end{pmatrix}$$
$$\equiv \begin{pmatrix} 475 & 456 & -95 \\ -323 & 190 & 0 \\ 152 & -456 & 114 \end{pmatrix} \equiv \begin{pmatrix} 10 & 22 & -2 \\ -13 & 4 & 0 \\ 28 & -22 & 21 \end{pmatrix} \equiv$$
$$\equiv \begin{pmatrix} 10 & 22 & 29 \\ 18 & 4 & 0 \\ 28 & 9 & 21 \end{pmatrix} \pmod{31}.$$

При этом для матриц должно быть справедливо равенство

$$A \cdot A^{-1} \equiv A^{-1} \cdot A \equiv I \pmod{31}.$$

Действительно

$$A^{-1}\cdot A\equiv\begin{pmatrix}10&22&29\\18&4&0\\28&9&21\end{pmatrix}\cdot\begin{pmatrix}24&9&20\\16&14&3\\1&13&9\end{pmatrix}\equiv$$

$$\equiv\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}(\mathrm{mod}\,31)$$

,

$$A\cdot A^{-1}\equiv\begin{pmatrix}24&9&20\\16&14&3\\1&13&9\end{pmatrix}\cdot\begin{pmatrix}10&22&29\\18&4&0\\28&9&21\end{pmatrix}\equiv$$

$$\equiv\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}(\mathrm{mod}\,31)$$

.

Для расшифровки сообщения

$Y=\text{"}\{6,8,20\},\{27,7,3\},\{12,12,4\},\{14,9,4\}\text{"}$

надо найти X из выражения

$$X\equiv A^{-1}\cdot Y(\mathrm{mod}\,31).$$

Находим

$$\begin{pmatrix}10&22&29\\18&4&0\\28&9&21\end{pmatrix}\cdot\begin{pmatrix}6\\8\\20\end{pmatrix}\equiv\begin{pmatrix}816\\140\\660\end{pmatrix}\equiv\begin{pmatrix}10\\16\\9\end{pmatrix}(\mathrm{mod}\,31),$$

$$\begin{pmatrix}10&22&29\\18&4&0\\28&9&21\end{pmatrix}\cdot\begin{pmatrix}27\\7\\3\end{pmatrix}\equiv\begin{pmatrix}511\\514\\882\end{pmatrix}\equiv\begin{pmatrix}15\\18\\14\end{pmatrix}(\mathrm{mod}\,31),$$

$$\begin{pmatrix}10&22&29\\18&4&0\\28&9&21\end{pmatrix}\cdot\begin{pmatrix}12\\12\\4\end{pmatrix}\equiv\begin{pmatrix}500\\264\\528\end{pmatrix}\equiv\begin{pmatrix}4\\16\\1\end{pmatrix}(\mathrm{mod}\,31),$$

$$\begin{pmatrix}10&22&29\\18&4&0\\28&9&21\end{pmatrix}\cdot\begin{pmatrix}14\\9\\4\end{pmatrix}\equiv\begin{pmatrix}454\\288\\557\end{pmatrix}\equiv\begin{pmatrix}20\\9\\30\end{pmatrix}(\mathrm{mod}\,31).$$

В результате получаем закодированное сообщение

$$X=\text{"}10,16,9,15,18,14,4,16,1,20,9,30\text{"}.$$

Применив к полученной последовательности таблицу кодирования (табл. 2), получаем исходное сообщение

$$X=\text{"криптография"}.$$

Таким образом, для решения задач криптографии необходимы из курса алгебры и геометрии умения выполнять действия с матрицами и векторами, находить значения определителей, алгебраических дополнений, строить обратную матрицу.

ЛИТЕРАТУРА

1. Данилова О. Ю. Математические основы криптографии: учебник / О. Ю. Данилова, В. Н. Думачев. – Воронеж: ВИ МВД России, 2017. – 301 с.

2. Думачев В. Н. Алгебра и геометрия: учебник / В. Н. Думачев, В. В. Меньших, С. А. Телкова. – Воронеж: ВИ МВД России. – 2014. – 431 с.

REALIZATION OF INTERDISCIPLINARY COMMUNICATIONS BETWEEN DISCIPLINES «ALGEBRA AND GEOMETRY» AND «MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY» IN THE INSTITUTES OF RUSSIAN INTERIOR MINISTRY

© 2018 O. Yu. Danilova, S. A. Telkova

Voronezh Institute of the Ministry of the Interior of the Russian Federation (Voronezh, Russia)

The article discusses the interdisciplinary communications between disciplines of mathematical and natural science cycles and professional disciplines and disciplines of specialization, which are taught to cadets of technical specialties in the institutes of Russian Interior Ministry.

Key words: interdisciplinary communications, teaching, basic disciplines, disciplines of specialization, cryptographic protocol, encryption matrix.