Известия Воронежского государственного педагогического университета. 2023. № 3 (300). С. 28–33.
Izvestia Voronezh State Pedagogical University. 2023. (3), 28–33.

Научная статья
УДК 378.147
DOI: 10.47438/2309-7078_2023_3_28

ГРАФОВОЕ ПРЕДСТАВЛЕНИЕ МЕЖПРЕДМЕТНЫХ СВЯЗЕЙ ДИСЦИПЛИН «АЛГЕБРА И ГЕОМЕТРИЯ» И «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ»

Ольга Юрьевна Данилова[1], Светлана Анатольевна Телкова[2], Татьяна Владимировна Ларина[3]

Воронежский институт МВД России[1, 2]
Воронеж, Россия
Воронежский государственный педагогический университет [3]
Воронеж, Россия

[1]*Кандидат физико-математических наук, доцент кафедры математики и моделирования систем, ORCID ID: 0009-0006-2300-0937, e-mail: danilova_olga@hotmail.com*
[2] *Кандидат педагогических наук, доцент кафедры математики и моделирования систем, ORCID ID: 0000-0003-2401-8363, e-mail: tsa76@inbox.ru*
[3]*Кандидат педагогических наук, доцент кафедры информатики, информационных технологий и цифрового образования, ORCID ID: 0000-0003-3942-4313, e-mail: tatilari06@rambler.ru*

Аннотация. В статье изучается связь дисциплины специализации «Математические основы криптографии», преподаваемой курсантам и слушателям на старших курсах радиотехнического факультета ВИ МВД России, с базовой дисциплиной «Алгебра и геометрия», которая изучается на первом курсе. Для рассматриваемых дисциплин введены основные темы и наглядно показаны их взаимосвязи в виде графов. Понимание связей между дисциплинами «Алгебра и геометрия» и «Математические основы криптографии» позволяет выстроить оптимальную траекторию обучения курсантов и слушателей. Формированию профессиональных компетенций способствуют практико-ориентированные задания, примеры которых приведены в статье. Рассмотренные задания разбираются на лабораторных занятиях в ходе изучения дисциплины «Математические основы криптографии». При этом при решении такого рода задач подчеркивается широкое использование знаний из курса «Алгебра и геометрия», что позволяет лучше понять межпредметные связи рассматриваемых дисциплин и определить, каким темам следует уделить наибольшее внимание. Таким образом, специалисту по защите информации необходимо уметь вычислять остатки от деления по модулю шифрования, функцию Эйлера; определять, является ли число простым или составным; раскладывать число на простые множители; решать сравнения и системы сравнений различными методами; находить обратные матрицы в кольце целых чисел.

Ключевые слова: алгебра и геометрия, математические основы криптографии, межпредметные связи, матрица, функция Эйлера, шифрование, криптографические алгоритмы, аффинная криптосистема, матричная криптосистема.

Для цитирования: *Данилова О.Ю., Телкова С.А., Ларина Т.В.* Графовое представление межпредметных связей дисциплин «Алгебра и геометрия» и «Математические основы криптографии» // Известия Воронежского государственного педагогического университета. 2023. № 3. С. 28–33. DOI: 10.47438/2309-7078_2023_3_28

Введение

В современном мире широко востребованными являются специалисты в области компьютерной и информационной безопасности. Это связано с распространением угроз, возникающих в системах защиты информации, поскольку информационные технологии проникли во все сферы жизнедеятельности человека. Во время обучения в образовательных организациях высшего образования МВД России курсанты и слушатели приобретают умения и навыки, которые

используются ими в своей профессиональной деятельности. Компетенции, сформированные при изучении базовых дисциплин, становятся основой для приобретения профессиональных компетенций. Поэтому нахождение оптимальной траектории обучения и определение межпредметных связей является актуальной современной задачей [10].

Понимание междисциплинарных связей позволяет выявить структурные элементы учебного процесса и объединить их в единое целое, что также способствует эффективному построению траекторий обучения и повышению качества научно-теоретической и практической подготовки курсантов и слушателей.

Проблему межпредметных связей освещали в своих работах известные ученые и педагоги:

– Г.И. Беленький, И.Д. Зверев, Д.М. Кирюшин, Н.С. Пурышева, Ф.П. Соколова (понятие и классификация межпредметных связей);

– П.Р. Атутов, С.Я. Батышев, И.В. Евграфова, Д.М. Кирюшкин, О.Е. Кириченко (межпредметные связи в области общего и среднего образования, в области профессионально-технического образования);

– Р.П. Исаева, Н.В. Чхаидзе (реализация межпредметных связей через построение оптимальной системы прикладных задач и упражнений, через систему лабораторных работ).

В работе исследуется связь дисциплины «Алгебра и геометрия», изучаемой на 1 курсе, с дисциплиной «Математические основы криптографии», преподаваемой на старших курсах. При рассмотрении математических основ криптографии обучающиеся знакомятся с современными математическими методами криптографии, получают навыки их использования при решении прикладных задач; у них формируются умения и навыки построения симметричных и асимметричных криптографических протоколов. Поэтому наличие базовых алгебраических и геометрических знаний и компетенций помогает в дальнейшем успешному освоению данного курса математических основ криптографии.

Результаты

Для успешного овладения предметом «Математические основы криптографии» и приобретения профессиональных навыков в области криптографии необходимы знания из курса «Алгебра и геометрия», при этом при построении разнообразных криптографических протоколов применяется сложный математический аппарат.

При проведении занятий по рассматриваемым дисциплинам следует использовать современные педагогические приемы [8], а именно: бинарные лекции, проблемные лекции, занятия с элементами визуализации и «мозгового штурма» [9; 11]. При изложении материала необходимо большое внимание уделять рассмотрению профессионально-прикладных задач, при решении которых применяются знания из разных областей науки, что позволяет показать реализацию межпредметных связей на практике [6; 7].

Введем следующие обозначения для основных тем дисциплины «Алгебра и геометрия».

1. Основные алгебраические структуры – АГ1.
2. Кольцо целых чисел – АГ2.
3. Матрицы и определители над полем – АГ3.
4. Системы линейных уравнений над полем – АГ4.
5. Векторная алгебра – АГ5.
6. Векторные пространства и линейные операторы – АГ6.
7. Многочлены над полем – АГ7.
8. Кривые второго порядка – АГ8.

Алгебраические и геометрические навыки применяются в математических основах криптографии при построении как симметричных, так и асимметричных криптопротоколов и доказательстве их корректности [1; 5].

Обозначим темы курса «Математические основы криптографии».

1. Линейные криптосистемы – КР1.
2. Шифры на основе матриц – КР2.
3. Обмен ключами по Диффи-Хэллману – КР3.
4. Криптопротоколы без обмена ключами – КР4.
5. Криптосистемы с секретным и открытым ключами – КР5.
6. Асимметричная криптосистема Рабина – КР6.
7. Процедуры проверки подлинности – КР7.
8. Электронная цифровая подпись – КР8.
9. Использование эллиптических кривых в криптопротоколах – КР9.
10. Использование эллиптических кривых при построении электронной цифровой подписи – КР10 [2; 3].

Анализ содержания указанных тем позволил выявить межпредметные взаимосвязи и представить их с помощью графов (рисунки 1–3). При этом видно, что темы АГ1 и АГ2 алгебры и геометрии имеют связи со всеми темами математических основ криптографии (рис. 1). С учетом этого в рабочей программе дисциплины «Алгебра и геометрия» следует скорректировать в сторону увеличения количество часов на изучение основных алгебраических структур и кольца целых чисел.

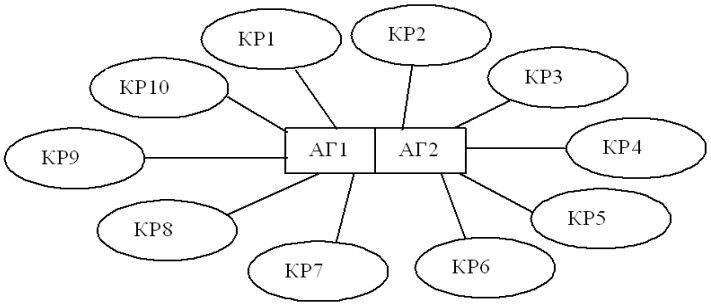

Рисунок 1 – Сильные связи тем предмета «Алгебра и геометрия» с темами предмета «Математические основы криптографии»

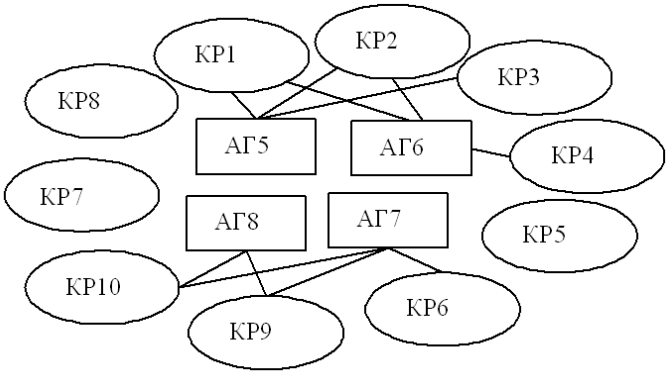

Рисунок 2 – Средние связи тем предмета «Алгебра и геометрия» с темами предмета «Математические основы криптографии»

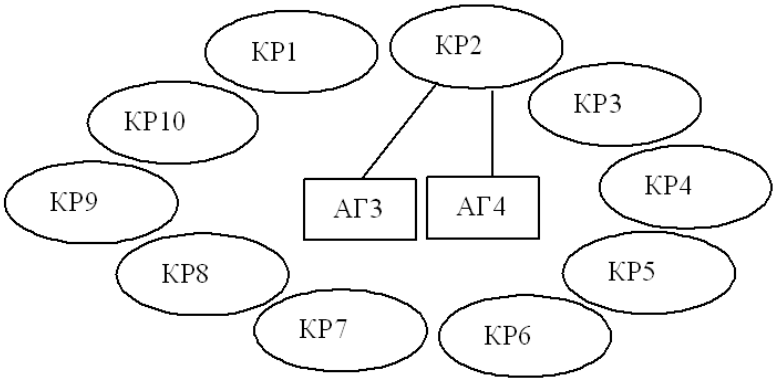

Рисунок 3 – Слабые связи тем предмета «Алгебра и геометрия» с темами предмета «Математические основы криптографии»

Рассмотрим несколько задач, которые решаются на занятиях по математическим основам криптографии [4]. В ходе их решения широко применяется математический аппарат из линейной и векторной алгебры.

При решении задач будем применять следующую таблицу кодирования (табл. 1).

Таблица 1 – 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	« _ »

При кодировании буквы «ь» и «ъ», «е» и «ё», «и» и «й» считаются одинаковыми. При данном упрощении возможность прочтения сообщения сохраняется, а текст не искажается.

Задача 1. Зашифровать сообщение X = «пришел_увидел_победил», используя двухраундовый аффинный криптографический протокол $Y = aX + b \pmod{31}$, где $a = P(5)$, $b = P(7)$ – криптоключи, $P(5) = 11$ – пятое простое число, $P(7) = 17$ – седьмое простое число.

Решение. Закодировав сообщение X при помощи таблицы кодирования, получаем последовательность:

$X =$"15, 16, 9, 24, 6, 11, 0, 19, 3, 9, 5, 6, 11, 0, 15, 14, 2, 6, 5, 9, 11".

Применяем к полученной последовательности криптографический протокол $Y = 11X + 17 \pmod{31}$, то есть вычисляем

$$11 \cdot 15 + 17 \pmod{31} \equiv 182 \equiv 27 \pmod{31},$$

$$11 \cdot 16 + 17 \pmod{31} \equiv 193 \equiv 7 \pmod{31} \text{ и т д.}$$

В итоге получаем последовательность

$Y =$"27, 7, 23, 2, 21, 14, 17, 9, 19, 23, 10, 21, 14, 17, 27, 16, 8, 21, 10, 23, 14"

или зашифрованное сообщение

$Y =$"ьжчбхосиучкхосьрзхкчо".

Для того чтобы расшифровать сообщение Y, надо для каждой цифры из сообщения найти обратное преобразование $X = A \cdot (Y - 17) \pmod{31}$. A вы-

числяется как обратный элемент к a, то есть находится из условия $A\cdot a\equiv 1(\mathrm{mod}\, n)$, где $n=31$, $a=11$. Решаем сравнение $A\cdot 11\equiv 1(\mathrm{mod}\ 31)$ по методу Эйлера $A\equiv a^{\varphi(n)-1}(\mathrm{mod}\, n)$, где $\varphi(n)$ – функция Эйлера. Получаем

$$A\equiv 11^{29}(\mathrm{mod}\ 31)\equiv (11^2)^{14}\cdot 11\equiv (121)^{14}\cdot 11\equiv 28^{14}\cdot 11\equiv$$
$$\equiv (-3)^{14}\cdot 11\equiv 3^{14}\cdot 11\equiv (3^3)^4\cdot 3^2\cdot 11\equiv (-4)^4\cdot 3^2\cdot 11\equiv$$
$$\equiv 64\cdot 4\cdot 9\cdot 11\equiv 2\cdot 4\cdot 99\equiv 2\cdot 4\cdot 6\equiv 48\equiv 17(\mathrm{mod}\ 31).$$

Таким образом, для расшифровки сообщения Y надо для каждого значения из последовательности Y вычислить

$$X=17\cdot(Y-17)(\mathrm{mod}\ 31),$$
$$17\cdot(27-17)(\mathrm{mod}\ 31)\equiv 170\equiv 15,$$
$$17\cdot(7-17)(\mathrm{mod}\ 31)\equiv -170\equiv -15\equiv 16 \text{ и т.д.}$$

В итоге получаем

$X=$"15,16,9,24,6,11,0,19,3,9,5,6,11,0,15,14,2,6,5,9,11"

или $X=$ «пришел_увидел_победил».

Задача 2. Зашифровать сообщение $X=$ «пришел_увидел_победил», используя двумерный матричный криптопротокол $Y=AX\ (\mathrm{mod}31)$ и криптоключ $A=$"криптография".

Решение. Кодируем сообщение X и криптоключ A, применяя таблицу кодирования. Получаем две последовательности чисел:

$X=$"15,16,9,24,6,11,0,19,3,9,5,6,11,0,15,14,2,6,5,9,11",

$A=$"10,16,9,15,18,14,4,16,1,20,9,30".

Так как для зашифрования сообщения применяется шифрующая матрица размера 2 Ч 2, то для формирования шифрующей матрицы необходимы первые четыре символа криптоключа A. Получаем

$$A=\begin{pmatrix}10 & 16\\ 9 & 15\end{pmatrix}.$$

Теперь разбиваем сообщение X на блоки по две цифры (если в блоке меньше двух цифр, то добавляем в блок нули). Имеем:

$X=$"{15,16},{9,24},{6,11},{0,19},{3,9},{5,6},
{11,0},{15,14},{2,6},{5,9},{11,0}".

Шифруем сообщение, умножая ключевую матрицу A на поблочно разбитое закодированное сообщение X

$$\begin{pmatrix}10 & 16\\ 9 & 15\end{pmatrix}\cdot\begin{pmatrix}15\\ 16\end{pmatrix}\equiv\begin{pmatrix}406\\ 375\end{pmatrix}\equiv\begin{pmatrix}3\\ 3\end{pmatrix}(\mathrm{mod}\ 31),$$
$$\begin{pmatrix}10 & 16\\ 9 & 15\end{pmatrix}\cdot\begin{pmatrix}9\\ 24\end{pmatrix}\equiv\begin{pmatrix}474\\ 441\end{pmatrix}\equiv\begin{pmatrix}9\\ 7\end{pmatrix}(\mathrm{mod}\ 31),$$
$$\begin{pmatrix}10 & 16\\ 9 & 15\end{pmatrix}\cdot\begin{pmatrix}6\\ 11\end{pmatrix}\equiv\begin{pmatrix}236\\ 219\end{pmatrix}\equiv\begin{pmatrix}19\\ 2\end{pmatrix}(\mathrm{mod}\ 31) \text{ и т.д.}$$

В итоге получим зашифрованное сообщение

$Y=$"3,3,9,7,19,2,25,6,19,7,22,11,17,6,2,4,23,15,8,25,17,6"

или

$Y=$"в,в,и,ж,у,б,щ,е,у,ж,ц,л,с,е,б,г,ч,п,з,щ,с,е".

Для расшифрования сообщения Y требуется ключ расшифровки. Он находится из условия $A\cdot A_1=I\ (\mathrm{mod}31)$ или $A_1=A^{-1}\ (\mathrm{mod}31)$ (то есть надо вычислить обратную матрицу к матрице A по модулю 31). Для нахождения обратной матрицы используется формула

$$A^{-1}=\frac{1}{|A|}\cdot\begin{pmatrix}A_{11} & A_{21}\\ A_{12} & A_{22}\end{pmatrix},$$

где $A_{ij}=(-1)^{i+j}M_{ij}$, M_{ij} — минор элемента a_{ij} матрицы A, $|A|$ — определитель матрицы A.

Имеем:

$$|A|=10\cdot 15-9\cdot 16=6,$$
$$A_{11}=(-1)^2\cdot 15=15,\ A_{12}=(-1)^3\cdot 9=-9,$$
$$A_{21}=(-1)^3\cdot 16=-16,\ A_{22}=(-1)^4\cdot 10=10.$$

Находим:

$$A^{-1}=\frac{1}{6}\cdot\begin{pmatrix}15 & -16\\ -9 & 10\end{pmatrix}.$$

Теперь надо вычислить все компоненты обратной матрицы в кольце целых чисел Z_{31}. Для нахождения $\frac{1}{6}(\mathrm{mod}31)$ решаем сравнение первой степени

$$\frac{1}{6}\equiv x(\mathrm{mod}31) \text{ или } 6x\equiv 1(\mathrm{mod}31).$$

Так как 6 и 13 общих делителей не имеют, то полученное сравнение можно решить методом Эйлера

$$x\equiv 6^{\varphi(31)-1}(\mathrm{mod}31)\equiv 6^{29}(\mathrm{mod}31)\equiv$$
$$\equiv (6^2)^{14}\cdot 6\equiv (36)^{14}\cdot 6\equiv 6\cdot(5)^{14}\equiv$$
$$\equiv 6\cdot(5^2)^7\equiv 6\cdot(25)^7\equiv 6\cdot(-6)^7\equiv$$
$$\equiv -(6^2)^4\equiv -(36)^4\equiv -(5)^4\equiv -(25)^2\equiv$$
$$\equiv -(-6)^2\equiv -(36)\equiv -5\equiv 26,$$

то есть

$$\frac{1}{6}\equiv 26(\mathrm{mod}31).$$

Получаем

$$A^{-1}=\frac{1}{6}\cdot\begin{pmatrix}15 & -16\\ -9 & 10\end{pmatrix}\equiv 26\cdot\begin{pmatrix}15 & -16\\ -9 & 10\end{pmatrix}\equiv$$
$$\equiv\begin{pmatrix}390 & -416\\ -234 & 260\end{pmatrix}\equiv\begin{pmatrix}18 & -13\\ -17 & 12\end{pmatrix}\equiv\begin{pmatrix}18 & 18\\ 14 & 12\end{pmatrix}(\mathrm{mod}\ 31).$$

Проверим для обратной матрицы выполнение равенства

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

Действительно

$$A^{-1}\cdot A\equiv\begin{pmatrix}10 & 16\\ 9 & 15\end{pmatrix}\cdot\begin{pmatrix}18 & 18\\ 14 & 12\end{pmatrix}\equiv\begin{pmatrix}404 & 372\\ 372 & 342\end{pmatrix}\equiv$$
$$\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}(\mathrm{mod}31),$$
$$A^{-1}\cdot A\equiv\begin{pmatrix}18 & 18\\ 14 & 12\end{pmatrix}\cdot\begin{pmatrix}10 & 16\\ 9 & 15\end{pmatrix}\equiv\begin{pmatrix}342 & 558\\ 248 & 404\end{pmatrix}\equiv$$
$$\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}(\mathrm{mod}31),$$

Для расшифрования сообщения

Y ="3, 3, 9, 7, 19, 2, 25, 6, 19, 7, 22, 11, 17, 6, 2, 4, 23, 15, 8, 25, 17, 6",

необходимо его разбить на блоки по два символа, каждый блок умножить на матрицу A^{-1} и полученные числа привести по модулю 31:

$$\begin{pmatrix}18 & 18\\ 14 & 12\end{pmatrix}\cdot\begin{pmatrix}3\\ 3\end{pmatrix}\equiv\begin{pmatrix}108\\ 78\end{pmatrix}\equiv\begin{pmatrix}15\\ 16\end{pmatrix}(\mathrm{mod}\,31),$$

$$\begin{pmatrix}18 & 18\\ 14 & 12\end{pmatrix}\cdot\begin{pmatrix}9\\ 7\end{pmatrix}\equiv\begin{pmatrix}288\\ 210\end{pmatrix}\equiv\begin{pmatrix}9\\ 24\end{pmatrix}(\mathrm{mod}\,31),$$

$$\begin{pmatrix}18 & 18\\ 14 & 12\end{pmatrix}\cdot\begin{pmatrix}19\\ 2\end{pmatrix}\equiv\begin{pmatrix}378\\ 290\end{pmatrix}\equiv\begin{pmatrix}6\\ 11\end{pmatrix}(\mathrm{mod}\,31)\ \text{и т.д.}$$

Полученное закодированное сообщение X ="15,16, 9, 24, 6, 11, 0, 19, 3, 9, 5, 6, 11, 0, 15, 14, 2, 6, 5, 9, 11" при помощи таблицы преобразуется в исходное сообщение

X = «пришел_увидел_победил».

Выводы

В работе на основе изучения графа отношений между темами дисциплин «Алгебра и геометрия» и «Математические основы криптографии» определены разделы предмета «Алгебра и геометрия», на которые следует отвести большее количество часов на изучение.

В рассмотренных примерах решения задач из области криптографии показано использование алгебраических и геометрических знаний и навыков. Действительно, необходимо уметь вычислять обратную матрицу, определять алгебраические дополнения, складывать и вычитать матрицы и векторы, уметь решать сравнения и находить остатки от деления.

Следует отметить, что учебные занятия оптимально проводить с использованием передовых активных и интерактивных методов обучения, а именно: используя проблемное изложение материала, метод мозгового штурма и другие.

Конфликт интересов

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

Библиографический список

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

2. Данилова О.Ю., Телкова С.А. Реализация межпредметных связей дисциплин «Алгебра и геометрия» и «Математические основы криптографии» в вузах МВД России // Вестник Воронежского института высоких технологий. 2018. № 2 (25). С. 107–111.

3. Данилова О.Ю., Телкова С.А. Использование информационных технологий в процессе обучения математическим основам криптографии // XIX Международная научно-методическая конференция «Информатика: проблемы, методология, технологии» : сборник материалов конференции. Воронеж : Научно-исследовательские публикации (Вэлборн). 2019. С. 1958–1963.

4. Данилова О.Ю., Думачев В.Н. Математические основы криптографии : практикум. Воронеж : ВИ МВД России, 2019. 145 с.

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

6. Евграфова И.В. Межпредметные связи курсов физики и высшей математики в технических вузах : дис. ... канд. пед. наук. СПб., 2010. 160 с.

7. Кириченко О.Е. Межпредметные связи курса математики смежных дисциплин в техническом вузе связи как средство профессиональной подготовки студентов : дис. ... канд. пед. наук. Орел, 2003. 170 с.

8. Полат Е.С., Бухаркина М.Ю. Современные педагогические и информационные технологии в системе образования : учеб. пособие для студ. высш. учеб. заведений. 3-е изд., стер. М. : Академия, 2010. 368 с.

9. Селевко Г.К. Энциклопедия образовательных технологий : в 2 т. М.: НИИ школьных технологий, 2006. Т. 1. 816 с.

10. Сластенин В.А., Исаев И.Ф., Шиянов Е.Н. Педагогика : учеб. пособие для студ. высш. пед. учеб. заведений /отв. ред. В.А. Сластенин. М. : Академия, 2002. 576 с.

11. Современные образовательные технологии : учебное пособие / под ред. Н.В. Бордовской [и др.]. М. : КНОРУС, 2010. 432 с.

References

1. Danilova, O.Yu., Dumachev, V.N. (2017) *Matematicheskie osnovy kriptografii* [Mathematical foundations of cryptography: textbook]. Voronezh, VI MVD Rossii publ. 301 p. (In Russian)

2. Danilova, O.Yu., Telkova, S.A. (2018) Realizatsiya mezhpredmetnykh svyazei distsiplin «Algebra i geometriya» i «Matematicheskie osnovy kriptografii» v vuzakh MVD Rossii [Realization of intersubject communications of the disciplines "Algebra and Geometry" and "Mathematical Foundations of Cryptography" in the universities of the Ministry of Internal Affairs of Russia]. *Vestnik Voronezhskogo instituta vysokikh tekhnologii*. 2 (25), 107–111. (In Russian)

3. Danilova, O.Yu., Telkova, S.A. (2019) The use of information technologies in the process of teaching the mathematical foundations of cryptography. In: *XIX International Scientific and methodological Conference "Informatics: problems, methodology, technologies" : a collection of conference materials*. Voronezh: Nauchno-issledovatel'skiye publikatsii (Velborn) publ., pp. 1958–1963. (In Russian)

4. Danilova, O.Yu., Dumachev, V.N. (2019) *Matematicheskie osnovy kriptografii : praktikum* [Mathematical foundations of cryptography : practical work]. Voronezh, VI MVD Rossii publ. 145 p. (In Russian)

5. Dumachev, V.N., Men'shikh, V.V., Telkova, S.A. (2014) *Algebra i geometriya* [Algebra and geometry: textbook]. Voronezh, VI MVD Rossii publ. 431 p. (In Russian)

6. Evgrafova, I.V. (2010) *Mezhpredmetnye svyazi kursov fiziki i vysshei matematiki v tekhnicheskikh vuzakh. Diss. kand. ped. nauk* [Interdisciplinary connections of courses of physics and higher mathematics in technical universities. Cand. ped. sci. diss.]. St. Petersburg. 160 p. (In Russian)

7. Kirichenko, O.Ye. (2003) *Mezhpredmetnye svyazi kursa matematiki smezhnykh distsiplin v tekhnicheskom vuze svyazi kak sredstvo professional'noi podgotovki studentov. Diss. kand. ped. nauk* [Intersubject communications of the course of mathematics of related disciplines in a technical university of communication as a means of professional training of students. Cand. ped. sci. diss.]. Orel. 170 p. (In Russian)

8. Polat, Ye.S., Bukharkina, M.Yu. (2010) *Sovremennye pedagogicheskie i informatsionnye tekhnologii v sisteme obrazovaniya* [Modern pedagogical and information technologies in the education system]. Moscow, Akademiya publ. 368 p. (In Russian)

9. Selevko, G.K. (2006) *Entsiklopediya obrazovatel'nykh tekhnologii* [Encyclopedia of Educational Technologies]. Moscow, NII shkol'nykh tekhnologii publ. Vol. 1. 816 p. (In Russian)

10. Slastenin, V.A., Isayev, I.F., Shiyanov, Ye.N. (2002) *Pedagogika* [Pedagogy]. Moscow, Akademiya publ. 576 p. (In Russian)

11. Bordovskaya, N. V. et al. (ed.) (2010) *Sovremennyye obrazovatel'nyye tekhnologii* [Modern educational technologies]. Moscow, Knorus publ. 432 p. (In Russian)

Поступила в редакцию 25.07.2023
Подписана в печать 28.09.2023

Original article
UDC 378.147
DOI: 10.47438/2309-7078_2023_3_28

GRAPHIC REPRESENTATION OF INTERDISCIPLINARY RELATIONS OF THE DISCIPLINES "ALGEBRA AND GEOMETRY" AND "MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY"

Olga Yu. Danilova[1], Svetlana A. Telkova[2], Tatyana V. Larina[3]

Voronezh Institute of the Ministry of Internal Affairs of Russia[1, 2]
Voronezh, Russia
Voronezh State Pedagogical University[3]
Voronezh, Russia

[1]*Cand. Phys. and Mathl. Sci., Docent of the Department of Mathematics and Modeling Systems, ORCID ID: 0009-0006-2300-0937, e-mail: danilova_olga@hotmail.com*
[2]*Cand. Padagog. Sci., Docent of the Department of Mathematics and Modeling Systems, ORCID ID: 0000-0003-2401-8363, e-mail: tsa76@inbox.ru*
[3]*Cand. Padagog. Sci., Docent of the Department of Department of Computer Science, Information Technology and Digital Education, ORCID ID: 0000-0003-3942-4313, e-mail: tatilari06@rambler.ru*

Abstract. The article studies the relationship of the discipline of specialization "Mathematical Foundations of Cryptography", taught to cadets and students at the senior courses of the radio engineering faculty of the Voronezh Institute of the Ministry of Internal Affairs of Russia, with the basic discipline "Algebra and Geometry", which is studied in the first year. For the disciplines under consideration, the main topics are introduced and their relationships are shown visually in the form of graphs. At the same time, the topics that should be given the most attention are highlighted from the subject "Algebra and Geometry". Understanding the connections between the disciplines "Algebra and Geometry" and "Mathematical Foundations of Cryptography" allows you to build an optimal learning path for cadets and students, which allows you to understand which topics contribute most to obtaining the knowledge necessary in the future for professional activities. The formation of professional competencies is facilitated by practice-oriented tasks, examples of which are given in the article. The considered tasks are analyzed in laboratory classes in the course of studying the discipline "Mathematical Foundations of Cryptography". At the same time, when solving such problems, the wide use of knowledge from the course "Algebra and Geometry" is emphasized, which makes it possible to better understand the interdisciplinary connections of the disciplines under consideration and determine which topics should be given the most attention. Thus, an information security specialist needs to be able to calculate the remainders of division modulo encryption, the Euler function; determine whether a number is prime or composite; decompose a number into prime factors; solve comparisons and systems of comparisons by various methods; find inverse matrices in the ring of integers.

Key words: algebra and geometry, mathematical foundations of cryptography, interdisciplinary relations, matrix, Euler function, encryption, cryptographic algorithms, affine cryptosystem, matrix cryptosystem.

Cite as: Danilova, O.Yu., Telkova, S.A., Larina, T.V. (2023) Graphic representation of interdisciplinary relations of the disciplines "Algebra and geometry" and "Mathematical foundations of cryptography". *Izvestia Voronezh State Pedagogical University*. (3), 28–33. (In Russ., abstract in Eng.). DOI: 10.47438/2309-7078_2023_3_28

Received 25.07.2023
Accepted 28.09.2023