Актуальность внедрения основ криптографии в школьную программу: анализ целей, возможные подходы и средства программной поддержки

Анна Сергеевна Зуфарова
старший преподаватель кафедры «Высшая математика»
Тихоокеанский государственный университет
Хабаровск, Россия
006694@pnu.edu.ru
0000-0000-0000-0000

Юлия Сергеевна Бузыкова
доцент кафедры МОСИТ
Российский технологический университет
Москва, Россия
juliaserg_buz@mail.ru
0000-0000-0000-0000

Анастасия Дмитриевна Бурыкина
Группа КБ(с)-81
Тихоокеанский государственный университет
Хабаровск, Россия
2018102772@pnu.edu.ru
0000-0000-0000-0000

Поступила в редакцию 11.03.2023
Принята 22.04.2023
Опубликована 15.05.2023

10.25726/n6037-4575-5676-p

Аннотация

Актуальность данной темы обусловлена потребностью в специалистах в области информационной безопасности. Внедрение в школьный курс информатики основ криптографии может значительно повлиять на выбор профессии и качество специалистов в области защиты информации. В данной статье анализируется ситуация с изучением основ криптографии и основ защиты информации в школах. Предлагаются способы решения этой проблемы. Данная исследовательская работа обосновывает актуальность внедрения основ криптографии в школьную программу. В работе проанализированы цели обучения криптографии, рассмотрены возможные подходы и средства программной поддержки для эффективной реализации данного предмета в школьном образовании. Исследование основано на сравнительном анализе международных опытов внедрения криптографии в школьные программы. Результаты работы позволят определить оптимальные методы и подходы к преподаванию криптографии, выбрать подходящие инструменты программной поддержки и сформировать рекомендации для образовательных учреждений и учителей, желающих внедрить данную тему в школьную программу с целью развития информационной грамотности и кибербезопасности у учащихся.

Ключевые слова

криптография, информатика, шифрование, кодирование, информационная безопасность, защита информации, образовательный процесс, информационная культура.

Введение

Сегодня большинство населения Земли даже не задумывается над тем, что можно прожить хотя бы часть своей жизни без использования современных информационных технологий.

Ноутбуки, компьютеры, смартфоны, планшеты и другие IT технологии стали частью нашей повседневной жизни, они полноценное продолжение нас. С помощью этих гаджетов не только общаемся друг с другом, обмениваемся информацией, но и совершаем покупки в интернет магазинах и их приложениях. Так же бронируем и покупаем билеты на самолет и поезда, бронируем жилье, вызываем такси, записываемся на прием к врачу, используем телефоны как навигаторы, фото и видеокамеры, читалки, онлайн-банки, и просто как способ развлечься и скоротать время. Наши личные данные например, информация о платежных картах, данные паспорта, телефон и многое другое могут стать доступными для мошенников.

Для примера, пользователи, в своем большинстве, даже не представляют своего ежедневного существования без доступа к всемирной сети и по большей части не интересуются принципами ее работы, какие средства и современные инструменты при этом используются. Их основной целью и желанием является относительно легкое получение корректной к запросу, актуальной и наиболее полной информации вовремя, бесперебойно, в любой момент времени и качественно. Всемирная паутина стала отображением нашей цифровой жизни. Люди регистрируются в различных социальных сетях, заводят аккаунты, оставляют комментарии, ставят лайки. При регистрации указывают свою почту и данные карты при покупке товара. Например, почту взломали, в итоге этими данные могут воспользоваться мошенники. Так же эту информацию можно собрать и использовать в определенных целях, например фишинг, вейлинг и многое другое. Ресурсов, где мы можем оставить о себе информацию, сейчас существует множество и нужно быть подкованным человек в сфере информационной безопасности.

Одной из наиболее актуальных проблем современного общества является защита информации. Из-за низкой грамотности населения в области информационной безопасности возникает необходимость обучения школьников основам защиты информации и криптографии, а не которые выбираю такую профессию связанную с защитой информацией.

Самый популярный пароль в 2022 был password, на втором месте 12345. Простые пароли – одна из ключевых проблем обеспечения информационной безопасности организаций. Пользователи не соблюдают базовые требования к безопасности паролей и правила их хранения из-за того, что недостаточно хорошо понимают необходимость соблюдения требований к защите своих аккаунтов. Многие люди используют в качестве паролей личные данные: имена детей или родственников, дни рождения, клички животных и другое.

Получается учащиеся младшего, среднего и высшего звена и даже их родители не знают основ информационной безопасности. А многие выпускники не понимают специфики данной профессии. Поступают на данную профессию и разочаровываются. Понимают, что в основе лежит математика – царица наук.

Актуальность данной темы обусловлена дефицитом высококвалифицированных специалистов по защите информации. В ситуации возрастающей значимости вопросов информационной безопасности не во всех школьных программах по информатики рассматривается тема «Основы защиты информации», «Криптография», а в математике «теория чисел».

Материалы и методы исследования

Сейчас классы делятся на профильный и общий класс. Классы с профильном уклоном рассматривают эти темы, но не всех школах есть педагогические кадры, которые компетентны в этих вопросах. Например, учебный комплекс по информатике для учащихся 10-11 класс И.А.Калинин, Н.Н.Самылкина есть раздел «Система RSA, ключи открытые, закрытые, их получение». В учебники по информатике за 5 класс Л.Л.Босовой, А.Ю.Босовой присутсвует тема «Шифры», в учебнике информатика для учащихся 10-11 классов Н.В.Маркова затрагивают тему меры информационной безопасности-антивирусы. Проблема еще в самих учебниках по данной дисциплине. Каждое учебное заведение выбирают учебники под свою программу обучения. Хотелось бы ввести единые учебники для всей нашей

страны. Чтоб учебная программа не различалась в разных российских регионах. Например, семья с ребенком переехали из одного региона в другой. Дети поменяли школы, в итоге получаются разные программы обучения по данной дисциплине. Вследствие учащийся получает пробелы в знаниях по изучаемым дисциплинам.

Так же хотелось бы, чтоб данный материал читался на одном уровне в среднем звене, чтоб учащиеся в высшем звене определились со своей будующей профессией уже в школе. Чтоб они понимали, что их ждет в Вузе и было подготовленная база для освоения дисциплин.

Главным составляющем информационной безопасности, является криптография. Криптография (τκρυπτός «скрытый» + γράφω «пишу») с греческого переводится тайнопись. Это наука о методах обеспечения целостности данных.

В школьной программе среднего звена по информатике криптография рассматривается в рамках темы «кодирование», при этом не дается пояснение о разнице между понятиями шифрования и кодирования. Рассмотрим задание 2 из ОГЭ по информатике (рис.1).

2 От разведчика было получено следующее сообщение.

001001110110100

В этом сообщении зашифрован пароль – последовательность русских букв. В пароле использовались только буквы А, Б, К, Л, О, С; каждая буква кодировалась двоичным словом по следующей таблице.

А	Б	К	Л	О	С
01	100	101	111	00	110

Расшифруйте сообщение. Запишите в ответе пароль.

Ответ: _____.

Рисунок 1. Пример задания 2 из ОГЭ по информатике

Основой исследования являются работы в данных областях:

– защиты информации (А. И. Алексенцев, С. Г. Баричев, П. Гаррет);
– математических основ защиты информации (М. Айгнер, Дж. Андерсон, Е. Андреева);
– методики преподавания информатики в школе (С. А. Бешенков, А. Г. Гейн, А. П. Ершов);
– компетентностного подхода к образованию (А. А. Вербицкий, Д. А. Иванов, Е. Я. Коган).

Криптография и защита информации – это очень подвижный пласт науки, особенно в 21 веке, благодаря информационным технологиям. Так как почти вся информации хранится, обрабатывается и передается в цифровом формате. При этом нужно использовать актуальные методы защиты для нее.

Поэтому рабочие программы по этой дисциплине всегда должны оставаться актуальными.

На рынке труда в области информационной безопасности высокие требования к уровню знаний выпускников вузов, также требуется опыт работы в этой области. Увеличивается число хакерских атак, вследствие чего возрастает потребность в высококвалифицированных специалистах по защите информации, в то время как средние и высшие образовательные учреждения дают только базовые знания в этой профессии.

Результаты и обсуждение

В школьном образовании приоритетом является подготовка к сдаче базовых экзаменов для выдачи аттестатов, вследствие этого учителя, которые преподают неосновные предметы, могут не иметь соответствующей квалификации. Многие учителя информатики имеют низкий уровень знаний в области информационных технологий, программирования, защиты информации.

Для решения этой проблемы нужно вводить льготы для молодых специалистов, дополнительные выплаты, повышать уровень образования в педагогических вузах (ввести изучение криптографии или основ криптографии в программу подготовки учителей информатики), сотрудничать с IT компаниями.

Также проблемой является слабая, устаревшая материально-техническая база в школах: нехватка компьютеров, устаревшее аппаратное и программное обеспечение. Хотелось бы организовать «секретную комнату» или лабораторные стенды по основе защите информации.

Был проведен опрос студентов с первого по пятый курс специальности компьютерная безопасность ТОГУ. По результатам исследования видно, что 88% опрошенных студентов не изучали криптографию в школе, 68% не изучали теорию чисел в курсе математики, что приводит к трудностям в изучении криптографических методов защиты информации.

Так же 60 % опрошенных не знали простые и исторические шифры. А с современной криптографией не знакомы было 90% опрошенных студентов.

Решением проблемы является введение криптографии в школьный курс информатики – «Основы информатики, защиты информации и криптографии».

Этот курс разделим на три пласта: начальный, базовый, продвинутый, как раз по звеньям школы (начальная, средняя и старшая школы).

Начальный курс проводить в начальной школе в игровом формате, квестах, максимально использовать картинки, инфограмм и схем - визуализация данных способствует быстрому усвоения информации (Зуфарова, 2020), так же нужно включить ассоциации для учащихся - ассоциативное мышление очень важно на начальном этапе изучения предмета (Зуфарова, 2020), креативная педагогика (Зуфарова, 2020). В этот период обучения подготовим фундамент для бушующих знаний.

Этот тандем элементов педагогики обеспечит понимание и освоение тематики и созданию базы знаний для дальнейшего обучения в среднем и высшем звене школы.

На рисунке 2, учащихся знакомят с определением криптография

Рисунок 2. Пример презентации

Переходя в среднее звено нужно так же взять за основу обучение в младшем звену (креативная педагогика, инфограмма, игровая форма), но добавлять уже усложнённые элементы данного курса (Угринович, 2011).

В средней школе – начнем изучение исторические шифры и основы криптографии (рис.3).

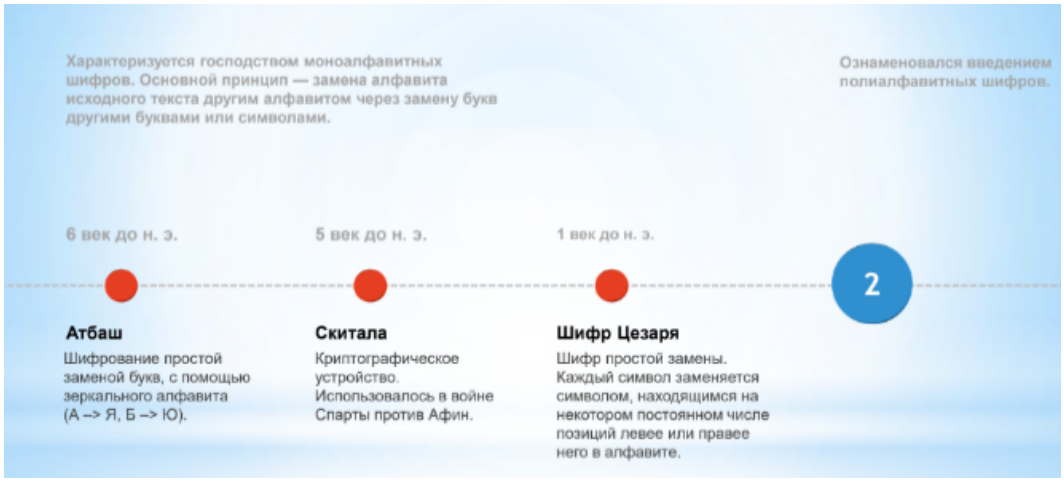

Рисунок 3. Пример презентации

На первом этапе ребята проходят исторические шифры. Знакомство и изучение исторических шифров – первый шаг в сторону освоения профессии криптоаналитика. Освоение первых шифров помогает точнее понять, с какой целью применяется та или иная операция в современном алгоритме шифрования. Изучение исторических шифров — это основа для понимания, что такое шифр, ключ и что такое наука криптография. Так же показывает математические основы алгоритмов (Калинин, 2014). К историческим шифрам относятся шифр Цезаря, шифр Виженера, квадрат Полибия и многие другие.

Шифрование шифром Цезаря «безкомпьютерным» вариантом на практике осуществляется проще, чем написание полноценного криптографического алгоритма. Как раз в этой теме поможет разобраться MS Excel. В MS Excel есть удобная функция – копирование формул и показ формул. Пример реализации шифра Цезаря в MS Excel (рис. 4 и рис. 5).

D7 =ЕСЛИ(ПОИСКПОЗ(B7;ABC;0)+$D$4>40;ПОИСКПОЗ(B7;ABC;0)+$D$4-40;ПОИСКПОЗ(B7;ABC;0)+$D$4)

	A	B	C	D	E	F	G	H
1		Гай Юлий Цезарь:"Пришел, увидел, победил!"						
2								
3		ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ!"		42				
4			k=	1				
5								
6	1	Г	11	12	Д	Д		
7	2	А	8	9	Б	ДБ		
8	3	Й	18	19	К	ДБК		
9	4		3	4	:	ДБК:		
10	5	Ю	39	40	Я	ДБК:Я		
11	6	Л	20	21	М	ДБК:ЯМ		
12	7	И	17	18	Й	ДБК:ЯМЙ		
13	8	Й	18	19	К	ДБК:ЯМЙК		
14	9		3	4	:	ДБК:ЯМЙК:		
15	10	Ц	31	32	Ч	ДБК:ЯМЙК:Ч		
16	11	Е	13	14	-	ДБК:ЯМЙК:Ч-		
17	12	З	16	17	И	ДБК:ЯМЙК:Ч-И		
18	13	А	8	9	Б	ДБК:ЯМЙК:Ч-ИБ		
19	14	Р	25	26	С	ДБК:ЯМЙК:Ч-ИБС		
20	15	Ь	37	38	Э	ДБК:ЯМЙК:Ч-ИБСЭ		
21	16	:	4	5	"	ДБК:ЯМЙК:Ч-ИБСЭ"		
22	17	"	5	6	!	ДБК:ЯМЙК:Ч-ИБСЭ"!		
23	18	П	24	25	Р	ДБК:ЯМЙК:Ч-ИБСЭ"!Р		
24	19	Р	25	26	С	ДБК:ЯМЙК:Ч-ИБСЭ"!РС		
25	20	И	17	18	Й	ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙ		
26	21	Ш	33	34	Щ	ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙЩ		
27	22	Е	13	14	-	ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙЩ-		
28	23	Л	20	21	М	ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙЩ-М		
29	24	,	2	3		ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙЩ-М		
30	25		3	4	:	ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙЩ-М :		

Рисунок 4. Шифрование. Шифр Цезаря.

D6 =ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)-$D$4<0;ПОИСКПОЗ(B6;ABC;0)-$D$4+40;ПОИСКПОЗ(B6;ABC;0)-$D$4)

	A	B	C	D	E	F	G	H	I	J	K	L	M
1		ДБК:ЯМЙК:Ч-ИБСЭ"!РСЙЩ-М :ФГЙЕ-М :РПВ-ЕЙМ;!											
2													
3				42									
4			k=	1									
5													
6	1	Д	12	11	Г	Г							
7	2	Б	9	8	А	ГА							
8	3	К	19	18	Й	ГАЙ							
9	4	:	4	3		ГАЙ							
10	5	Я	40	39	Ю	ГАЙ Ю							
11	6	М	21	20	Л	ГАЙ ЮЛ							
12	7	Й	18	17	И	ГАЙ ЮЛИ							
13	8	К	19	18	Й	ГАЙ ЮЛИЙ							
14	9	:	4	3		ГАЙ ЮЛИЙ							
15	10	Ч	32	31	Ц	ГАЙ ЮЛИЙ Ц							
16	11	-	14	13	Е	ГАЙ ЮЛИЙ ЦЕ							
17	12	И	17	16	З	ГАЙ ЮЛИЙ ЦЕЗ							
18	13	Б	9	8	А	ГАЙ ЮЛИЙ ЦЕЗА							
19	14	С	26	25	Р	ГАЙ ЮЛИЙ ЦЕЗАР							
20	15	Э	38	37	Ь	ГАЙ ЮЛИЙ ЦЕЗАРЬ							
21	16	"	5	4	:	ГАЙ ЮЛИЙ ЦЕЗАРЬ:							
22	17	!	6	5	"	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"							
23	18	Р	25	24	П	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"П							
24	19	С	26	25	Р	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПР							
25	20	Й	18	17	И	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИ							
26	21	Щ	34	33	Ш	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШ							
27	22	-	14	13	Е	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕ							
28	23	М	21	20	Л	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ							
29	24		3	2	,	ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ,							

Рисунок 5. Дешифрование. Шифр Цезаря

Второй по простоте это шифр Виженера. Шифр Виженера – способ полиалфавитной замены с использованием ключевого слова. Для реализации шифра Виженера в MS Excel используется данный алгоритм (рис.6).

Современный мир все больше зависит от цифровых технологий и интернета, что влечет за собой увеличение угроз в области информационной безопасности. В этом контексте внедрение основ криптографии в школьную программу приобретает особую актуальность. Криптография – это наука о методах защиты информации путем шифрования и дешифрования данных. Одной из основных целей внедрения криптографии в школьную программу является развитие информационной грамотности и кибербезопасности у учащихся. Обучение основам криптографии позволит детям и подросткам понять принципы шифрования, защиты информации и основные методы криптоанализа. В рамках внедрения криптографии в школьную программу можно использовать различные подходы. Один из них – интеграция криптографии в предметы, такие как информатика или математика. Это позволит связать изучение криптографии с уже существующими учебными программами и упражнениями. Другой подход – создание специального курса по криптографии, который будет изучаться в отдельных классах или кружках. Для эффективной реализации криптографии в школьной программе необходима программная поддержка. Существуют специализированные программы и инструменты, которые помогают учащимся понять и применять основы криптографии на практике. Эти средства программной поддержки могут включать интерактивные задания, визуализацию шифров и дешифрования, а также симуляции криптоанализа. В заключение, внедрение основ криптографии в школьную программу является актуальным и важным шагом для подготовки учащихся к цифровой среде и обеспечения их информационной безопасности. Это позволит им развивать навыки анализа, критического мышления и защиты данных, что является неотъемлемой частью современного образования.

B6 =СИМВОЛ(КОДСИМВ("a")+ОСТАТ(КОДСИМВ(B5)-КОДСИМВ("a")+B4;26))

	A	B	C	D	E	F	G	H	I
1									
2					Шифр Виженера				
3	Ключ	b	a	n	k	b	a	n	k
4	Сдвиг	2	1	14	11	2	1	14	11
5	Исходный текст	g	e	o	m	e	t	r	y
6	Зашифрованный текст	i	f	c	x	g	u	f	j
7									
8	Ключ	b	a	n	k	b	a	n	k
9	Сдвиг	2	1	14	11	2	1	14	11
10	Исходный текст	d	i	s	c	o	v	o	d
11	Зашифрованный текст	f	j	g	n	q	w	c	o
12									
13	Ключ	b	a	n	k	b	a	n	k
14	Сдвиг	2	1	14	11	2	1	14	11
15	Исходный текст	c	o	m	p	u	t	e	r
16	Зашифрованный текст	e	p	a	a	w	u	s	c
17									
18	Ключ	b	a	n	k	b	a	n	k
19	Сдвиг	2	1	14	11	2	1	14	11
20	Исходный текст	k	e	y	b	o	a	r	d
21	Зашифрованный текст	y	f	m	m	q	b	f	o

Рисунок 6. Реализация шифра Виженера

Третий исторический шифр, рассмотренный нами – полибианский квадрат. Полибианский квадрат – шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (рис.7).

	A	B	C	D	E	F	G	H	I	J	K	L
1	а	б	в	г	д	е/ё						
2	ж	з	и/й	к	л	м						
3	н	о	п	р	с	т						
4	у	ф	х	ц	ч	ш/щ						
5	ъ	ы	ь	э	ю	я						
6	метод 1											
7	к	р	и	п	т	о	г	р	а	ф	и	я
8	D2	D3	C2	C3	F3	B3	D1	D3	A1	B4	C2	F5
9												
10	метод 2											
11	к	р	и	п	т	о	г	р	а	ф	и	я
12	р	ц	п	х	ш/щ	ф	к	ц	ж	ы	п	ш/щ

Рисунок 7. Квадрат Полибия

Преимуществами использования MS Excel для изучения исторических шифров является доступность программы, интуитивно понятный интерфейс, возможность легко построить наглядные таблицы, что позволяет применять MS Excel в обучении школьников, так как не нужно глубокого знания в программировании. Так же существуют множество специализированных программ для изучения криптографии (Ниссенбаум, 2012). Например CrypTool. С помощью этой программы можно реализовать исторические шрифты.

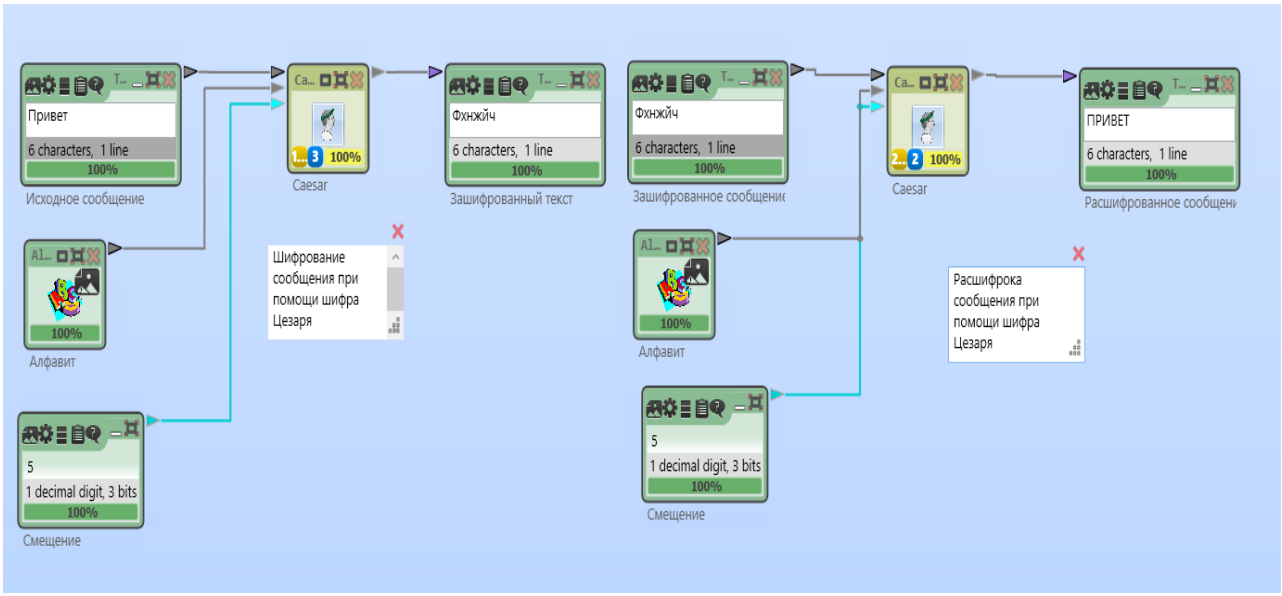

Рисунок 8. Реализация шифра Цезаря в CrypTool

Так же с ребятами можно создать виртуальный тренажер на сайте педагога (Макарова, 1999). Это уже углубленная форма изучения криптографии и программирования.

Рисунок 9. Реализация. шифра Цезаря на сайте педагога

В старшей школе – изучение криптосистем с открытым ключом: шифр RSA, шифр Эль-Гамаля, алгоритм Диффи-Хеллмана, электронную цифровую подпись и основы криптографических протоколов (рис.9).

Рисунок 9. Пример презентации для среднего звена школы

Электронная подпись, созданная с помощью криптографических алгоритмов, является надежным способом защиты данных и сообщений от несанкционированного доступа и изменения. История создания электронной подписи началась в конце XX века, и на данный момент она является неотъемлемой частью электронной коммуникации (Василенко, 2012).

Также в средней и старшей школе нужно использовать теоретические и практические задания, в которых нужно использовать наглядное пособие (Рябко, 2011).

На первом этапе учащиеся высшего звена должны пройти ассиметричные и симметричные системы шифрования. Подробно изучит систему RSA и Эль-Гамаля, для дальнейшего ЭЦП.

Для изучения школьниками электронных подписей были выбраны алгоритмы: RSA, электронная подпись Эль-Гамаля, и российский ГОСТ Р 34.10–2012 основанный на эллиптических кривых. По ним можно разработать программный комплекс для изучения и проверки данных.

Данные алгоритмы отличаются математическими подходами к защите информации и стойкостью криптосистемы. Так же имеют свои уникальные преимущества и недостатки. Поэтому ученики в школе

смогут ознакомиться с различными криптографическими системами. Так как многие школьники не обладают достаточными знаниями для вычисления электронных подписей по выше указанным алгоритмам (Нестеренко, 2012).

Рисунок 10. Пример презентации для среднего звена школы по ЭЦП

Разработанная программа даст возможность ученикам опробовать свои силы в криптографии, и позволит им более глубоко понять, насколько эта сфера может быть увлекательной и интересной (Коблиц, 2001).

По мере изучения разделов учащиеся должны усвоить следующие основные понятия: шифр, секретный и открытый ключ, кодирование, шифрование, дешифрование данных, криптографический протокол, электронная подпись, электронные деньги и разберутся в математике и теории чисел (Босова, 2015).

Благодаря этому ново введению, у учеников появятся основные знания и навыки работы в информационной безопасности. Что благоприятно повлияет в выборе их будущей профессии и в качестве выпускников Вузов.

Заключение

Из вышесказанного можно сделать вывод, чтобы решить проблемы в обучении специалистов по защите информации, нужно:

– ввести в школах предметы по изучению основ криптографии, защиты информации, теория чисел;
– создать актуальную техническую базу;
– развивать сотрудничество с IT-компаниями в области обучения учеников, проводить экскурсии;
– ежегодно обновлять и добавлять актуальную информацию в рабочие программы;
– актуализировать теоритическую и практическую информацию;
– ежегодное повышение квалификации педагогов и многое другое.

В данной статье была представлены примерная структура обучения учащихся, примерные практические работы, что позволит расширить знания учащихся в области защиты информации.

Список литературы

1. Босова Л.Л., Босова А.Ю. Информатика: учебник для 5 класса. М.: Бином, 2015.184 с.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО,2003. 328 с.
3. Зуфарова А.С. Роль информационных технологий в образовательном процессе // Управление образованием:т еория и практика. 2020. № 3(39). С. 105-114.
4. Зуфарова А.С., Роль технологии визуализации в учебной информации // Современное педагогическое образование. 2020. № 9. С. 39-41.
5. Калинин И.А., Самылкина Н.Н. УМК «Информатика», 10–11 классы. Углубленный уровень. М.: Бином, 2014. 344 с.
6. Коблиц Н. Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001. 260 с.
7. Макарова Н.В. Информатика. 10–11 класс. СПб.: ПитерКом, 1999. 304 с.
8. Нестеренко А.Ю. Теоретико-числовые алгоритмы в криптографии. М.: МГИЭиМ,2012. 224 с.
9. Ниссенбаум О.В., Поляков Н.В. Криптографические протоколы: лабораторный практикум: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем». Тюмень: ТюмГУ, 2012. 40 с.
10. Рябко Б. ., Фионов А.Н. Основы современной криптографии и стеганографии. М.:Горячая линия-Телеком, 2011. 232 с.
11. Угринович Н.Д. Информатика. Учебник для 10–11 кл. М.: Лаборатория Базовых Знаний, 2011. 512 с.

The relevance of introducing the basics of cryptography and the basics of information security in the school course in computer science

Anna S. Zufarova
Senior lecturer of the Department of "Higher mathematics"
Pacific State University
Khabarovsk, Russia
006694@pnu.edu.ru
0000-0000-0000-0000

Yulia S. Buzykova
Associate Professor of the Department of MOSIT
MIREA-Russian Technological University
Moscow, Russia
juliaserg_buz@mail.ru
0000-0000-0000-0000

Anastasia D. Burykina
KB Group(s)-81
Pacific State University
Khabarovsk, Russia
2018102772@pnu.edu.ru
0000-0000-0000-0000

Received 11.03.2023
Accepted 22.04.2023
Published 15.05.2023

10.25726/n6037-4575-5676-p

Abstract

The relevance of this topic is due to the need for specialists in the field of information security. The introduction of the basics of cryptography into the school computer science course can significantly affect the choice of profession and the quality of specialists in the field of information security. This article analyzes the situation with the study of the basics of cryptography and the basics of information security in schools. The ways of solving this problem are suggested. This research paper substantiates the relevance of introducing the basics of cryptography into the school curriculum. The paper analyzes the goals of teaching cryptography, considers possible approaches and software support tools for the effective implementation of this subject in school education. The study is based on a comparative analysis of international experiences of implementing cryptography in school curricula. The results of the work will allow us to determine the best methods and approaches to teaching cryptography, choose suitable software support tools and form recommendations for educational institutions and teachers who want to introduce this topic into the school curriculum in order to develop information literacy and cybersecurity among students.

Keywords

cryptography, computer science, encryption, encoding, Information Security.

References

1. Bosova L.L., Bosova A.Ju. Informatika: uchebnik dlja 5 klassa. M.: Binom, 2015.184 s.
2. Vasilenko O.N. Teoretiko-chislovye algoritmy v kriptografii. M.: MCNMO,2003. 328 s.
3. Zufarova A.S. Rol' informacionnyh tehnologij v obrazovatel'nom processe // Upravlenie obrazovaniem:t eorija i praktika. 2020. № 3(39). S. 105-114.
4. Zufarova A.S., Rol' tehnologii vizualizacii v uchebnoj informacii // Sovremennoe pedagogicheskoe obrazovanie. 2020. № 9. S. 39-41.
5. Kalinin I.A., Samylkina N.N. UMK «Informatika», 10–11 klassy. Uglublennyj uroven'. M.: Binom, 2014. 344 s.
6. Koblic N. Kurs teorii chisel i kriptografii. M.: Nauchnoe izd-vo TVP, 2001. 260 s.
7. Makarova N.V. Informatika. 10–11 klass. SPb.: PiterKom, 1999. 304 s.
8. Nesterenko A.Ju. Teoretiko-chislovye algoritmy v kriptografii. M.: MGIJeiM,2012. 224 s.
9. Nissenbaum O.V., Poljakov N.V. Kriptograficheskie protokoly: laboratornyj praktikum: uchebno-metodicheskoe posobie dlja studentov special'nostej «Komp'juternaja bezopasnost'» i «Informacionnaja bezopasnost' avtomatizirovannyh sistem». Tjumen': TjumGU, 2012. 40 s.
10. Rjabko B. ., Fionov A.N. Osnovy sovremennoj kriptografii i steganografii. M.:Gorjachaja linija-Telekom, 2011. 232 s.
11. Ugrinovich N.D. Informatika. Uchebnik dlja 10–11 kl. M.: Laboratorija Bazovyh Znanij, 2011. 512 s.