Краснодарский университет МВД России

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

Материалы
XVI Всероссийской научно-практической конференции
(19 июня 2020 г.)

Краснодар
2020

УДК 004+51
ББК 22.1+32.97
М34

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

М34 **Математические методы** и информационно-технические средства : материалы XVI Всерос. науч.-практ. конф., 19 июня 2020 г. / редкол.: И. Н. Старостенко, Е. В. Михайленко, А. В. Еськов, С. К. Ефремов, А. А. Хромых, К. И. Руденко. – Краснодар : Краснодарский университет МВД России, 2020. – 132 с.

ISBN 978-5-9266-1616-0

В сборнике содержатся материалы XVI Всероссийской научно-практической конференции, состоявшейся в Краснодарском университете МВД России 19 июня 2020 г., по направлениям: «Математические методы и моделирование», «Программное обеспечение и информационно-технические средства», «Информационные технологии в борьбе с экстремизмом, терроризмом и организованной преступностью», «Проблемы информационной безопасности», «Информационные технологии в образовании».

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 004+51
ББК 22.1+32.97

ISBN 978-5-9266-1616-0

Архангельская Екатерина Владиславовна

ПРИМЕР РАЗРАБОТКИ ЭЛЕКТРОННОГО ПОСОБИЯ ДЛЯ ОСВОЕНИЯ МЕТОДОВ РЕШЕНИЯ НЕЛИНЕЙНЫХ УРАВНЕНИЙ

Численные методы решения различных прикладных задач изучаются в рамках многих дисциплин: «Математика», «Вычислительная математика», «Системный анализ» и т.п. Обучающимся, для которых математические дисциплины не являются профилирующими,в рамках рабочих программ предъявляются требования освоить вычисления по формулам численных методов в ручном режиме без разработки программ и без использования специальных математических прикладных программных пакетов [1]. Процесс поверки решения задач с помощью численных методов в этом случае является достаточно трудоемким и длительным по времени. Время может быть ограничено, например, при проведении зачета или экзамена, где в качестве практического задания требуется решить задачу, применяя определенный численный метод. В статье представлен вариант электронного пособия для освоения метода Ньютона нахождения решения нелинейных алгебраических уравнений с автоматической проверкой правильности выполнения первого шага метода, что значительно ускоряет процесс проверки общего решения задачи.

Электронное пособие представляет собой файл Excel с поддержкой макросов [2]. При открытии файла пособия на листе книги Excel представлено условие задания, которое нужно выполнить – уравнение и численный метод, который нужно использовать для его решения. В задании требуется найти решение кубического у равнения методом Ньютонасточностьюε = 0,01 и заданным начальным приближением x_0, вычисления проводить до трех знаков после запятой. Так как основной целью разработанного пособия является именно освоение вычисления по формулам метода, поэтому в заданиях представленные уравнения третьей степени вида $ax^3 + bx + c = 0$, что позволяет избежать громоздких расчетов. Метод Ньютоны обладает достаточно быстрой сходимостью, что позволяет найти решение за небольшое число итераций. Уравнение и начальное приближение x_0 подбираются таким образом, чтобы первое приближение метода выражалось десятичным числом с одним или двумя знаками после запятой, именно первое приближение нужно будет указать пользователю в качестве промежуточного результата для проверки правильности процесса решения. Указанное требование к первому приближению позволяет избежать необходимость округления числа при вводе и тем самым произвести автоматическую проверку сравнением двух чисел. Для подбора коэффициентов уравнения использовались расчеты в Excel. На рисунке 1 представлены результаты вычисления величин, необходимых для нахождения решения уравнения $x^3 – x + 4 = 0$ методом Ньютона с начальным приближением $x_0 = –1$ и заданной точностью ε = 0,01.

	x_k	$f(x_k)$	$f'(x_k)$	x_{k+1}	$\lvert x_k - x_{k+1}\rvert$
0	-1	4	2	-3	2
1	-3	-20	26	-2,2308	0,769230769
2	-2,23077	-4,87028	13,92899	-1,8811	0,34965035
3	-1,88112	-0,77542	9,615825	-1,8005	0,080640395
4	-1,80048	-0,03617	8,725168	-1,7963	0,004145896

Рис.1. Расчеты для решения уравнения $x^3 – x + 4 = 0$ методом Ньютона

Как видно из рисунка 1, в данной задаче первое приближение $x_1 = –3$, и число итераций $n = 4$, которое необходимо для достижения заданной точности ε = 0,01. Таким способом подобраны несколько уравнений для заданий, например, для уравнения $2x^3 – x + 4 = 0$ и начального приближения $x_0 = –1$ первое приближение $x_1 = –1,6$ и число ите-

раций $n = 4$, для уравнения $x^3 - 2x + 8 = 0$ и начального приближения $x_0 = -2$ первое приближение$x_1 = -2{,}4$ и число итераций $n = 3$, и т.п.

Открывая файл пособия, пользователь видит на экране условие одной из всех имеющихся постановок задач. Для осуществления выбора одного из вариантов случайным образом все задачи размещены на листе, скрытом от пользователя, в виде таблицы, представленной на рисунке 2.

	A	B	C	D	E
1	Номер задания	Уравнение	Начальное значение	Первое приближение	Число итераций
2	1	$x^3 - x + 4 = 0$	-1	-3	5
3	2	$x^3 - x + 2 = 0$	-1	-1,5	4
4	3	$x^3 - x + 3 = 0$	-1	-2,5	5
5	4	$x^3 - 2x + 8 = 0$	-2	-2,4	3
6	5	$x^3 - 2x + 8 = 0$	-3	-2,48	3
7	6	$x^3 - 7x + 7 = 0$	-2	-4,6	5
8	7	$2x^3 - x + 4 = 0$	-1,5	-1,4	2
9	8	$2x^3 - x + 4 = 0$	-1	-1,6	4
10	9	$3x^3 - x + 8 = 0$	-1	-1,75	4

Рис.2. Данные для формирования условия задачи

Выбор варианта реализован с помощью программного кода, разработанного в среде программирования VBAExcel, который срабатывает при открытии файла пособия. Данный программный код случайным образом определяет число от одного до девяти и записывает его в ячейку X1 листа с заданием, которая не видна пользователю. Для того чтобы код срабатывал при открытии файла, его команды записаны внутри процедуры Workbook_Open() [3]. Кодпроцедурыпредставленниже:

```
PrivateSubWorkbook_Open()
Randomize
Range("X1").Value = Int((9 - 1 + 1) * Rnd + 1)
End Sub
```

В данном коде запускается генератор случайных чисел командой Randomize, выражение Int((9 - 1 + 1) * Rnd + 1) определяет случайное число от одного до девяти [4]. Затем условие задачи формируется с помощью функций табличного процессора Excel. Вид задачи, которую требуется решить, формирующуюся при открытии файла пособия, представлен на рисунке 3:

	A	B	C	D	E	F	G	H
1	Найдите решение данного уравнения методом Ньютона с точностью ε = 0,01 и начальным приближением $x_0 = -3$							
2								
3				$x^3 - 2x + 8 = 0$				
4								
5	Введите первое приближение				$x_1 =$			
6								
7	Введите необходимое число итераций				$n =$			

Рис.3. Условия задачи в файле электронного пособия

Для отображения уравнения в ячейке D3 используется функция ВПР(X1;Лист2!A1:E10;2), которая задает значение, содержащееся во втором столбце исходной таблицы с заданиями (рис. 2) и в строке с номером, сформированном случайным образом в ячейке X1 при открытии файла, в данном случае значение подставляется из строки с номером задания 5. При разработке пособия автор столкнулся с особенностями обработки текстовых строк в функциях и формулах программы Excel, а именно при отображении текста с помощью функций теряются элементы форматирования шрифта, такие как надстрочное и подстрочное видоизменения шрифта и начертание курсив. Так, в частности, при использовании функции ВПР для отображения уравнения, в ячейке D3 появляется не уравнение вида $x^3 - 2x + 8 = 0$, которое записано в ячейке B6 таблицы с исходными данными, расположенной на скрытом от пользователя листе (рис. 2), а выражение вида x3 – 2x + 8 = 0. Для того чтобы вернуть знак степени, нужно применить надстрочное видоизменение к символу 3, который является вторым в данной текстовой строке. По этой причине функция ВПР(X1;Лист2!A1:E10;2) для отображение уравнения вводится в ячейку X3, невидимую для пользователя, затем в программном коде процедуры Workbook_Open() значение этой ячейки копируется в ячейку D3, чтобы можно было использовать команды преобразования строк. Изменение видоизменения шрифта символа на надстрочный выполняется в программном коде с помощью команды Range("D3").Characters(2, 1).Font.Superscript = True, в которой указывается позиция символа – 2. Но в уравнениях с номерами 7, 8, 9 (рис. 2) перед элементом x^3 стоит коэффициент, т.е. нужно учитывать, что показатель степени 3 является третьим символом в текстовой строке. Программный код, который определяет окончательный вид уравнения в ячейке D3 (рис. 3), представлен ниже:

```
Range("D3") = Range("X3")
If Range("X1").Value < 7 Then
Range("D3").Characters(2, 1).Font.Superscript = True
Else
Range("D3").Characters(3, 1).Font.Superscript = True
EndIf
```

Аналогичным образом формируется условие задачи в ячейке A1. В ячейку X2 записывается текст «Найдите решение данного уравнения методом Ньютона с точностью ε = 0,01 и начальным приближением x_0 =», в ячейку Y2 вводится выражение =X2& ВПР(X1;Лист2!A1:E10;3), которое выполняем слияние условия задачи и начального значения, записанного в таблице исходных данных в третьем столбце, в единый текст. Затем в программном коде процедуры Workbook_Open() значение этой ячейки копируется в ячейку A1 с помощью команды Range("A1") = Range("Y2"). С помощью команды Range("A1").Characters(98, 1).Font.Subscript = True задается видоизменение подстрочный символа 0 в выражении x_0, и с помощью команды Range("A1").Characters(63, 1).Font.Name = "Symbol" задается шрифт Symbol символу ε, в противном случае, данный символ будет отображаться в ячейке как e.

После решения задачи пользователю необходимо ввести требуемые в задании полученные величины, а именно первое приближение x_1 в ячейку F5 и необходимое число итераций для достижения заданной точности в ячейку F7. Вычисленное первое приближение позволяет определить, что обучаемый освоил формулы метода, а число итераций – что вычисления проведены верно. Автоматическая проверка правильности введенных результатов реализована с помощью функций ЕСЛИ и ВПР. Так, в ячейку X5 введена функция ЕСЛИ(F5=ВПР(X1;Лист2!A1:E10;4);”Верно”;“Неверно!!!”), которая сравнивает значение первого приближения, введенного пользователем в ячейку F5, и

значение первого приближения задачи, которое записано в четвертом столбце таблицы исходных данных (рис. 2).

Аналогичная функцияЕСЛИ(F7=ВПР(X1;Лист2!A1:E10;5);”Верно”;“Неверно!!!”) введена в ячейку X7, которая сравнивает значение числа итераций, введенного пользователем в ячейку F7, и необходимое число итераций для решения уравнения с заданной точностью, записанное в пятом столбце таблицы исходных данных и соответствующее заданному варианту. Провести такое сравнение с помощью функции ЕСЛИ возможно, т.к. изначально было выполнено требование, что искомые величины выражаются конечными десятичными числами. Для проверки правильности решения достаточно воспользоваться полосой прокрутки. В электронном пособии можно реализовать проверку правильности нахождения корня уравнения, но в этом случае нужно учитывать погрешность округления до двух знаков на каждом шаге, и целесообразно проверять не само значение корня, а его попадание в некоторый диапазон.

Описанное в статье электронное пособие предназначено для использования на практических занятиях в компьютерных классах. В нем обеспечивается формирование разных вариантов задач на разных компьютерах и автоматическая проверка правильности решения задачи. Данный информационный ресурс может использоваться для самостоятельного [5] и дистанционного обучения.

Литература

1. Изотова В.Ф. Применение дистанционных образовательных технологий в заочном обучении. Вестник Саратовской государственной юридической академии. 2016. № 1 (108). С. 255-259.

2. Архангельская Е.В. Изучение комплексного взаимодействия офисных программ при использовании информационных технологий в практике юриста. Информатизация образования и науки. 2019. № 2 (42). С. 146-153.

3. Архангельская Е.В. Об одной реализации метода динамического программирования для решения задачи о замене оборудования с помощью прикладной программы. Системы и средства информатики. 2018. Т. 28. № 2. С. 178-188.

4. Архангельская Е.В. Курс информатики для юристов. Учебно-методическое пособие / Е. В. Архангельская; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, Гос. Образовательное учреждение высш. Проф. Образования «Саратовская гос. акад. права». Саратов, 2008.

5. Изотова В.Ф. Электронные и дистанционные технологии в организации самостоятельной работы студентов. В сборнике: Непрерывная предметная подготовка в контексте педагогических инноваций сборник научных трудов: в 2-х частях. 2016.С. 190-193.

Сведения об авторе

Архангельская Екатерина Владиславовна, кандидат физико-математическихнаук, доцент кафедры информационного права и цифровых технологий Саратовская государственная юридическая академия; e-mail: katysar@rambler.ru.

Акапьев Виктор Львович,
Прокопенко Алексей Николаевич,
Савотченко Сергей Евгеньевич

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Проблемы, существующие в обеспечении экономической безопасности России, сейчас как никогда актуальны и находятся в постоянной динамике[1, 2]. Оценка степе-

ни государственного долга, ослабление потенциала в научно-технической сфере, дезорганизация экономики в рамках как отдельных субъектов, предприятий, так и всего государства, резкая дифференциация в доходах населения, утечка денежных средств за рубеж, а вместе с тем и снижение уровня жизнеобеспечения и благополучия граждан показывают, что уровень экономической безопасности нашей страны продолжает снижаться. Указанная причина требует применения безотлагательных мер практического и теоретического характера с использованием информационных технологий [3, 4].

Именно информационные технологии (ИТ) должны стать «спасителями» состояния экономической безопасности в XXI веке. На сегодняшний день ИТ представляют собой целый комплекс мероприятий, который строго регламентирован правилами и непосредственно направлен на переработку, защиту, хранение и осуществление операций различного характера над информацией[5].

ИТ реализуют процесс со значительным расширением масштабов перерабатываемой информации и, в конечном счёте, приводят к сокращению количества времени её обработки[6]. Информационные технологии представляют собой не только инструмент использования данных в управлении, но и средство переработки и защиты значимой, скрытой информации.

Для того, чтобы полностью понять сущность применения информационных технологий в сфере экономической безопасности, необходимо непосредственно обратиться к ряду проблем, возникающих в данной области и методам их решения с использованием ИТ.Особенно актуальна данная проблема именно сегодня, когда широко внедряется цифровая экономика [7].

В первую очередь, следует обозначить проблемы, связанные с защитой электронных денег как на уровне граждан, так и больших предприятий [8].

Актуальной проблемой в современном мире является похищение денежных средств со счетов граждан, частных и государственных организаций мошенниками. Так, в истории имел место случай хищения средств со счёта Центрального банка, которые принадлежали Пенсионному фонду Российской Федерации. Это преступление, которое вскоре было раскрыто, в сфере экономической безопасности назвали «кражей века». Как показывает практика, этот случай далеко не единичный [9].

Второй, не менее важной проблемой, является неправомерное обналичивание денежных средств, которое необходимо дифференцировать с правомерным обналичиванием. Это действие, называемое «обналичкой», представляет собой деятельность индивидуальных предпринимателей и частных экономических предприятий с целью уклонения от оплаты налогов и сборов и приём «чёрных» денег, которые не числятся в документах официального характера.

Не менее наболевшим вопросом является сейчас отмывание денег, которое представляет собой легализацию финансовых средств, полученных противозаконным путём. То есть это операции по сокрытию истинного источника дохода и приданию ему вполне законного характера.

В целом, внедрение информационных технологий частично нивелирует отрицательные эффекты хищения денежных средств, а также уклонения от уплаты налогов незаконными способами организаций следующими путями:

1) Технологическое сопровождение электронного денежного перевода с исчерпывающей информацией, находящейся в ведении правоохранительных органов, об отправителе и получателе и номер счёта, что помогает в раскрытии преступлений в сфере экономики и возвращении денежных средств потерпевшим гражданам и организациям.

2) Применение пластиковых кредитных и дебетовых карт, которые реализуют возможность распоряжения собственнымисредствами в пределах суммы на счету, обеспечивают удобство в их использовании, а самое главное – защиту находящихся на

них денежных средств. Это осуществляется с помощью специального электронного замка – скрытого ПИН-кода, а также возможности обращения в службу поддержки и блокирования карты в случае утери.

3) Метод банковского обслуживания – интернет-банкинг, который является технологией дистанционного банковского обслуживания с более удобной формой получения необходимой информации и предоставлением информации по операциям по счетам в любое время.

4) Резервирование как один из наиболее простых способов аппаратной защиты.

Также следует отметить такое новшество в экономике XXI века как электронная коммерция (ЭК), которая представляет собой продажу коммерческими организациями товаров через глобальную сеть Интернет. Быстро и активно развивающаяся ЭК представляет собой непосредственную угрозу финансовым средствам предпринимателей и потребителей, так как осуществляется с помощью кредитно-финансовых форм. Именно поэтому экономическая безопасность неразрывно связана с применением методов по реализации информационной безопасности, ведь именно от неё зависит сохранность информационных ресурсов и финансовых средств от мошенников, а также защита электронных версий документации организации от вирусной атаки.

Для устранения указанных проблем реализуется целый комплекс, который основан на разноплановых технологиях: шифрование – сокрытие данных с помощью кодирования информации, которое обеспечивает неприкасаемость к данным мошенников; stealth-технологии с применением электронных ключей; виртуальные и частные сети; брандмауэры, которые представляют собой аппаратный барьер между двумя сетями и осуществляют защиту корпоративной сети от посягательств на данные [10].

Также следует отметить, что информационные технологии в настоящее время активно применяются в целях защиты бланков ценных бумаг. С использованием определённых технологических методов фирма обеспечивает защиту данных ценных бумаг от несанкционированной выемки информации или их подделки мошенниками.

Так, одним из них является технологический метод защиты бумаг. В её основу входит, во-первых, подложка – использование информационно-технологических методов, задачей которых является создание специальной бумаги при нанесении на неё полиграфического слоя, который отличает ценную бумагу от подделки, а значит, не даёт мошенникам использовать ее в корыстных целях [8].

Во-вторых, актуальным способом защиты стало создание водяного знака на ценной бумаге. Как её отдельный элемент, водяной знак представляет собой рельефную структуру, которая отличается от плотности основы ценной бумаги, которая создаётся вследствие использования высокотехнологического специального оборудования и не даёт мошенникам подделать документы и денежные средства. На таком же принципе основаны и ирисовые плашки, которые, в отличие от водяного знака, имеют меньший размер и расположены на всей площади бумаги.

В-третьих, для защиты ценных бумаг используются защитные нити, защитные волокна, кинеграммы и голограммы и так далее.

Ещё одним из основных способов защиты является использование специальных печатающих устройств, которые также невозможно подделать неподготовленному человеку, а значит и защитить собственную информацию и денежные средства [8].

На сегодняшний день стало популярным заключение электронных сделок, которое позволяет опосредованно решать вопросы между фирмами. Это наиболее удобный способ реализации сделок, однако, и весьма опасный, потому как информационные данные с лёгкостью могут украсть и использовать в своих целях преступники. Однако реализация информационных технологий в этой сфере позволила создать условия защищённости данных.

В этих целях часто применяется усиленная электронная подпись, которую можно сделать с помощью подтверждённых ФСБ специальных криптографических инструментариев и имеет в наличии сертификат от официального удостоверяющего центра. Это обеспечивает снижение вероятности подделки ценной бумаги преступниками.

На сегодняшний день своё развитие находят денежные активы, которые производятся в цифровом виде. Электронные сделки реализуются гораздо проще, к примеру, в случае подписания по ссылке с использованием отправки SMS-уведомлений для идентификации лиц. В этих же целях может применяться биометрическая система, которая создаёт наибольший уровень безопасности для защиты личных данных.

Распространение получили и смарт-сделки, которые подразумевают самостоятельное совершение необходимых действий информационной системы при возникновении определённых случаев. В качестве примера можно использовать простейший автоплатёж, который легко можно настроить в банке или с использованием личного кабинета, который также является нововведением нашего века и позволяет быстро, а главное, безопасно совершать огромный перечень цифровых сделок.

Для полного проникновения в тему применения информационных технологий в сфере совершения сделок, необходимо рассмотреть один из их видов – смарт-контракты. Это специфическая программа для ЭВМ, которая определяет и реализует осуществление обязательств сторон. Стороны определяются с условиями сделки и устанавливают сроки, а также ответственность, которую понесут лица, не выполнившие условия именно в смарт-контракте. Также эта программа самостоятельно решает вопросы относительно правомерности действий участников сделки и реализует исполнение и завершение договора, выдачу финансовых средств, наложение и списание неустоек, блокировку счета и так далее. Это наиболее удобная форма цифрового контроля, которая необходима в том числе для применения в области страхования, продаж в Интернет, поставки и перевозки товаров, сфере исключительных прав и многих других.

Таким образом, угроза в области экономической безопасности продолжает не только нарастать, но и создавать новые современные и более опасные для будущего развития страны и граждан проблемы, что обуславливает острую необходимость выработки разнородной системы мер по реализации благоприятных тенденций в целях создания в нашей стране общества и экономики инновационного типа.

Таковые нововведения с использованием информационных технологий нашли своё применение в различных сферах общественной жизни и продолжают нарастать и совершенствоваться с каждым днём. Разработка и внедрение в жизнь новых технологий уже сдвинула с места уровень защиты данных, удобство в использовании информации и безопасность проведения различных сделок, что не может не отразиться на улучшении положения в экономике всей страны.

Таким образом, информационные технологии оказывают положительное влияние на сферу экономической безопасности, а значит, их необходимо совершенствовать и улучшать в дальнейшем в целях «наведения порядка» в случаях мошенничества в Интернет, хакерских и вирусных атак и др. Для достижения поставленной цели необходимо направить все усилия на преобразование в сфере экономической безопасности, используя при этом модель деятельности, базирующуюся на современных информационных технологиях.

Литература

1. Криворотов В.В. Экономическая безопасность государства и регионов: Учебное пособие для студентов вузов / В.В. Криворотов, А.В. Калина, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2018. - 351 с.

2. Арбатов А.А. Экономическая безопасность России: Общий курс: учебник / В.К. Сенчагов, А.А. Арбатов, А.А. Ведев; под ред. В.К. Сенчагова. - М.: БИНОМ. ЛЗ, 2018. - 118 с.

3. Кузнецова Е.И. Экономическая безопасность и конкурентоспособность. Формирование экономической стратегии государства: Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Е.И. Кузнецова. - М.: ЮНИТИ, 2017. -213 с.

4. Максимов С.Н. Экономическая безопасность России: системно-правовое исследование / С.Н. Максимов. - М.: МПСИ, МОДЭК, 2018. - 56 с.

5. Лбов Г.С., Полякова Г.Л. Информационные технологии в современном бизнесе // Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. – Красноярск, 2017. - Т.31- №5. – 256 с.

6. Демьянова О.В. Информационные технологии // Проблемы современной экономики. – 2018. − №1 (33). –С. 270.

7. Азизкулов Д.М. Цифровая экономика: понятие, особенности и перспективы на российском рынке // Вектор экономики. - 2018. - № 3. - С. 62.

8. Нехайчук Д.В., Нехайчук Ю.С., Будник С.А. к вопросу внедрения электронных средств платежей и электронных денег как современных инновационных банковских технологий // вестник алтайской академии экономики и права. – 2019. – № 3-2. С. 122-128.

9. Информационные технологии в области защиты данных в экономической структуре. // Студопедия: [сайт]. – URL: https://studopedia.ru/18_45195_III-porogovie-znacheniya-indikatorov-ekonomicheskoy-bezopasnosti.html (дата обращения: 04.03.2020.)

10. Прасолов В.И. Цифровая технологии в экономической безопасности как ответ на вызовы XXI века // Экономика и общество: международный научно-практический журнал: [сайт]. – URL: http://www.garant.ru/products/ipo/prime/doc/71452000/ (дата обращения: 10.03.2020).

Сведения об авторах

Акапьев Виктор Львович, кандидат педагогических наук, доцент кафедры информационно-компьютерных технологийв деятельности ОВДБелгородского юридического института МВД России имени И.Д. Путилина; e-mail: akapevvl@yandex.ru.

Прокопенко Алексей Николаевич, кандидат технических наук, доцент,начальник кафедры информационно-компьютерных технологий в деятельности ОВДБелгородского юридического институтаМВД России имени И.Д. Путилина; e-mail: aprokopenko11@mvd.ru.

Савотченко Сергей Евгеньевич,доктор физико-математических наук, доцент,профессор кафедры информационно-компьютерных технологий в деятельности ОВДБелгородского юридического институтаимени И.Д. Путилина; e-mail: savotchenko@hotbox.ru.

Васин Олег Иванович,
Щербаков Виктор Андреевич,
Курочкин Владимир Леонидович,
Курочкин Юрий Владимирович

КВАНТОВЫЕ КАНАЛЫ СВЯЗИ, ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

С помощью одиночных фотонов можно создать связь на сотни и тысячи километров. Характерными особенностями такой связи являютсяквантовые свойства фотонов. Уже существуют примеры построения квантовых информационных сетей как по опто-

волокну, так и по открытому пространству [1]. Наиболее интересными и важнейшими свойствами связи на одиночных фотонах являются возможность генерации и секретного квантового распределения ключа (КРК) между двумя абонентами.

Первая квантовая волоконно-оптическая линия связи (ВОЛС) была длиной 23 км [2]. Не так давно получено успешное КРК на расстояния свыше 300 км с поляризационным [3] и фазовым кодированием фотонов [4]. В настоящее время для ВОЛС преодолен рубеж КРК в 400 км [5, 6]. Сегодня ясно, что методы КРК могут успешно работать для создания квантовых линий связи точка-точка как во внутригородских, так и в ближних междугородних сообщениях.

В двухтысячных годах появились квантовые оптоволоконные сети. В 2002 году в США была построена первая сеть компанией DARPA [7]. В Европе волоконно-оптическая сеть КРК – SECOQC – была построена в Вене [8] и вскоре в Швейцарии [9]. Наиболее развитую квантовую сеть ВОЛС протяженностью более 2000 км недавно создали в Китае [9,10,11]. Эта сеть соединяет несколько городов и содержит 32 узла, соединенных последовательно. В каждом городе построена своя городская сеть КРК, содержащая несколько узлов. Не так давно проведены эксперименты по развитию технологии построения межконтинентальных сетей КРК с помощью спутникового распределения квантового ключа [10 -12].

Большое значение имеет конечная стоимость квантовых ВОЛС. Возможным путём решения этой проблемы может быть использование переключателей для увеличения длины линии при неизменном количестве квантовых приемников и передатчиков [13] или для увеличения количества потребителей внутри города [1,9].

В данной статье анализируется физика и техника квантовых каналов связи, квантовое распределение ключей, техника передачи информации с помощью «меченых поляризацией» одиночных фотонов, дан сравнительный анализ результатов КРК производителями разных стран.

Метод шифрования одноразовым случайным ключом был математически точно обоснован Шенноном. Он показал, что секретный ключ является действительно случайным, если он применяется только один раз, а длина ключа равна длине сообщения. В этом случае будет достигнут предел теоретической стойкости криптосистемы [14]. Идея «одноразового шифр-блокнота» была сформулирована Гилбертом Вернамом в 1917 году [14,15], а структура разработанного им шифра успешно используется до сих пор.

Квантоваякриптографияявляетсяоднимиз перспективных направлений развития телекоммуникационных систем. Она может обеспечить криптографическуютеоретическую стойкость передачи данных на основе однофотонных «меченых поляризацией» квантовых сигналов [16,17,18]. Это дает возможность применять ее методы на практике при передаче данных по оптоволокну или через атмосферу.

Невозможность перехвата поляризованного фотона потенциальным шпионом обусловлена фундаментальными законами квантовой физики (а именно принципом неопределенности Гейзенберга, который запрещает клонирование произвольных квантовых состояний). Это дает преимущество перед методами криптографии, которые основаны на математических функциях и в принципе могут быть расшифрованы. Законы квантовой механики запрещают создание физического устройства, которое способно копировать произвольное квантовое состояние фотона.

Абсолютно секретный канал связи предлагает квантовая физика. Его можно использовать для синтеза и передачи секретных ключей и секретных сообщений.

Есливкачестве битовкодавыступают квантовые состояния одиночных частиц,топрипопыткеперехвата, исходные сигналы разрушаются, что приводит кповышению уровня ошибоквканале связи. Это дает возможность обнаружить нелегитимного пользователя (подслушивателя). Результатом обнаружения перехвата является прекра-

щение передачи фотонов. Для выявления возможного перехвата заключается определенное соглашение (протокол) между «Отправителем» и «Получателем» информации [16-18].

Протокол квантовой криптографии BB-84.

Первый квантовый протокол был предложен для кодирования поляризационныхсостоянийфотоноввдвухальтернативных базисах [19]. На рисунке 1 дана схема кодирования поляризационных состояний одиночных фотонов по протоколу BB-84.

Для случайности кода Отправитель и Получательслучайноменяютзначение разряда и тип поляризатора (т.е. кодировку разряда). Принципиальной особенностью квантового распределения (генерации и передачи) секретных ключей является генерация этих ключей непосредственно в процессе сеанса связи по квантовому каналу с обязательным участием «Отправителя» и «Получателя» информации. Причем в процессе генерации симметричного ключа осуществляется непрерывный контроль несанкционированного доступа.

• Предварительно Отправитель и Получатель приписывают цифровое значение фотонам, например: фотоны с поляризацией 0° и 45° кодируют число 0, а фотоны с поляризацией 90° и 135° - единицу.  и  .

•Сеанс передачи ведется в однофотонном режиме и производится подсчет фотонов.

•Отправитель*случайным образом выбирает значение разряда: 0 или 1*.

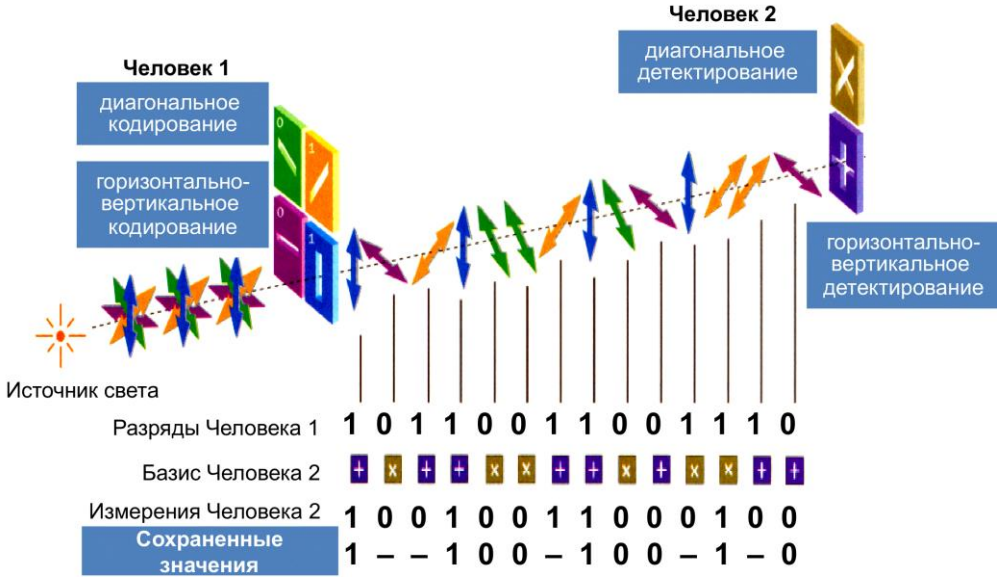


Рис. 1. Принцип кодирования поляризационных состояний одиночных фотонов.

• Отправитель случайно выбирает базис кодирования - (вертикально - горизонтальный или диагональный базис (способ)):  и  .

•Отправитель отправляет Получателю закодированный таким образом фотон.

• Получатель измеряет полученный фотон с помощью поляризационного светоделителя, *случайным образом настроенного* на вертикально-горизонтальное или диагональное кодирование.

• *Получатель получит верное значение только в том случае, если случайно использует ту же схему кодирования, что и Отправитель.*

• После передачи большого числа разрядов Отправитель и Получатель обмениваются *схемами* кодирования каждого разряда (это возможно по открытому каналу, а реально в автоматическом режиме). Так как *передача происходила на одиночных фото-*

нах, потенциальный перехватчик не может иметь полной информации о состояниях их поляризации.

• Отправитель и Получатель исключают из последовательности битов те случаи, в которых при регистрации фотона использовались разные схемы (базисы) кодирования.

• После этого у Отправителя и Получателя остаются идентичные, секретные последовательности разрядов, то есть одноразовый симметричный код (ключ).

Что произойдет в случае попытки перехвата?

• Перехватчик не знает базиса кодирования отправителя (горизонтально-вертикальный или диагональный) одиночного фотона.

• Перехватчик может детектировать, а затем генерировать и пересылать фотоны только в случайном базисе с вероятностью 50%, при этом его знания о состоянии конкретного фотона будут неполными, так как для полного измерения нужна серия экспериментов.

• Между секретными ключами отправителя и адресата возникнут расхождения.

• Перехват будет обнаружен и будет установленапопытканарушениясекретности [9,17,18].

Рис. 2. Общий вид квантовокриптографической системы связи по оптоволокну

На рис. 2 показана первая в России установка квантовой криптографии, разработанная авторами данной статьи вг. НовосибирскевИнститутефизикиполупроводников им. академика А. В. Ржанова Сибирского отделения РАН [18].

Схема экспериментальной установки представлена на рисунках 3 и 4 [20].

В эксперименте авторов генерация квантового ключа осуществлялась следующим образом [20]. Отправителем применялся программный генератор случайных чисел. Тактовая частота повторения лазерных импульсов задавалась компьютером передающего узла (рис. 3). Каждый такт сопровождался синхроимпульсом (стробом), который синхронизировал передачу-прием и посылался Получателю. Другойимпульс подавался одновременно со стробом случайным образом на один из четырех лазеров (2) Отправителя, который генерировал световой импульс длительностью 8-10 нс. Использовались полупроводниковые микрохолодильникинаоснове элементов Пельтье для термостабилизации лазеров(3).

В данной крипт-системе получена скорость генерация квантового ключа ~0,5

кбит/с. Передача данных велась в инфракрасном диапазоне оптического спектра на длине волны 1550 нм [21].Уровень ошибок в ключе не превышал 3.7%. Теоретически допустимый уровень ошибок 11%, (т.е.полученный результат) является удовлетворительным для экспериментальнойгенерациикключа.

После получения синхроимпульса получатель вырабатывет, собственный строб-импульс длительностью 20 нс (рис. 4) [20]. Во время подачи строба регистрируются импульсы с выходов фотоприемников (4). Это позволяет избавиться от большей части темновых шумов фотоприемников. Импульсы на выходе фотодетектора считались информационными только при временном совпадении с лазерными синхроимпульсами передатчика. Компьютером считывались данные с четырех фотодетекторовПолучателяпо синхроимпульсу Отправителя.

Есливтечениестроб-импульса приходил импульс с какого-либо детектора Получателя, то Получатель запоминал для него номер тактового импульса и вырабатывал и посылал сигнальный импульсОтправителю, по которому Отправитель также запоминал номер своего синхроимпульса и номер лазера, который излучал в этом такте.

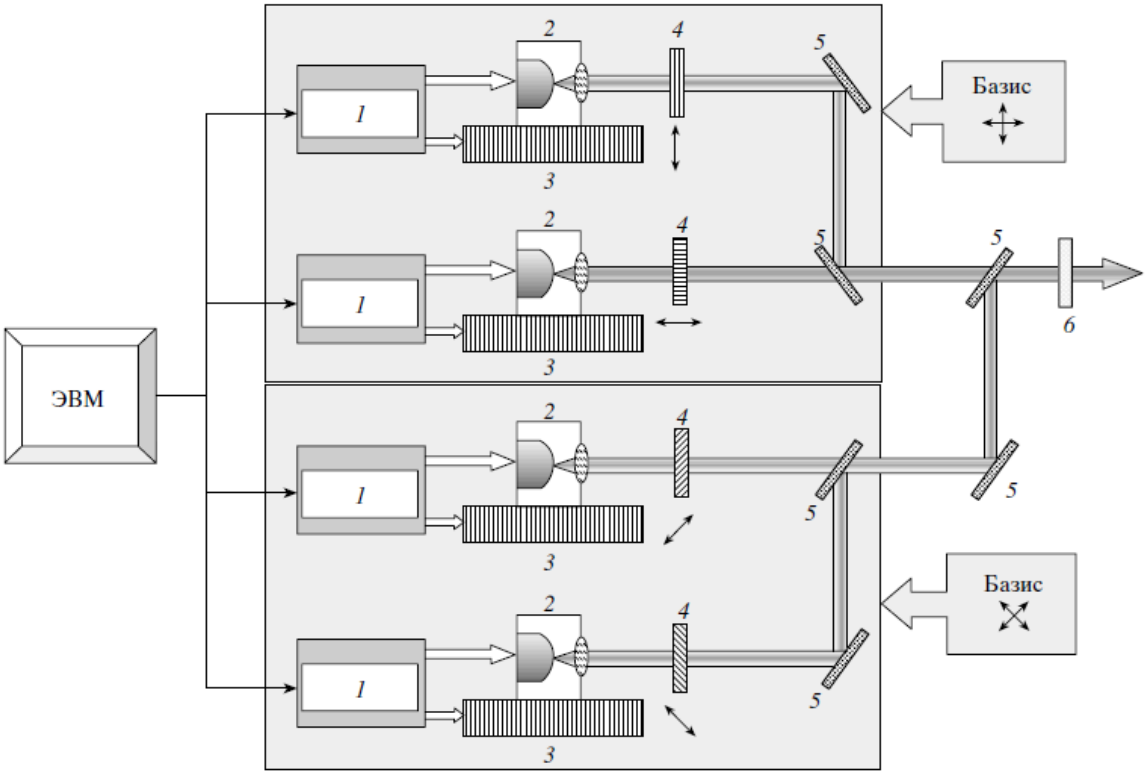


Рис. 3 – Схема передающего узла[20]: (1) источники тока полупроводниковых лазеров, управляемые от компьютера; (2) полупроводниковые лазеры; (3) микрохолодильники; (4) поляризаторы (призмы Глана); (5) зеркала; (6) поглощающий фильтр

Поскольку среднее число фотонов в световом импульсе было много меньше единицы, то запоминать всю передачу не было необходимости.

Если базисы Отправителя и Получателя совпадали, то результатам измерений присваивался очередной порядковый номер, и они добавлялись к генерируемому ключу. В противном случае данные не учитывались. В соответствии с протоколом BB-84, по окончании процедуры у Отправителя и Получателя генерировался согласованный случайный секретный ключ требуемой длины [20].

Внастоящеевремяавторыэтойразработки (и данной статьи) Курочкин В.Л. и Курочкин Ю.В. успешно продолжают исследования в Российском квантовом центре (РКЦ) (Москва-Сколково).

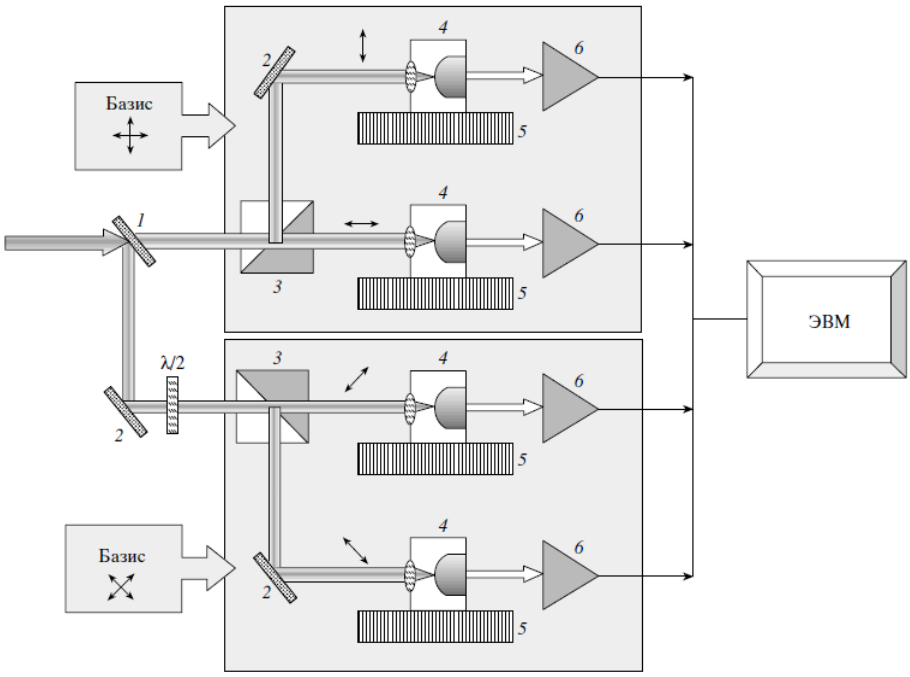


Рис. 4 – Схема приемного узла: (1) полупрозрачное светоделительное зеркало; (2) зеркала; (3) поляризационные разделительные призмы Глана; (4) лавинные фотодиоды с собирающими линзами; (5) микрохолодильники; (6) усилители с активным гашением лавины; (λ/2) полуволновая пластинка

Установки с поляризационным кодированием можно с успехом использовать для передачи информации в открытом пространстве. В выше упомянутом Институте физики полупроводников СО РАН для выполнения демонстрационных экспериментов по генерации квантового ключа в атмосферной линии связи была создана квантово-криптографическая система, позволяющая осуществить поляризационное кодирование состояний одиночных фотонов по протоколу BB84. Установка на основе модернизированной оптической схемы с телескопическим расширением лазерного пучка представлена на рис. 5 [18].

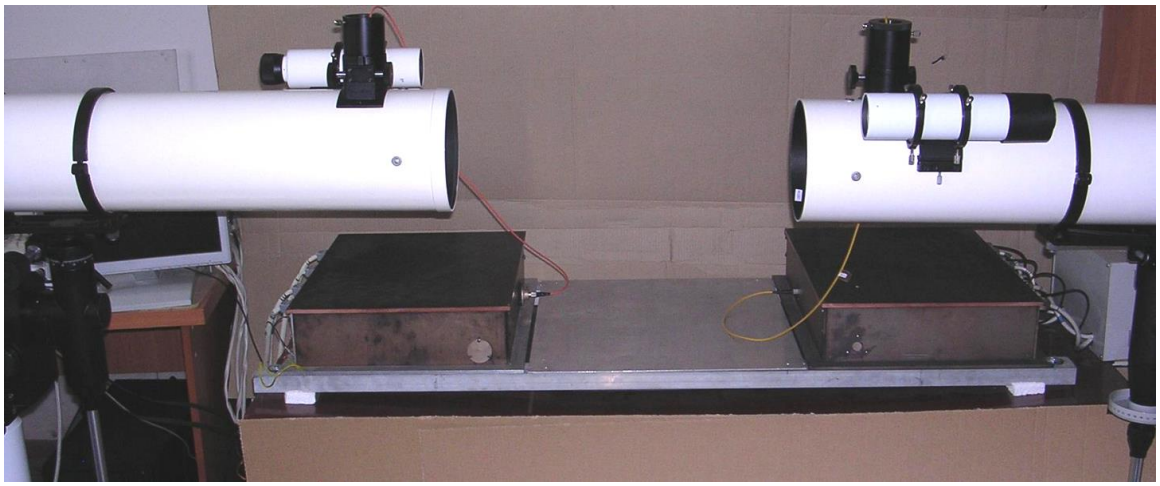


Рис. 5. Установкадля квантовой криптографии на дальние расстояния.

Для практических применений важносуществование так называемых оптических окон прозрачности атмосферы (рис. 6), внутри которых поглощение фотонов является очень слабым [27]. Вертикальная оптическая плотность атмосферы от Земли до космоса эквивалентна расстоянию ~ 8 км на уровне моря при нормальных условиях.

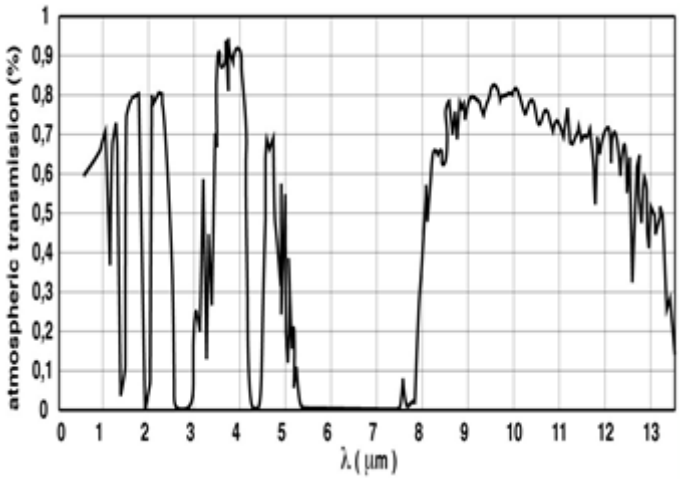


Рис. 6.Спектр пропускания атмосферы [27].
Видимыйдиапазон соответствуетλ = 0,39-0,77 мкм.

Затухание в спутниковом квантовом канале связи по теоретическим оценкам составляет не менее 50 дБ [22,23]. Экспериментальные работы подтверждают эту величину [24,25]. Затухание,соответствующее спутниковому каналу связи, было смоделировано нами в работе [26], гдеосуществлено распределениеквантового ключа в оптическом волокне длиной 302 км. При длине 302 км общее затухание составило 50,2 дБ. Для понижения шумов использовались сверхпроводящие детекторы фотонов, охлажденные до температуры ~2,2º К.

В 2008 г. был проведен первый эксперимент по регистрации отраженного от спутника Земли однофотонного лазерного сигнала, посланного с наземной станции рис. 7 [28].Движение спутника позволяет совершить генерацию ключа и обмен секретным ключом между любыми точками на Земле и другими спутниками, которые видны с его орбиты.

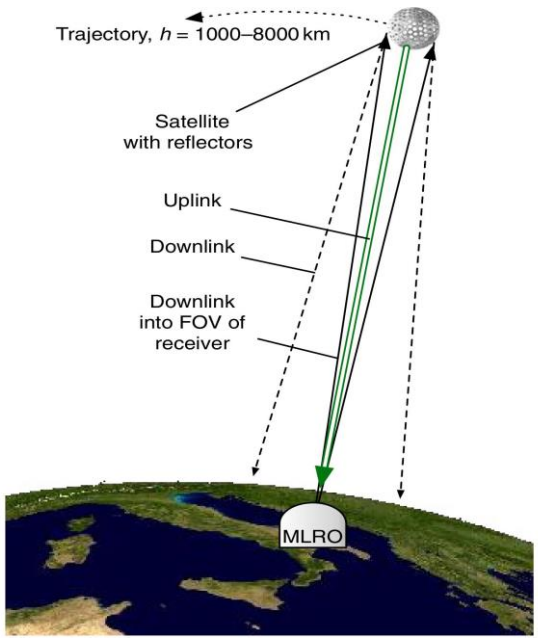


Рис. 7 Схема передачи-приема однофотонного сигнала через спутниковый канал связи.

Коммерческие продукты квантовой криптографии

В настоящее время основными игроками рынка коммерческих квантовых систем являются компании: idQuantique (Швейцария), MAGIQ (США),SeQureNet(Франция)иQRATE(Россия-РКЦ).

Рис. 8. Квантовые коммуникации компании«QRATE» (содержит передатчик сгенератором фотонов и приемник)

Российский квантовыйцентр [29,30]: устанавливает квантовый канал генерации и передачи симметричныхключейнастандартном оптоволокне(рабочаядлинаволны излучения лазера 1,55 мкм);

• Передает случайную последовательностьна два разнесенных сайта;

• Позволяет генерироватьираспределять ключи на расстоянии до 100 км со скоростью более 10 Кб/с;

• Интегрируетсясиспользуемыми устройствами шифрования;

• Прошлоиспытанияу клиентовилегловосновустроящихся квантовых сетей.

Таблица 1

Сравнение основных продуктов квантового распределения ключа

Устройство	Страна	Скорость генерации ключа по данным производителя	Предельная дальность
Clavis2,idQuantique	Швейцария	0,5 Кбит/с	100 км
Q-Box,MAGIQ	США	1Кбит/с	140 км
Cygnus,SeQureNet	Франция	0,1 Кбит/с	80 км
QRATE	Россия (РКЦ)	10 Кбит/с	100 км
QuantumCTek	Китай		7600 км

Можно выделить следующие области применения данных продуктов:

- государственные структуры;
- оборонные ведомства;
- банковские, финансовые и промышленные учреждения.

Результаты внедренияпромышленного устройства квантового распределения ключа QRATE Российского производства

(разработано авторами настоящей статьи из Российского квантового центра (РКЦ) – компания «QRATE»):

• Декабрь 2017 – Первая в России линия квантовой связи. Forbes СБЕРБАНК - Компания «Сбербанк» провела квантовую линию связи между офисами.В России впервые переданы 29.12.2017 банковские данные по линии, которая абсолютно защищена от подключения злоумышленников с помощью квантовых технологий. Тесты провели специалисты Российского квантового центра и компании «Forbes».

• Май 2018 – Первая в России линия скоростной квантовой связи с высокой пропускнойспособностью успешно прошла испытания 23.05.2018 на телеканале «ВЕСТИ.RU». Тесты провели специалисты Российского квантового центра и компании "С-Терра СиЭсПи».

• Декабрь 2018 – январь 2019 – испытание отечественной квантовой системы QRATE для передачи защищенных данных по волоконно-оптической линии связи (ВОЛС) провел «Ростелеком». В демонстрации были задейчтвованы Российский квантовый центр (РКЦ), компании «QRATE» и «С-Терра СиЭсПи».

• В настоящее время в мире функционирует несколько многоузловых квантовых сетей:

Восьми узловая сеть точка-точка работает в Австрии и соединяет между собой следующие организации: idQuantique (3 устройства), ToshibaResearch, GAPOptique, UniversityofVienna, CentreNationaldelaRechercheScientifique, Ludwig Maximillians University. Среднее расстояние между узлами 25 км, скорость 10 кбит/с.

В Японии по средствам сети TokyoQKDnetwork реализована передача видеосигнала, закодированного с помощью квантового ключа. Данная сеть включает в себя 6 узлов, среднее расстояние между которыми 45 км.

Крупнейшая в мире квантовая криптографическая ВОЛС, называемая DARPA, находится в США. Состоит из 10 узлов расстояние между которыми доходит до 55 км (среднее 35 км).

Система SwissQuantum используется в пятерке крупнейших банков Швейцарии, среднее расстояние между узлами 12 км [31].

Недостатки квантовой криптографии

Для увеличения длины оптоволоконной линии связи в квантово-криптографических системах из-за невозможности применения усилителей, необходимо использовать станции перешифрования (узлы) через 50 - 150 км. Например, квантовая ВОЛС, которая возможно уже построена в КНРна расстояние 2000 км имеет 32 станции перешифрования [9].

На рис. 9 показана зависимость скорости передачи фотонов от расстояния. Видно, что скорость передачи фотонов по оптоволокну на расстоянии всего около 85 км уменьшается почти в 10^5 раз!

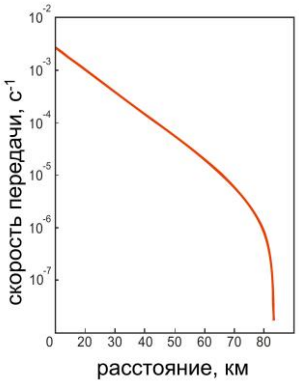


Рис. 9. Зависимость от расстояния скорости передачи поляризованных фотонов по оптоволокну.

Станция перешифрования – это техническое устройство, которое компенсирует затухание фотонов в квантовой линии связи. На этой станции шифровка вскрывается, т.е. рассекречивается, затем информация шифруется новым ключом и отправляется на следующую станцию перешифрования [9]. Таким образом, секретная информация передаваемая по ВОЛС в КНР [9] на расстоянии 2000 км 32 раза подвергается вероятности перехвата.

1. Реальная квантовая криптографическая система требует создания механизма активной компенсации поляризационных изменений состояния фотонов при их распространении в среде. В оптоволоконной транспортной среде – это серьезная проблема. Без управления поляризацией в квантово-криптографических системах с фазовым ко-

дированием 50% фотонов не будет нести никакой информации.

3. Для передачи фотоновсквозь атмосферу на спутник при организации квантового канала связи требуется решить ряд задач:

• Во-первых, необходимо увеличить суммарную квантовую эффективность регистрации фотонов при передачи их с околоземной орбиты.

• Во-вторых, необходимо разработать промышленную аппаратуру для спутниковых квантовых каналов связи.

Необходимость применения станций перешифрования тормозит развитие построения оптоволоконных квантовых линий связи длиной в тысячу и более километров. Это обусловлено высокой стоимостью таких станций, дорогостоящей их эксплуатацией и большим затуханием однофотонного квантового сигнала.

Несмотря на недостатки и высокую цену, две крупнейшие державы строят квантовые оптоволоконные линии связи протяженностью в тысячи км: КНР – 2000 км – цена около 100 млн. $ [9]. В США возможно уже построеныоптоволоконные линии связи протяженностью 650 км и 10000 км [32].

В последние годы значительные успехи по передаче квантовой информациисо спутников на Землю и обратно достигнуты в КНР [33,34]. В [33] осуществлено квантовое распределение секретного ключа с орбиты спутника высотой 1200 км на Землю. Затухание интенсивности фотона оказалось меньше – 50 дБ. В 2018 году[34] осуществлена квантово-криптографическая связь на расстояние 7600 км между двумя наземными станциями из Китая в Европу через спутник на орбите.

Литература

1. Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Large scale quantum key distribution: challenges and solutions // Optics Express.– 2018 – , V. 26, № 18, P. 24260-24273) •https://doi.org/10.1364/OE.26.024260.

2. Ribordy, G., J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, “Fast and user-friendly quantum key distribution” // J. Modern Opt.–2000 – , V. 47, P.517-531.

3. Ozhegov R. Elezov M.,Kurochkin Y., Kurochkin V., et al, Quantum key distribution over 300 km // Proc. SPIE – 2014 – 9440, 94401F.

4. Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu et al, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber// Phys. Rev. Lett. – 2016 – V. 117, 190501.

5. Alberto Boaron, Gianluca Boso, Davide Rusca et al, Secure Quantum Key Distribution over 421 km of Optical Fiber// Phys. Rev. Lett. – 2018 – V. 121, 190502.

6. Elliott C. Building the quantum network, //New Journal of Physics. – 2002 – ,V. 4,№ 1,P. 46.

7. Poppe A., Peev M., Maurhart O.Outline of the SECOQC quantum-key-distribution network in Vienna // International Journal of Quantum Information. – 2008. – V. 6, № 02,p. 209–218.

8. Stucki D., Legré M., Buntschu F.,[et al.] Long-term performance of the Swiss quantum key distribution network in a field environment // New Journal of Physics. –2011. – V. 13, № 12, P. 123001.

9. Qiu J., “Quantum communications leap out of the lab// Nature – 2014. – V. 508 (7497), p. 441–442.

10. Liao S. K., Cai W. Q., Liu W. Y., [et al.]Satellite-to-ground quantum key distribution// Nature. –2017. – V. 549, № 7670, p. 43–47.

11.Yin J ., Cao Y., Li Y. H., [et al.]Satellite-to-ground entanglement-based quantum key distribution // Physical review letters. – 2017. – V. 119. – № 20, P. 200501.

12. Liao S.-K., Cai W.-Q., Handsteiner J., [et al.] “Satellite-relayed intercontinental quantum network, // Phys. Rev. Lett. –2018 – V. 120, № 3, 030501.

13. Duplinskiy A., Fat'yanov O., Pavlov I., [et al.]Switch-based quantum network for the cost reduction of QKD. QCrypt 2019 Int/ Conference on Quantum cryptography, Montreal, Canada, 26–30 August 2019http://2019.qcrypt.net/poster-session-wednesday-28-august-2019/.

14. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ 1963 – 830 с.

15. Шнаер Б. Прикладная криптография. – М.: ТРИУМФ, 2003. – 816 с.

16. Нильсен М.А., Чанг И. Квантовые вычисления и квантовая информация. – М.: Мир, 2006.

17. Холево А.С., Квантовая теория информации. Каналы и пропускные способности // Информационные технологии и вычислительные системы – 2010.– № 3, С. 39–46.

18. Рябцев, И.И. Экспериментальная квантовая информатикасодиночными атомами и фотонами / И.И. Рябцев,И.И. Бетеров,Д.Б. Третьяков, В.М. Энтин, Е.А. Якшина, В.Л. Курочкин, А.В. Зверев, Ю.В. Курочкин, И.Г.Неизвестный // Юбилейный сборник избранных трудов Института физики полупроводников им. А.В.Ржанова СО РАН. / отв. ред. А.В. Латышев, А.В. Двуреченский, А.Л. Асеев – Новосибирск:Параллель, 2014. – С. 657-678.

19. Bennet C.H., Brassard G**.** Quantum cryptography: public key distribution and cointossing// Proc. of IEEE Inter. Conf. on Comput.Sysems and Signal Processing – December 1984. –Bangalore, India, V. 1, P.175-179.

20. КурочкинВ. Л., РябцевИ.И., НеизвестныйИ.Г. Квантоваякриптографияигенерацияквантовогоключасиспользованиемодиночныхфотонов//Микроэлектроника.– 2006. – Т. 35, № 1, С. 41-47.

21. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography// Rev. Mod. Phys. – 2002. – V. 74, P. 145 – 175.

22. Rarity J.G., Tapster P.M., Gorman P.M.,Knight P.Ground to Satellite Secure Key Exchange Using Quantum Cryptography// New J. Physics. – 2002. -V. 4. -P. 82.1-82.21.

23.Erven C., Heim B., Meyer-Scott E. et al.Studying free-space transmission statistics and improving free-space quantum key distributionin theturbulent atmosphere//New J. Physics. –2012. –V. 14. –P. 123018.

24.Juan Yin, Yuan Cao, Shu-Bin Liu, et al. Experimental quasi-single-photon transmission from satellite to earth // Optics Express. – 2013. –V. 21, Issue 17. – P. 20032-20040.

25.Giuseppe Vallone G., Bacco D., Dequal D. et al.ExperimentalSatelliteQuantum Communications // arXiv – 2014. – V. 1, – P. 1406.4051.

26.Курочкин В.Л.,Курочкин Ю.В., Белый А.Ф., Васин О.И., Мирошниченко Е.Л. Спутниковая квантовая криптография. // Сб. трудов X-XI Всерос. НТК, г. Геленджик 2015«Информационная безопасность - актуальная проблема современности» / отв. ред. д.т.н., проф. А.В.Крупенин. –Краснодар: КВВУ, 2015. –С.270 – 272.

27.Фотоника: Словарь терминов / Ковалевская Т.Е., Овсюк В.Н., Белоконев В.М., Дегтярев Е.В.;Под ред.ОвсюкаВ.Н. – Новосибирск: ИздательствоСОРАН, 2004. – 342 с.

28. Villoresi P., Jennewein T., Tamburini F., Aspelmeyer M., Bonato C.,UrsinR.,Pernechele C., Luceri V., Bianco G., Zeilinger A., and Barbieri C. Experimental verification of the feasibility of a quantum channel between space and earth// New J. Phys. – 2008. – V. 10. – P. 033038. (http://www.njp.org/).

29. Киктенко Е.О.,Пожар Н.О.,Дуплинский А.В.,Канапин А.А.,Соколов А.С., Воробей С.С., Миллера А.В., Устимчик В.Е.,Ануфриев М.Н.,Трушечкин А.С., ЮнусовР.Р.,Курочкин В.Л.,Курочкин Ю.В.,Федоров А.К. Демонстрация сети квантового распределения ключа в городских оптоволоконных линиях связи // Квантовая электроника. – 2017 – Т. 47, № 9, С. 798 – 802.

30. Duplinskiy A.V.,Kiktenko E.O.,Pozhar N.O.,Anufriev M.N.,Ermakov R.P.,Kotov A.I., Brodskiy A.V.,Yunusov R.R., Kurochkin V.L., Fedorov A.K., Kurochkin Y.V. Quan-

tum-secured data transmission in urban fibre-optic communications lines // Journal of Russian Laser Research. – 2018. – V. 39, Issue 2. – P. 113 – 119. (http://link.springer.com/article./10.1007/s10946-018-9697-1).

31. Peev M.,Pacher C.,Alleaume R.//NewJournalofPhysics – 2009. – V. 11, P. 075001.

32. Nature.– 2012 – V. 492, P. 22.

33. Liao S.-K., et al. Satellite-to-ground quantum key distribution // Nature. – 2017. –V. 549, p. 43 – 59.

34. Liao S.-K., et al.Satellite-relayedintercontinentalquantumnetwork//Phys.Rev.Lett– 2018.–V. 10,–P.120.030501.https://www.researchgate.net/publication/322517705).

Сведения об авторах

Васин Олег Иванович, кандидат физико-математических наук, старший научный сотрудник НИЦ Краснодарского высшего военного орденов Жукова и Октябрьской революции Краснознаменного училища имени генерала армии С.М.Штеменко; e-mail: ovassin@mail.ru.

Щербаков Виктор Андреевич,кандидат технических наук, старший научный сотрудник НИЦ Краснодарского высшего военного орденов Жукова и Октябрьской революции Краснознаменного училища имени генерала армии С.М.Штеменко; e-mail:sherbakov_viktor@list.ru.

Курочкин Владимир Леонидович, гандидат физико-математических наук, доцент, главный исследователь Российского квантового центра (Москва-Сколково); e-mail: v.l.kurochkin@gmail.com.

Курочкин Юрий Владимирович,кандидат физико-математических наук, руководитель группы квантовых коммуникаций Российского квантового центра; e-mail: yk@rqc.ru.

Гавришев Алексей Андреевич

ПРИМЕНЕНИЕ ПАКЕТА ПРОГРАММ SCICOSLAB ДЛЯ МОДЕЛИРОВАНИЯ СИСТЕМЫ СВЯЗИ С ППРЧ

Из литературы известно [3, 6, 7], что в настоящее время одной из самых распространенных систем связи является система связи с псевдослучайнойперестройкой рабочей частоты (ППРЧ). Упрощенная структурная схема системы связи с ППРЧ приведена на рис. 1 [3, 6]. На рис. 1 изображены передающая часть, состоящаяиз кодера данных, модулятора, генератора псевдослучайной последовательности (ПСП), синтезатора частоты, микшера и приемная часть, состоящая из микшера, синтезатора частоты, генератора ПСП, блока синхронизации, демодулятора, декодера данных.

Рис. 1. Упрощенная структурная схема системы связи с ППРЧ

На передающей и приемной сторонах используются одинаковые генераторы ПСП, которые позволяют, как расширить спектр передаваемого сообщения, так и сжать его в приемной части.

В данной работе авторы хотят провести моделирование системы связи с ППРЧ в пакете программ ScicosLab и исследование полученных данных с помощью известных методов нелинейной динамики.

Целью данной статьи является анализ применения пакета программ ScicosLab для моделирования системы связи с ППРЧ.

В пакете программ ScicosLab, в соответствии с рис. 1, авторами построена модель системы связи с ППРЧ, представленная на рис. 2. При построении данной модели системы связи с ППРЧ авторы опирались на результаты, приведенные в работах [3, 6].

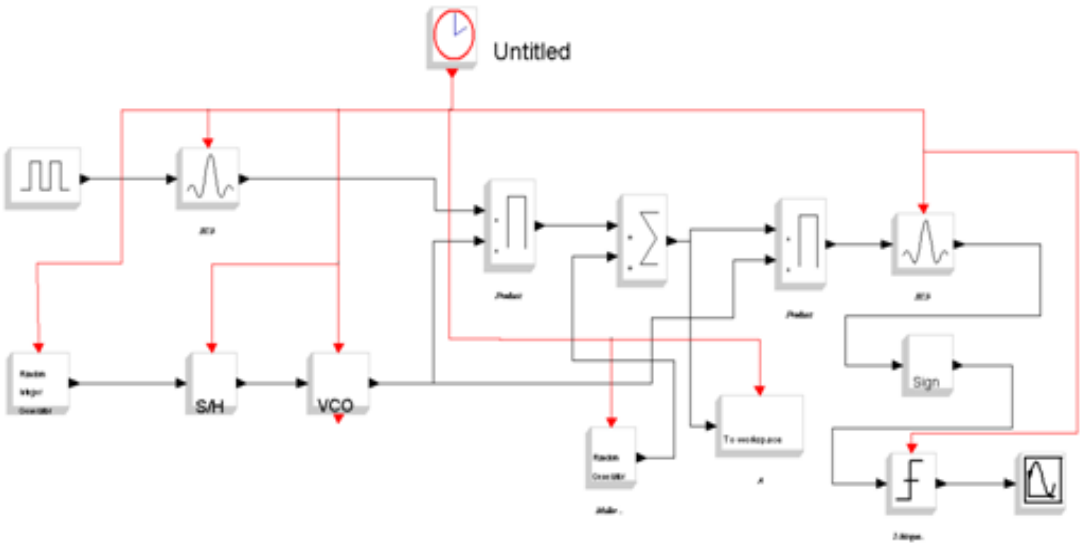


Рис. 2. Модель системы связи с ППРЧ, построенная в пакете программ ScicosLab

Проведеманализ полученных при моделировании данных с помощью известных методов нелинейной динамики [4, 5]. К таким методам отнесем: временные диаграммы, спектральные диаграммы, автокорреляционную функцию, BDS-статистикуw(ε).

Пример полученной временной диаграммы передаваемых сигналов приведен на рис. 3. Временная диаграмма построена с помощью программы PAST.

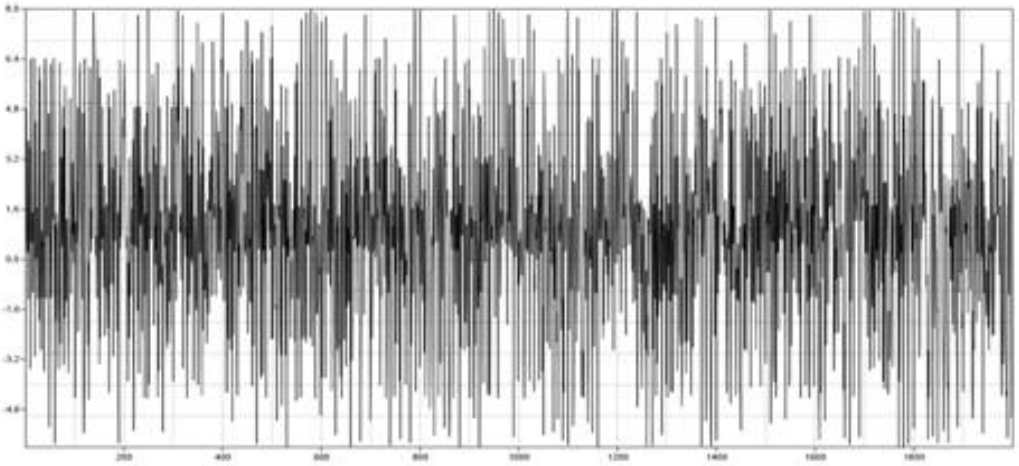


Рис. 3. Пример полученной временной диаграммы передаваемых сигналов

Пример спектральной диаграммы, соответствующей передаваемому сигналу с рис. 3, изображен на рис. 4. Спектральная диаграмма построена с помощью программы PAST.

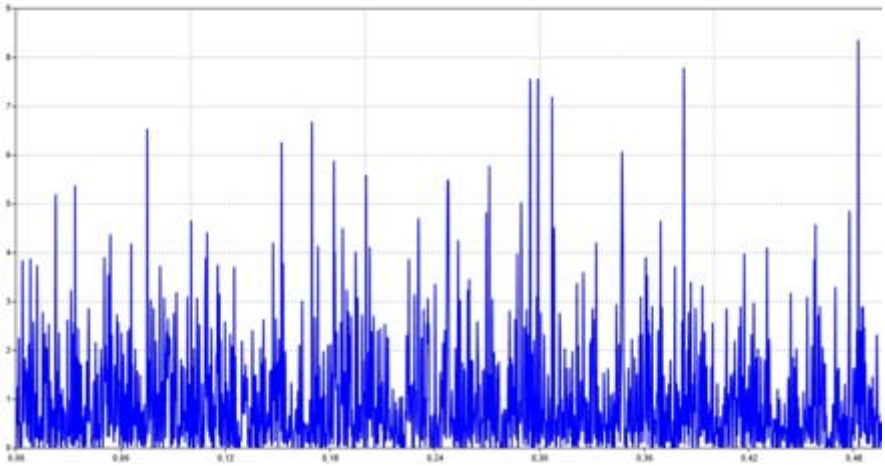


Рис. 4. Пример полученной спектральной диаграммы передаваемых сигналов

Пример автокорреляционной функции, соответствующей передаваемому сигналу с рис. 3, изображен на рис. 5. Автокорреляционная функция построена с помощью программы PAST.

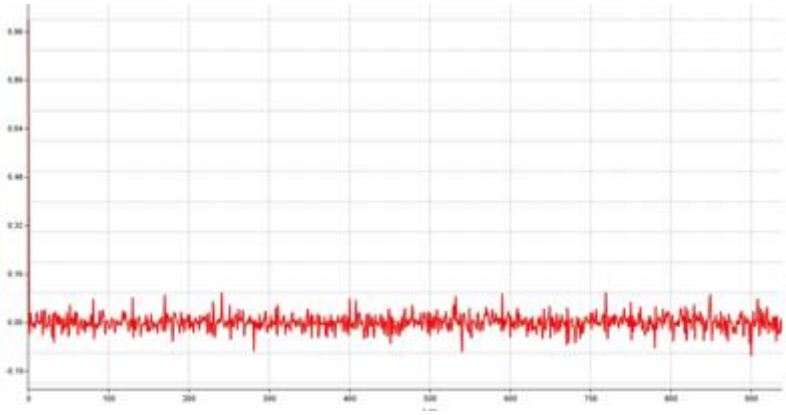


Рис. 5. Пример полученной автокорреляционной функции передаваемых сигналов

Как видно из рис. 3 – 5, передаваемые сигналы системы связи с ППРЧ схожи с сигналами шума.Кроме того, их автокорреляционная функция имеет быстроспадающий вид, что так же указывает на то, что исследуемые сигналы схожи с сигналами шума.

Рассмотрим количественные оценки передаваемых сигналов, полученных с помощью разработанной модели. В качестве количественной оценки обратимся к понятию BDS-статистики $w(\varepsilon)$, которая является аналогом энергетической скрытности [1, 4]. Значения BDS-статистики $w(\varepsilon)$ получены с помощью программы EviewsStudentVersionLite. Полученные значения приведены в таблице 1.

Таблица 1.

Полученные значения BDS-статистики $w(\varepsilon)$ для передаваемых сигналов

№	Длина передаваемых сигналов	Значение BDS-статистики $w(\varepsilon)$
1	1000	≈17
2	2000	≈20
3	5000	≈36

Как видно из таблицы 1, для передаваемых сигналов значение BDS-статистики находится примерно в диапазоне $w(\varepsilon)\in[17\div36]$. Проведем сравнение полученных результатов с известными исследованиями из данной предметной области. В соответствии с работами [1, 2, 4, 5] известно, что значения BDS-статистики $w(\varepsilon)$для известных подходов формирования широкополосных сигналов и их производных (например, фазоманипулированные сигналы; система связи с прямым расширением спектра, исполь-

зующая в качестве ПСП m-последовательности; регистр сдвига с линейной обратной связью и некоторые другие) находятся около значений $w(\varepsilon)\approx 40$.

Таким образом, в данной статье авторами проведено моделирование системы связи с ППРЧ в пакете программ ScicosLab и исследование полученных данных с помощью известных методов нелинейной динамики. В результате проведенных исследований установлено, что сигналы, генерируемые системой связи с ППРЧ, имеют вид, схожий с сигналами шума. Кроме того, их автокорреляционная функция имеет быстроспадающий вид, что так же указывает на то, что исследуемые сигналы схожи с сигналами шума. Вместе с тем, количественные расчеты показали, что значения BDS-статистики сигналов, генерируемых системой связи с ППРЧ, находятся примерно в диапазоне $w(\varepsilon)\in[17\div 36]$. В соответствии с известными исследованиями из данной предметной области [1, 2, 4, 5], это указывает на то, что система связи с ППРЧотносится к системам связи, основанным на известных подходах формирования широкополосных сигналов и их производных. На основании полученных данных можно заключить, что пакет программ ScicosLabявляется подходящим инструментом для моделирования различных систем связи, в том числе и системы связи с ППРЧ.

Литература

1. Альтман Е.А., Малютин А.Г., Чижма С.Н. Повышение скрытности шумоподобных сигналов в системах радиосвязи // Сборник докладов II Международной научно-технической конференции «Радиотехника, электроника и связь («РЭИС-2013»). Омск: ОАО «ОНИИП». 2013. С. 329–337.

2.Бодягин И.А., Дернакова О.В. Статистический анализ частично наблюдаемых выходных последовательностей криптографических генераторов с использованием модели DAR(p) // Веснік сувязі. 2018. № 1(147). С. 51–55.

3.Бояршинов М.А., Зыкин А.А. Методика моделирования радиолинии, использующейсигналы с ППРЧ в условиях воздействия преднамеренных помех // Приборостроение в XXI веке – 2017. Интеграция науки, образования и производства [Электронный ресурс]: сб. материалов XIII Междунар. науч.-техн. конф. (Ижевск, 22–24 нояб. 2017 г.). – Ижевск: Изд-во ИжГТУ имени М. Т. Калашникова, 2018. С. 525-532.

4. Васюта К.С. Классификация процессов в инфокоммуникационных радиотехнических системах с применением BDS-статистики // Проблемы телекоммуникаций. 2012. № 4(90). С. 63-71.

5. Гавришев А.А. Моделирование и количественно-качественный анализ распространенных защищенных систем связи // Прикладная информатика. 2018. Т. 13. № 5 (77). С. 84-122.

6. Кокорева Е.В., Белезекова А.С. Теоретические основы современных технологий беспроводной связи: методические указания к лабораторной работе. Томск: Факультет дистанционного обучения, ТУСУР, 2014.81 с.

7. Макаренко С.И., Иванов М.С., Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография.СПб.: Свое издательство, 2013.166 с.

Сведения об авторе

Гавришев Алексей Андреевич,старший преподавательСеверо-Кавказского федерального университета; e-mail: alexxx.2008@inbox.ru.

Генк Алексей Владимирович

О ПРИМЕНЕНИИ СИСТЕМ КОМПЬЮТЕРНОЙ АЛГЕБРЫ ВКУРСАХВЫСШЕЙ МАТЕМАТИКИ

В последние 15-20 лет возникло и получило бурное развитие новое фундаментальное научное направление – компьютерная математика [3], которое зародилось на стыке математики и информатики. Были разработаны новейшие программные системы символьной математики или компьютерной алгебры (СКМ). Среди них наибольшую известность получили системы Mathcad, Derive, Matlab, Mathematica, Mapleи др. СКМ Maple и Mathematica по праву считаются мировыми лидерами в области символьных (аналитических) вычислений [1,3-5]. Особенно велика роль СКМ в образовании – они становятся не только удобным средством для выполнения огромного числа учебных расчетов, но и средством предоставления обучающимся, а нередко и преподавателям, знаний в области математики, физики и в иных науках, использующих математические методы. Трудно переоценить и их роль в подготовке высококачественных электронных лекций, учебных курсов и книг.

Рассмотрим сначала некоторые возможности систем Maple и Mathematica в области математического анализа. Так, при изучении темы “ряд Тейлора (Маклорена)” полезно сочетать разложение функций в ряд Тейлора с графической визуализацией такого разложения. Пример разложения в ряд Тейлора (Маклорена) функции sin(x) спостроением графика самой функции иее разложения в ряд шестого порядка в СКМ “Maple” приведен на рис.1. Это хороший пример визуализации результатов математических вычислений – здесь наглядно видно, что при малых значениях x график ряда практически повторяет разлагаемую функцию, но затем начинает сильно от нее отходить. Если увеличить число членов ряда до 12, то область совпадения увеличится примерно в 2,5 раза, что легко можно продемонстрировать в том же документе СКМ Maple.

В СКМ Maple и Mathematica реализованы мощные средства таких основных операций анализа как дифференцирование и интегрирование (как аналитического, так и численного). Возможности этих программ при вычислениии неопределенных, и определенных интегралов нередко просто поражают.Рассмотрим следующий поучительный пример. При изучении темы “интегрирование по частям” часто разбирается пример $\int xe^{-x}dx = -e^{-x}(x+1)$, и соответствующий определенный интеграл$\int_0^1 xe^{-x}dx = 1 - \frac{2}{e} \sim 0.264$. Отметим, что при подключении пакета “student” устудентовесть возможность не только получить конечный результат, но и увидеть промежуточные выкладки (в данном случае с помощью команды *intparts,* такая же возможность есть и в мобильном приложении Wolfram-Alpha). Немного сложнее пример$\int x^2e^{-x}dx = -e^{-x}(x^2 + 2x + 2)$и$\int_0^1 x^2e^{-x}dx = 2 - \frac{5}{e} \sim 0.160$, поскольку он решается *двукратным* интегрированием по частям (при каждоминтегрировании по частям“мешающая”степень *x*под интегралом понижается на единицу). Толковый студент может справится и с интегралами$\int x^3e^{-x}dx$ и $\int_0^1 x^3e^{-x}dx$, - потребуется *трехкратное* интегрирование по частям. Ну а если поставить задачу вычислить, например, интегралы$I_{20} = \int x^{20}e^{-x}dx$ и$J_{20} = \int_0^1 x^{20}e^{-x}dx$? Можетли ее решить самый сильный студент илиопытный преподаватель “в ручную”?Оказывается -что нет! Казалось бы, никаких принципиальных трудностей нет- требуется по стандартной методикевыполнить “всего лишь”*двадцатикратное* интегрирование по частям.

Однако по мере увеличения кратности начинают стремительно нарастать коэффициенты полинома в ответе, и вычисления становятся для ручного счета практически невыполнимой задачей(даже если активно использовать калькулятор!). Более того, с

определенным интегралом J_{20} не справлялись даже рассматриваемые СКМ в ранних версиях [ ] (не говоря уже о пакетах общего применения типа Excel).Но Maple8-10 (как и Mathematica 5-7) с легкостью берет этот интеграл и позволяет сразу и без какой-либо настройки вычислить для него как точное, так и приближенное значение.Вот как выглядитответ в этих примерах (получен в СКМ “Maple-8”):

$I_{20} = \int x^{20} e^{-x} dx$ = - $e^{(-x)}$(x^{20} + 20 x^{19}+380 x^{18}+ 6840 x^{17} +116280 x^{16} + 1860480 x^{15}+ 27907200 x^{14}+ 390700800 x^{13} + 5079110400 x^{12}+ 60949324800 x^{11}+ 670442572800 x^{10} + + 6704425728000 x^9 + 60339831552000 x^8 + 482718652416000 x^7 + 3379030566912000 x^6 + +20274183401472000 x^5 + 101370917007360000 x^4 +405483668029440000 x^3 + 1216451004088320000 x^2+ 2432902008176640000 x+ 2432902008176640000)$J_{20} = \int_0^1 x^{20} e^{-x} dx$ = - 661331331924808000 1$e^{(-1)}$ +2432902008176640000.

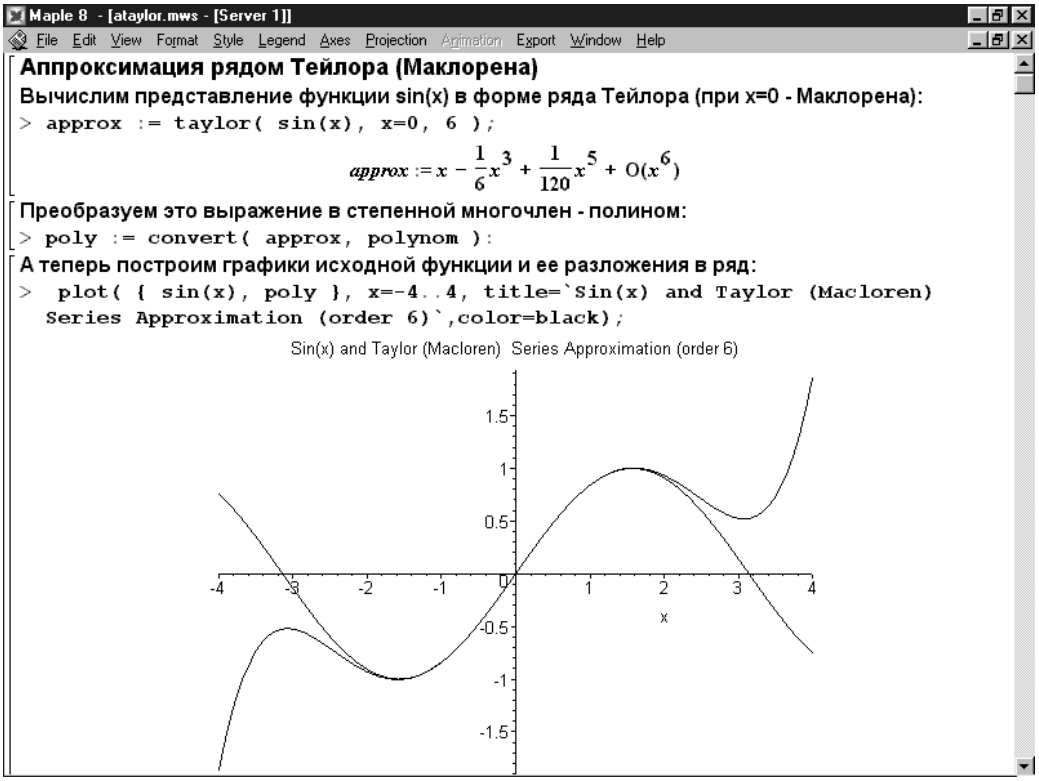


Рис.1. Сравнение графиков функции sin(x) и ее разложения в ряд Маклорена

В каждом слагаемом имеются огромные (а в J_{20}и очень близкие по модулю!) числа и потому для вычислений *принципиально необходимо* применение *арифметики высокой точности* (или разрядности). СКМ и Maple и Mathematicaтакими средствами, причем превосходными, обладают. В данном случае для получения приближенного значения интеграла J_{20} необходима разрядность не менее 25-30 цифр. В СКМ Maple тогда используется команда*evalf* (%, 30);= 0.01835046770 = J_{20} . При недостаточной точности (10-15 знаков) в обычных математических программах для J_{20}всегда получится грубо ошибочное нулевое значение.

Однако СКМ Mapleсправляется и со значительно более сложной задачей, когда в интеграле конкретный показатель степени заменен на обобщенный - *п. Как ни удивительно,* Maplec легкостью выдает аналитическое (!) решение для данного определенного интеграла:

$J_n = \int_0^1 x^n e^{-x} dx$ =($e^{(-1/2)}$/(n+1))Whittaker M (n/2,n/2+1/2,1).

Ответ выражен через сложную специальную функцию WhittakerM с тремя параметрами, и численное значение интеграла, рассчитанное Maple по этой формуле, при

n=20 совпадает с вышеуказанным. И как триумф СКМ Mapleприведем график (рис.2) зависимости значений данного интеграла от показателя степени *n*при его изменении от 0 до 50 (!) Плавный ход графика показывает, что в вычислении этого интеграла нет никаких признаков неустойчивости решения при изменении n, если соблюдать правило выбора разрядности вычислений.

В рассмотренном примере ярко проявилось важнейшая особенность СКМ Maple и Mathematica- возможность вычислений с любым (задаваемым пользователем) числом значащих цифр.Например, на любого обучающегося производит сильное впечатление, как эти системы практически мгновенно вычисляют значение иррациональных чисел $\sqrt{2}$, π, *e*со 100 или даже с 1000 (!) десятичных знаков.Разумеется, в практических расчётах такая точность почти никогда не нужна. Например, всего 40 точных цифр числа π достаточно, чтобы вычислить длину окружности всейвидимой Вселенной с точностью до диаметра атома водорода. Однако истинные математики одно время были просто «помешаны» на вычислении числа π с большой точностью. Кое кто потратил на это всю жизнь. Выдающийся вклад в такие расчеты внес Рамануджан, который еще в 1916 году предложил формулы для вычисления числа π с произвольной точностью. Они до сих пор используются для оценки эффективности суперкомпьютеров. В СКМ Maple и Mathematica благодаря встроенному аппарату точной арифметики можно обеспечить эффективную проверку подобных формул. Например, можно убедится, что все 600 цифр при вычислении числа π и по одной из формуле Рамануджана (она имеют вид суммы некоторых рациональных дробей и множитель $\sqrt{2}$) , и по встроенному в Maple алгоритму полностью совпадают.

Целочисленные операции обе СКМ выполняются абсолютно точно, сколько цифрне потребовалось бы. Среди них выделяются операции с вычислением факториалов (n! -произведение всех натуральных чисел от 1 до n включительно). Например, СКМ Maple моментально выдает результат 1000! – это число, содержащее примерно 2500 цифр (с трудом поместится на экране монитора)! А за пару секунд расчета – даже 100000! (это 450 тыс. цифр).

Если вычисление, например, числа π с большим числом знаков имеет чисто академический интерес, то вычисление факториалов более важно для практических расчетов. Дело в том, что факториалы входят в формулы комбинаторики (числа перестановок, размещений, сочетаний), и соответственно во многие формулы теории вероятностей и математической статистики, где значение n=100 или 1000 – обычное для практики дело. Например, вероятность появленийнекоторого события при *n* повторяющихся испытаниях ровно *k* раз дается известной формулой Бернулли [2]

$$p_n(k) = C_n^k p^k q^{n-k},$$

где $C_n^k = \frac{n!}{k!(\mathrm{n}-\mathrm{k})!}$ - число сочетаний из *n*по *k*.Если раньшепрямой расчет по этим формулам для больших *n*и *k*был невозможен, и приходилось использовать приближенные формулы (Муавра-Лапласа, и с не вполне ясной погрешностью),тоСКМ.

Maple и Mathematica легко вычисляют с требуемой точностью прямо по этим формулам даже для *n* = 1000 или даже 10000. Пусть, например, требуется вычислить вероятность того, что среди 1000 новорожденных будет не менее половины мальчиков, если вероятность рождения мальчика *p* = 0.515 (и соответственно, девочки q = 0.485). В формуле Бернулли тогда n=1000, а k меняется от 500 до 1000, т.е. нужно сложить 500 результатов по этой формуле, содержащих факториалы порядка 1000! ибольшие показатели степени. СКМ Maple выдает результат [2] за доли секунды (!):p = 0.8366435978 .

Рассмотренные примеры использования СКМ Maple и Mathematica в процессе изучения общих курсов математики в ВУЗе –лишь очень малая часть таких возможно-

стей. В любом разделе математики, в любой теме с помощью этих систем можно значительно расширить кругозор обучающихся, углубить знания, решать гораздо более сложные иболее интересные задачи и т.д.

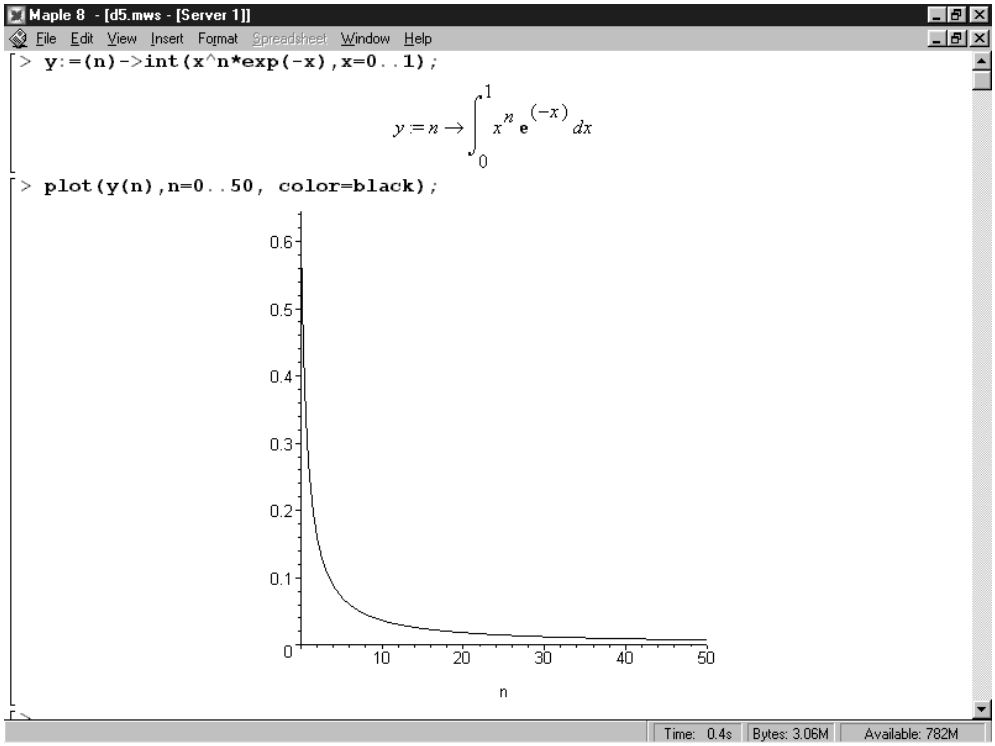


Рис.2. Значение интеграла от x^n*exp(-x) в пределах от 0 до 1 как функция n.

В идеале изучение этих систем должно идти параллельно с соответствующим разделом курса математики даже на тех специальностях, где математика отнюдь не является профилирующей. Опасения, что применяя эти системы “студенты ничего не будут знать”- обычно исходят от тех, кто их сам никогда и не использовал. Практика показывает, что все обстоит как раз наоборот – применяя эти системы студенты лучше усваивают основной материал, а полученные навыки работы с СКМ позволяет им решать задачи, которые обычным способом не под силу решить даже самому квалифицированному преподавателю.

Литература

1. Васильев, А.Н. Mathematica. Практический курс с примерами решения прикладных задач. Санкт-Петербург: Корона-Век, 2008

2. Горохов, В.Л., Семенов, В.А., Генк, А.В. Математика и информатика. Теория вероятностей и статистика (учебное пособие). Санкт-Петербург: СПбГИЭУ, 2007

3. Дьяконов, В.П. Maple 9.5/10 в математике, физике и образовании. Москва: Солон-пресс, 2006.

4. Дьяконов, В.П. Maple 10/11/12/13/14 в математических расчетах. Москва: ДМК Пресс, 2011

5. Фридман, Г.М., Леора, С.Н. Математика и Mathematica. Санкт-Петербург: Невский Диалект, 2010

Сведения об авторе

Генк Алексей Владимирович, старший преподаватель Санкт-Петербургскогоуниверситета ГПС МЧС России; e-mail genk_av@mail.ru.

Гераськин Алексей Сергеевич,

ВОЗМОЖНОСТЬ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В АУДИОФАЙЛ С ПОМОЩЬЮ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

С развитием информационных технологий возникла потребность в защите информации от различных модификаций. С использованием различных средств вычислительной техники злоумышленнику легко осуществить незаконное распространение и модификацию мультимедийной информации, что наносит ущерб законному владельцу. Это привело к необходимости разработки средств защиты мультимедийной информации от незаконного распространения. Одним из решений этой проблемы стала технология цифровых водяных знаков.

Цифровой водяной знак (ЦВЗ) – это некоторая информация, которая внедряется в защищаемый файл таким образом, чтобы различие между исходным файлом и файлом с водяным знаком не было заметно человеку. С другой стороны, механизм внедрения должен быть достаточно стойким, чтобы противостоять основным атакам[1].

Особый интерес представляет собой проблема внедрения ЦВЗ в аудиофайл. В аудиофайл ЦВЗ могут быть внедрены во временной области, либо в области преобразования (частотной области). Методы внедрения во временной области, как правило, основаны на замене наименьшего значащего бита или скрытии информации в эхосигнале. Скрытие информации в частотной области учитывает характеристики человеческого слуха, а также особенности типичных атак. Сигнал разлагается на составляющие для получения данных о фазе и амплитуде, после чего коэффициенты разложения изменяются определённым образом.

Для разложения сигнала чаще всего используются такие преобразования, как дискретное преобразование Фурье, дискретное косинусное преобразование и дискретное вейвлет-преобразование. В нашей работе мы использовали вейвлет-преобразование из-за удобства обработки сигнала. Оно раскладывает сигнал на несколько частотных поддиапазонов. Преимущества вейвлет-преобразования также в том, что оно, во-первых, вычисляется за линейное время, а во-вторых, хорошо противостоит атакам. Хотя при вейвлет-преобразовании искажения, вносимые в аудиофайл, несколько выше, чем при других преобразованиях, но с помощью изменений параметровпреобразования их можно снизить.

На практике используются следующие величины для оценки эффективности методов внедрения ЦВЗ:

- отношение сигнал/шум, объективная оценка различия;
- вероятность ошибки на бит.

Эти величины позволяют определить соответствие методов внедрения требованиям неразличимости и стойкости.

Отношение сигнал/шум (signal-to-noise ratio, SNR) – мера, используемая в науке, которая выражает соотношение уровня исследуемого сигнала к уровню фонового шума. Чаще всего результат выражается в децибелах (положительный SNR говорит о преобладании сигнала над шумом).

В общем случае SNR определяется как отношение мощности сигнала к мощности шума, согласно формуле (1):

$$SNR = \frac{P_{\text{сигнала}}}{P_{\text{шума}}} \quad (1)$$

В случае с внедрением водяных знаков SNR выражает разницу между исходным и защищённым файлом и определяется по формуле (2):

$$SNR(A,\tilde{A}) = 10log_{10}\frac{\sum_{n=1}^{N} a^2(n)}{\sum_{n=1}^{N}\left(a(n)-\tilde{a}(n)\right)^2}\text{Дб}, \quad (2)$$

где A – исходный сигнал, $\tilde{A}$ – защищённый сигнал, N – длина сигналов, a – составляющие сигнала (сэмплы), $\tilde{a}$–составляющие защищённого сигнала.Значение SNR должно быть выше 20 Дб.

Во время проведения исследования был выполнен анализ возможного внедрения ЦВЗ различными вейвлетами: Хаара, Добеши 2, Добеши 20 и Койфлет [2]. При этом был найден наиболее эффективный вейвлет-фильтр.

В качестве водяного знака будем использовать небольшое по размеру изображение (в пределах 5000 пикселей). Изображение представляется в виде одномерной последовательности байтов. Для простоты необходимо привести изображение к черно-белому виду. Тогда каждый пиксель будет описываться числом от 0 до 255. Последовательность этих чисел и будет искомым водяным знаком. Для внедрения ЦВЗ с помощью вейвлетов использовались следующие методы:

1. Первый метод внедрения заключается в разложении аудиосигнала на поддиапазоны с помощью дискретного вейвлет-преобразования и последующем внедрении водяного знака в поддиапазон, содержащий детализирующие коэффициенты последнего уровня. Изменение этих коэффициентов наименее заметно в результирующем аудиофайле. Процесс внедрения состоит из следующих основных этапов: разложение сигнала с помощью вейвлет-преобразования и, собственно, внедрение информации в полученные коэффициенты. Применяем дискретное вейвлет-преобразование к исходному сигналу. При выборе уровня преобразования необходимо найти компромисс между точностью разложения и вместимостью контейнера. Следует отметить, что с каждым уровнем точность представления повышается, однако объём информации, который можно будет скрыть, уменьшается вдвое. Также необходимо, чтобы длина сигнала была кратна 2^N, где N – уровень разложения. Самым оптимальным выбором будет являться разложение до второго уровня [2]. Данный метод будем называть простейшим методом;

2. Основная идея второго метода,который будет называться методом на основе статистических характеристик, заключается в том, что в зависимости от значений вейвлет-коэффициентов определяется, в какие из них можно внести большие изменения (для увеличения стойкости), а в какие из них – меньшие (чтобы избежать сильного искажения аудиосигнала). Водяной знак должен быть представлен в виде последовательности нулей и единиц.

Сначала необходимо провести вейвлет-преобразование исходного сигнала. Затем этот набор коэффициентов делится на блоки фиксированной длины s. Длина блока может варьироваться, её увеличение приводит к увеличению стойкости и одновременно усилению вносимых искажений. Компромисс между стойкостью и неразличимостью достигается, если блок состоит примерно из 10 коэффициентов.

После разбиения на блоки вычисляется среднее значение каждого блока m_i, по формуле (3):

$$m_i = \frac{1}{s}\sum_{j=is}^{(i+1)s-1}|c_j|, \quad (3)$$

где $0 \le i < k$ (k – количество блоков), c – значения коэффициентов в блоке.

После чего вейвлет-коэффициенты каждого блока изменяются по формуле (4):

$$c_j' = \begin{cases} m_i, \text{если } \left|\frac{c_j}{m_i}\right| < k \text{ и } w_l = 1 \\ -m_i, \text{если } \left|\frac{c_j}{m_i}\right| < k \text{ и } w_l = 0 \\ c_j, \text{если } \left|\frac{c_j}{m_i}\right| \geq k \end{cases} \quad (4)$$

Здесь c_j' – изменённые коэффициенты, k – интервал внедрения (изменяемый параметр, $k > 2$), w_l – l-ый бит водяного знака (начинается с нуля и инкрементируется, если для очередного j выполнилось условие 1 или 2),$i = \left\lfloor \frac{j}{s} \right\rfloor$. Иными словами, эта формула означает, что если c_j попадает в интервал $[-km_i, km_i]$, то в зависимости от очередного бита водяного знака, коэффициент меняется на $-m_i$ или m_i. Параметр k может изменяться в зависимости от требований к свойствам алгоритма (увеличение k увеличивает объём контейнера и вносимые искажения). Оптимальное значение параметра – около 10.

После применения формулы производится обратное вейвлет-преобразование, которое порождает аудиосигнал с водяным знаком.Стоит отметить, что необходимой стойкости и неразличимости можно добиться, введя ещё один параметр α $(0{,}5 < \alpha < k)$ и заменив в рабочей формуле m_i и $-m_i$ на αm_i и $-\alpha m_i$, соответственно.

Для извлечения водяного знака необходимо разложить сигнал с помощью вейвлет-преобразования, разбить полученные коэффициенты на блоки и подсчитать их средние m_i. После чего нужно применить формулу извлечения (5):

$$w_i = \begin{cases} 1, \text{если } 0 \leq \frac{c_j'}{m_i'} \leq \left(\frac{k+\alpha}{2}\right) \\ 0, \text{если } -\left(\frac{k+\alpha}{2}\right) \leq \frac{c_j'}{m_i'} < 0 \end{cases} \quad (5)$$

При такой схеме внедрения среднее значение коэффициентов в каждом блоке не изменяется. Однако, если сигнал был подвергнут каким-либо атакам, то m_i' могут быть несколько модифицированы, однако благодаря тому, что весь массив коэффициентов разбивается на блоки, водяной знак можно извлечь даже после атак [4];

3. Третий метод представляется следующим образом,произвольная матрица размера $m \times n$ может быть представлена в виде $A = Q_1 \Sigma Q_2^T$, где Q_1 есть ортогональная матрица размера $m \times m$, Q_2 – ортогональная матрица размера $n \times n$, а матрица Σ имеет размер $m \times n$, причём элементы, лежащие на её главной диагонали – сингулярные числа, а все остальные элементы являются нулевыми.

На первом этапе внедрения, водяной знак представляется в виде последовательности битов, а аудиосигнал разбивается на равные блоки. Чем больше длина блока, тем меньшее количество информации можно будет внедрить (оптимальной является длина блока в районе 2048). Затем каждый блок подвергается вейвлет-преобразованию 4 уровня, в результате чего получаются поддиапазоны $D1$, $D2$, $D3$, $D4$ и $A4$. После этого полученные поддиапазоны формируют матрицу D так, как показано на рисунке 1:

<table>
<tr><td colspan="8">$D1$</td></tr>
<tr><td colspan="4">$D2$</td><td colspan="4">$D2$</td></tr>
<tr><td colspan="2">$D3$</td><td colspan="2">$D3$</td><td colspan="2">$D3$</td><td colspan="2">$D3$</td></tr>
<tr><td>$D4$</td><td>$D4$</td><td>$D4$</td><td>$D4$</td><td>$D4$</td><td>$D4$</td><td>$D4$</td><td>$D4$</td></tr>
</table>

Рис.1. Формирование матрицы D из вейвлет-коэффициентов.

Таким образом, во внедрении водяного знака будут участвовать сразу все детализирующие поддиапазоны, а не только поддиапазон последнего уровня.Полученная матрица раскладывается с помощью вышеупомянутой процедуры сингулярного разложе-

ния ($D = U\Sigma V^T$). Из полученной матрицы Σ выделяется подматрица размера 4x4 (обозначим её S), так как использование для внедрения всей матрицы Σ может повлиять на неразличимость. Затем взять очередные 12 бит водяного знака и также образовать из них матрицу 4x4, при этом на главной диагонали у неё будут нули (эту матрицу обозначим W). Внедрение происходит по формуле: $S_w = S + \alpha W$, где S_w – результирующая матрица, α – интенсивность водяного знака (может регулироваться для достижения компромисса между неразличимостью и стойкостью, оптимальное значение – около 3). Такая техника оставляет нетронутыми сингулярные значения матрицы D, что позволяет избежать сильных искажений исходного аудиосигнала.

На следующем этапе матрица S_w подвергается сингулярному разложению, причём полученные в результате матрицы U_1 и V_1^T сохраняются для каждого блока (они понадобятся в процессе извлечения). Затем вычисляется матрица $D_w = U\Sigma' V^T$, где Σ' – матрица Σ с заменённой подматрицей S на S_w. Матрица D_w подвергается обратному вейвлет-преобразованию.Этот процесс повторяется для каждого блока, таким образом, получается аудиосигнал с водяным знаком.

Для извлечения изображения необходимо вначале получить матрицу S_1' для каждого блока согласно процедуре, описанной выше, затем вычислить матрицу $S_w' = U_1 S_1' V_1^T$. Из матрицы S_w' извлекаются и анализируются 12 недиагональных значений. Значения, в которые был внедрён бит 0 намного меньше, чем те, в которые была внедрена единица. Таким образом, вначале необходимо вычислить среднее всех недиагональных значений (обозначим его M) и вычислить биты водяного знака по формуле (6):

$$W(n) = \begin{cases} 0, S_{w_{ij}}' \le M \\ 1, \text{иначе} \end{cases} \quad (6)$$

Объединяя биты из всех блоков, получаем исходное изображение [5]. Далее этот метод будем называть методом с использованием сингулярного разложения.

Для оценки эффективности методов используется несколько параметров. Одним из таких параметров является объективная оценка различия (objectivedifferencegrade, ODG). Эта величина вычисляется согласно алгоритму PEAQ (оценка восприятия качества звука). Алгоритм симулирует восприятие звука человеческой слуховой системой, благодаря чему он позволяет оценить качество аудиосигнала в той же степени, что и реальные люди.

После внедрения цифрового водяного знака, алгоритм PEAQ может быть применён к выходному файлу, в результате чего будет получено значение ODG, которое характеризует, на сколько водяной знак различим на слух в аудиофайле. Аудиосигнал, с внедрённым в него водяным знаком, может быть подвержен ряду атак и стандартных операций над сигналами (фильтрация, сжатие, и т.д.). Хотя эти операции могут существенно не повлиять на качество аудиосигнала, они способны повредить водяной знак, внедрённый в него.

Устойчивость алгоритма измеряется с помощью величины, называемой вероятность ошибки на бит (bit error rate, BER). Она определяется как отношение ошибочно извлечённых бит водяного знака к общему числу внедрённых бит и может быть выражена формулой (7):

$$BER = \frac{100}{l} \sum_{n=0}^{i-1} \begin{cases} 1, W_n' = W_n \\ 0, W_n' \ne W_n \end{cases}, \quad (7)$$

где l – длина водяного знака, W_n' – n-ый извлечённый бит водяного знака, W_n – n-ый бит оригинального (внедрённого) водяного знака.Приемлемыми являются значения BER не выше 20%.

Для оценки неразличимости будут использоваться два критерия. Первый – соотношение сигнал/шум (SNR), используется для проверки внедренного ЦВЗ. Значение

SNR было вычислено отдельно для каждого метода и каждого вейвлет-фильтра. Результаты приведены в таблице 1. В данной и последующих таблицах используются следующие сокращения: ПРОСТ – простейший метод, СТАТ – метод на основе статистических характеристик, СИНГ – метод с использованием сингулярного разложения.

Таблица 1.

Значения SNR

	Вейвлет Хаара, Дб	Вейвлет Добеши порядка 2,Дб	Вейвлет Добеши порядка 20,Дб	Вейвлет Койфлет,Дб
ПРОСТ	61,46	66,61	70,07	65,7
СТАТ	22,2	22,65	21,82	22,81
СИНГ	115,97	115,99	117,22	116,13

Вторым критерием неразличимости является объективная оценка различия (ODG). Результаты оценки этого параметра приведены в таблице 2.

Таблица 2.

Значения ODG

	Вейвлет Хаара	Вейвлет Добеши порядка 2	Вейвлет Добеши порядка 20	Вейвлет Койфлет
ПРОСТ	-0,05	-0,08	0	-0,09
СТАТ	-0,67	-0,67	-0,67	-0,67
СИНГ	-0,02	-0,02	-0,02	-0,02

Степень совпадения извлечённого ЦВЗ и исходного определялась с помощью величины вероятность ошибки на бит (BER). Как уже было указано, при значении BER не выше 20% считается, что извлечение не удалось. Однако, стоит отметить, что если BER не превосходит 40%, то визуально изображение можно распознать. Поэтому в таблице 3 значения от 0 до 20% извлечение удалось, от 20,01% до 40% –извлечение удалось, но с большими искажениями, выше 40% –водяной знак распознать невозможно.

Результаты, полученные в результате исследования, приведены в таблице 3.

Таблица 3.

Значения BER атак

№ атаки	1Х	1Д2	1Д20	1К	2Х	2Д2	2Д20	2К	3Х	3Д2	3Д20	3К
1	13	27	39	27	4	8	13	5	13	13	12	11
2	3	2	13	1	0	0	1	0	1	1	2	1
3	27	40	45	38	2	2	6	2	6	9	7	1
4	40	47	48	45	6	7	13	11	6	5	3	3
5	40	43	46	41	9	12	13	16	7	16	21	17
6	46	45	46	49	3	1	3	1	0	0	0	0
7	55	54	53	54	58	49	31	47	0	0	0	0
8	0	44	51	49	0	7	25	17	0	15	19	17
9	52	52	52	50	31	28	22	27	24	28	25	27
10	0	0	0	0	0	0	0	0	0	0	0	0
11	12	19	36	17	3	5	10	4	12	11	8	7
12	50	52	50	51	31	26	21	28	13	9	3	7

Здесь методы обозначены номером от 1 до 3: номер 1 – простейший метод, номер 2 – статистический метод, номер 3 – метод с сингулярным разложением, а также обозначения фильтров: Х – Хаара, Д2 – Добеши порядка 2, Д20 – Добеши порядка 20, К – койфлет. При исследовании использовались следующие атаки:

1. добавление к аудиосигналу низкочастотный шум, симулируя воздействие источника тока;

2. добавление к аудиосигналу синусоидальный сигнал с целью исказить поддиапазон с водяным знаком;

3. добавление к аудиосигналу белого шума;
4. замена каждого сэмпла на среднее между ним и следующим;
5. сглаживание сэмпла, снижая слишком большие значения и увеличивая слишком малые;
6. усиление громкости сигнала;
7. сдвиг фазы сигнала на 180 градусов;
8. замена местами каждых двух последовательных сэмплов;
9. симуляция исчезновение сигнала или потерю пакетов;
10. сбрасывание всех наименьших значащих битов в 0;
11. сбрасывание в ноль всех сэмплов, меньшие определённой величины;
12. удаление всех сэмплов, равных нулю.

Исходя из вышеприведённых данных, можно сделать вывод, что метод 1 обладает средней неразличимостью, но плохой стойкостью (выдерживает меньше половины атак). Метод 2 демонстрирует среднюю неразличимость и хорошую стойкость, особенно против естественных атак, например, зашумления. Метод 3 обладает самой лучшей неразличимостью и стойкостью, выдерживая практически все атаки, однако, следует помнить, что в нём используется два преобразования, что увеличивает вычислительную сложность. Что касается различных вейвлет-фильтров, можно увидеть, что каждый из них эффективен против разных атак, но в целом значения для разных фильтров не слишком различаются. Учитывая, что вейвлет Хаара обладает наименьшей вычислительной сложностью, предпочтительнее использовать именно его.

Литература

1. Гераськин А.С., Стрельникова С.Ю., Завенягин М.П. Исследование возможности улучшения реализации алгоритма метода коча для встраивания цифровых водяных знаков в изображения // Безопасность информационных технологий. 2018. Т. 25. № 4, С. 86-94.

2. ДреминИ.М., ИвановО.В., НечетайлоВ.А. Вейвлеты и их использование // Успехи физических наук. 2001. Т. 171. №5 С. 465-501.

3. Al-HajA. DWT-BasedAudioWatermarking [Электронныйресурс] / A. Al-Haj, A. Mohammad, L. Bata // TheInternationalArabJournal of Information Technology. – Vol. 8, No. 3, July 2011. – Pages 326-333. – URL: http://ccis2k.org/iajit/PDF/vol.8,no.3/1774.pdf (датаобращения: 20.06.2020).

4. Fallahpour M. High capacity audio watermarking using the high frequency band of the waveletdomain [Электронныйресурс] / M. Fallahpour, D. Megias // Multimedia Tools and Applications. – Volume 52, Issue 2-3, April 2011. – Pages 485-498. – URL: http://in3.uoc.edu/opencms_in3/export/sites/in3/webs/grups_de_recerca/Kison/_resources/documents/J3.pdf (датаобращения: 20.06.2020).

5. Al-Haj A. An imperceptible and robust audio watermarking algorithm [Электронныйресурс] / A. Al-Haj // EURASIP Journal on Audio, Speech, and Music Processing. – 2014:37 – URL: http://www.asmp.eurasipjournals.com/content/pdf/s13636-014-0037-2.pdf (датаобращения: 20.06.2020).

Сведения об авторе

Гераськин Алексей Сергеевич, кандидат педагогичекских наук, доцент кафедры теоретических основ компьютерной безопасности и криптографииСаратовского национального исследовательского государственного университета имени Н.Г. Чернышевского; e-mail: Gerascinas@mail.ru.

Ефремов Сергей Константинович

ОСОБЕННОСТИ УДАЛЕННЫХ ЗАНЯТИЙ С КУРСАНТАМИ НА МАССОВЫХ СПЕЦИАЛЬНОСТЯХ

Основными формами учебных занятий в высшем учебном заведении (ВУЗе) являются лекции, практические занятия и семинары. Вековой опытпроведения этих занятий со студентами в учебных аудиториях позволил отработать методики их проведения, используемые при этом педагогические приемы. Они широко обсуждены в педагогическом сообществе[1, 2, 4, 5].

Научно-технический прогресс позволил в последние десятилетия расширить возможности получения знаний. Появилось и в настоящее время часто используется дистанционное обучение, при котором сохраняются все присущие учебному процессу компоненты, но преподаватель и учащиеся пространственно разделены часто большими расстояниями. Дистанционное обучение требует некоторого пересмотра порядка предъявления учебного материала, в частности методики проведения занятий, в том числе структуры и содержания занятий. Дистанционное обучение применяется в системе повышения квалификации, переподготовке. При повышенной мотивации учащихся в усвоении учебного материала удаленность преподавателя от обучаемых не играет особой негативной роли. Все чаще дистанционное обучение используют в заочном обучении студентов ВУЗов.

Пандемия коронавируса 2020 года и связанное с ней довольно продолжительное нахождение в режиме самоизоляции заставили перейти на удаленное проведение занятий во всей системе образования. Но срочность, неожиданность перехода не позволила достаточно полно перестроиться на полноценное дистанционное обучение. Вводились в использование существующие вебинар-платформы, такие как Zoom, WebexMeeting, BBB и другие для проведения занятий с визуальным контактом преподавателя и обучаемых. Для дистанционного обмена учебными документами в цифровом формате массово осваивалась облачная память, в более простом варианте использовалась электронная почта, в самых простых случаях – телефонные службы WhatsAppи Viber. Но методики проведения занятий, многократно отлаженные на аудиторных занятиях, во многом сохранились и при переходе на «удалёнку». Дополнительные сложности создавала и недостаточная техническая готовность ВУЗов в случаях, когда использовались собственные учебные серверы. Они часто не выдерживали резко возросшей на них нагрузки.

Огромным преимуществом лекций в аудиториях является непосредственный контакт преподавателя и учащихся, дающий преподавателю по ходу лекции обратную связь в реальном времени. Это преимущество может быть сохранено за счет использования вебинар-платформ. Особенно удобны варианты, позволяющие преподавателю не только получать в чате тексты с вопросами и прочим, но и предоставлять учащимся трибуну для полноценного визуального и голосового общения. Кроме этого, сохраняется постоянный визуальный контакт преподавателя с каждым учащимся. Однако такой подход применим только при относительно небольшом количестве учащихся на занятии.

Такие платформы незаменимы и при проведении семинаров, когда предоставление трибуны учащимся для докладов и выступлений по вопросам семинара обязательно. Здесь существует опасность при выступлениях прямого зачитывания учащимися заранее заготовленных или найденных по ходу занятия в Интернет текстовок по теме семинара. Задача преподавателя здесь – вывести обсуждение вопроса за рамки материала, выданного на лекции или имеющегося в основных учебниках, т.е. перевести занятие в режим дискуссии, позволяющей понять степень освоения и осмысления каждым учащимся учебного материала.

Практические занятия обычно связаны с выполнением конкретных заданий по изучаемой теме. И здесь в полной мере проявляется стремление части обучаемых «жить за чужой счет», т.е. предоставлять преподавателю чужие отчеты о выполнении задания, в лучшем случае слегка измененные по форме, подписанные собственной фамилией. При небольшом количестве учащихся выход видится в выдаче индивидуальных вариантов заданий, что накладывает дополнительную часто большую нагрузку на преподавателя при подготовке занятия, но эту проблему решает.

Несколько другая ситуация возникает, когда количество обучаемых большое, достигает пятидесяти, ста и более человек.

Для проведения лекций на большие аудитории видится использование одного из двух вариантов:

– режим on-line – чтение лекции в вебинар-комнатах. При большой аудитории теряется возможность визуального двухстороннего контакта, но сохраняется обратная связь на уровне чата, в котором слушатели могут по ходу лекции задавать вопросы, а лектор сохраняет возможность оперативно реагировать на них;

– режим off-line- заблаговременная видеозапись лекции с просмотром ее слушателями во время, отведенное на лекцию расписанием занятий. При этом теряется стандартный контакт лектора со слушателями. Частично его можно восстановить, если в это время будет работать любой канал текстовой обратной связи (от включенной для вопросов слушателей вебинар-комнаты до пересылки вопросов с использованием WhatsApp в созданной для лекционного потока группе). Лектор имеет возможность реагировать на вопросы слушателей, оперативно создавая и выкладывая видеоролики с дополнительными пояснениями по заданному вопросу либо в простых случаях выкладывая в группе WhatsApp текстовый ответ на заданный вопрос. Преимуществом варианта видеозаписи является возможность для слушателя индивидуально управлять темпом лекции, переводить просмотр лекции на паузу при необходимости сделать подробные записи в конспект содержимого слайда, представленного на экране. Вторым преимуществом является возможность возврата воспроизведения лекции в любую временную точку для повторного просмотра фрагмента с рассмотрением сложного учебного материала.

Практические занятия проводятся в группах с количеством обучаемых, позволяющим в полной мере использовать возможности вебинар-комнат. Но здесь возникает другая проблема. При использовании единого для всех обучаемых задания на занятие почти автоматически проявляются любители «жить за чужой счет», выкладывающие преподавателю отчеты по работе на занятии других обучаемых под своей фамилией. При полностью стандартном задании выявить такие копии отчетов практически невозможно при решении на занятии задач численными методами или создании неких объектов по стандартным алгоритмам (например, отформатированный по заданию текст в текстовом процессоре или создание конкретной базы данных). Если отчет по выполнению задания создается в форме свободного текста, то преподавателю предоставляется возможность поработать в режиме компьютерной программы Антиплагиат. Нужно просмотреть несколько десятков или сотен отчетов и выявить совпадающие по содержанию, что крайне малопродуктивно даже с учетом того, что любители «жить за чужой счет» редко утруждают себя попытками хотя бы немного изменить построение фраз или элементы форматирования взятого отчета-первоисточника. Создавать полностью индивидуальные задания на каждое занятие для каждого обучаемого сопряжено для преподавателей с огромными временными затратами. И даже разработка 3-5 вариантов задания проблемы не решит.

Возможные выходы из данной ситуации:

– внедрение в текст задания в разных местах сменных условий. Вместе с заданием обучаемым предоставляются перечни вариантов по таким местам с описанием порядка выбора каждым обучаемым своего варианта из каждого перечня. Количество таких мест и количество вариантов по каждому из них должно быть таким, чтобы для каждого обучаемого его вариант задания хотя бы в одном месте отличался от задания любого другого обучаемого. При проверке отчетов у преподавателя дополнительная задача – особо контролировать учет в результатах работы обучаемого его индивидуальных фрагментов задания;

– использование современных информационных технологий. Формирование индивидуальных исходных данных в заданиях на занятие и проверка правильности полученных результатов решения задач, непосильные для использования в ручном режиме из-за огромных временных затрат преподавателей, могут осуществляться с помощью компьютерных программ. Временные затраты сводятся к минимуму вследствие несоизмеримо большей производительности компьютера по сравнению с человеком при решении вычислительных задач. Остается сделать одно – создать генерирующую и проверочную программу для каждого такого занятия. Такой подход подробно описан в работе [3] и прошел успешную проверку в учебном процессе.

Литература

1. Голованова Н.Ф. Педагогика: учебник и практикум для академического бакалавриата / Н.Ф. Голованова. – Люберцы: Юрайт, 2016.

2. Князева В.В. Педагогика / В.В. Князева. – Москва: Вузовская книга, 2016.

3. Лаптев В.Н.Отехнологиях разработки программных приложений для генерирования и проверки практических заданий по математическим дисциплинам/В.Н. Лаптев, Е.В. Михайленко// Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ). – Краснодар: КубГАУ, 2020. – №01(155).

4. Резник С.Д. Студент вуза: технологии и организация обучения в вузе: учебник / С.Д. Резник, И.А. Игошина; под общ. ред. д-ра экон. наук, проф. С.Д. Резника. – Пенза: ПГУАС, 2014.

5. Сорокина Е.И. Организационные формы обучения в вузе / Е.И. Сорокина,Л.Н. Маковкина//Инновационные педагогические технологии: материалы III Междунар. науч. конф. (г. Казань, октябрь 2015 г.). – Казань: Бук, 2015.

Сведения об авторе

Ефремов Сергей Константинович, кандидат технических наук, доцент, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: efremovsk@yandex.ru.

Епифанцева Виктория Александровна

МЕТОДЫ, СПОСОБЫ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ И БАЗ ДАННЫХ В ПОДРАЗДЕЛЕНИЯХ МВД РОССИИ С ПРИМЕНЕНИЕМ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ

В настоящее время, в связи с широким распространением средств вычислительной техники, почти в каждом отделе внутренних дел имеются объекты, предназначенные для автоматизированной обработки данных. Рост сложности обработки информации и увеличения объема, хранимой в Министерстве Внутренних дел резко повысили уязвимость информации, а также самого процесса. Постоянное расширение круга пользователей, имеющих непосредственный доступ к ресурсам, усложнение режимов экс-

плуатации вычислительных систем, привели к необходимости сохранности информации во времяее сбора, хранения и обработки.

Под обеспечением сохранности информации обычно понимают организованную совокупность методов, средств и мероприятий, предназначенных для предотвращения искажения, уничтожения или несанкционированного использования накапливаемых, хранимых и обрабатываемых данных [3].

С начала появления и использования вычислительной техники проблема защиты информационно-программного обеспечения в Министерстве Внутренних дел находится в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей.

Для нормального функционирования подобные объекты должны быть защищены от различного рода внешних и внутренних воздействий, которые могли бы привести к потере или искажению обрабатываемой и управляющей информации, а также к модификации самих систем. Одним из важнейших направлений в обеспечении надежной и безопасной работы являетсязащита информации и баз данных от различных угроз.

Воплощением ее последствий является применение систем автоматизированной защиты информации и проведение организационно-технических мероприятий, до их внедрения и во время использования.

В связи с особой важностью обеспечения безопасности информации в подразделениях Министерства Внутренних дел, требуется постоянный контроль за их состоянием. Это достигается путем назначения должностных лиц, ответственных за обеспечение безопасности информации. Их деятельность постоянно связана с проведением таких организационно-технических мероприятий как:

–разработка, ведение и обеспечение сохранности необходимой на объектах проектной и другой, в части вопросов специальной защиты, документации;

–контроль за своевременным выполнением мероприятий по поддержанию состояния объектов требованиям руководящих документов;

–контроль за порядком допуска в помещения объектов, к средствам вычислительной техники и обрабатываемой на них информации;

–своевременная проверка уровня знаний лиц, непосредственно работающих в подразделениях.

При большом количестве электронно-вычислительных машин, разных сроках введения их в эксплуатацию, периодическом изменении руководящих документов требуются значительные трудозатраты на выполнение всех организационно-технических мероприятий, превышающие, как правило, возможности специалистов, назначаемых ответственными за выполнение работ. Положение можно улучшить, если часть рутинной работы автоматизировать, что и определяет актуальность темы данной работы.

Объектно-ориентированный подходявляется основой современной технологии программирования, испытанным методом борьбы со сложностью систем [8]. Представляется естественным и, более того, необходимым, стремление распространить этот подход и на системы информационной безопасности, для которых, как и для программирования в целом, имеет место проблема сложности. Любой разумный метод борьбы со сложностью опирается напринцип «divide et impera» - «разделяй и властвуй».

В данном контексте этот принцип означает, что сложная система информационной безопасности на верхнем уровне должна состоять из небольшого числа относительно независимых компонентов.

С помощью объектно-ориентированного программирования создаются различные приложения, в которых используются следующие методы для обеспечения безопасности информации и баз данных в подразделениях Министерства Внутренних дел: доступ, сохранность, секретность.

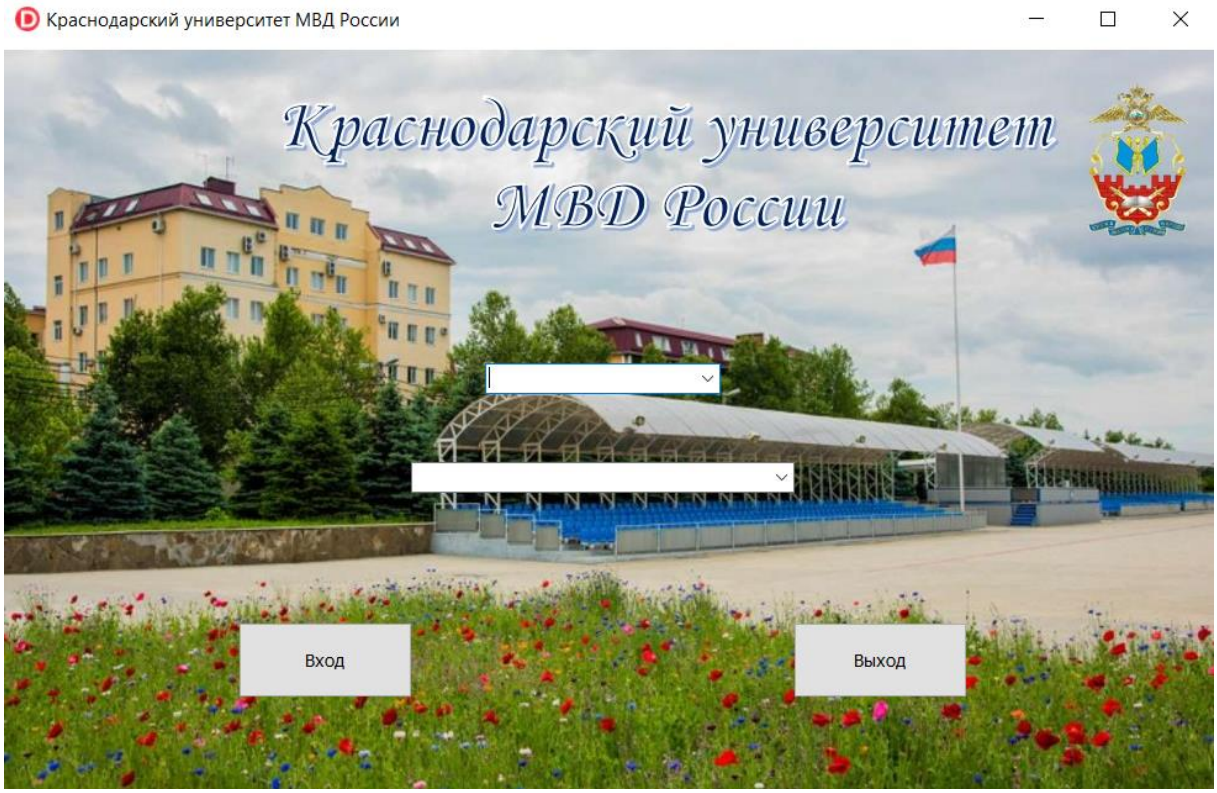


Рис. 1. Главное окно базы данных «Достижения курсантов Краснодарского университета МВД России»

К средствам защиты информации и баз данных можно отнести программные и аппаратные. Программные средства защиты информации реализуются через [2, 4]:

- идентификацию пользователя посредством присвоения уникального, идентификационного ключа;
- идентификацию пользователя согласно утвержденных полномочий;
- регистрацию действий пользователя в электронном журнале отчета.
- контроль окончания работы пользователем через подтверждение уникального, идентификационного ключа, либо через ввод ключа безопасности активизирующего аварийную систему защиты информации и базданных
- ограничение времени простоя.

К аппаратным средствам защиты информации и баз данных относятся: подтверждение личности пользователя посредством технологий FaceID, голосовой доступ, дактилоскопический доступ. Также контроль функций копировать, вставить, удалить и вырезать с использованием сочетания клавиш на клавиатуре и контекстного меню манипулятора мышь, трекбола, тачскрин в рамках действующих полномочий пользователя[6]. Использование специальных мониторов, препятствующих фото, видеофиксации изображения сторонними устройствами. Использование USB ключей, регистрация съемных носителей.

Прикладной характер объектно-ориентированного программирования позволяет не только создавать программы и программные комплексы защиты информации и баз данных, но и оперативно адаптировать, модифицировать относительно новых конкретных угроз [1, 5, 7].Даже при совокупном, абсолютном использовании программных и аппаратных средств и выше указанных мероприятий не будет максимально эффективным без динамично меняющихся, адаптируемых программ и программных комплексов защиты информации и баз данных в подразделениях Министерства Внутренних дел Российской Федерации.

Литература

1. Ашарина, И.В. Объектно-ориентированное программирование в C++: лекции и упражнения: Учебное пособие для вузов / И.В. Ашарина. – М.: РиС, 2015.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2016. – 136 с.
3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. – Рн/Д: Феникс, 2017.
4. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016.
5. Лафоре, Р. Объектно-ориентированное программирование в C++. Классика ComputerScience / Р. Лафоре. – СПб.: Питер, 2013.
6. Михайленко, Е.В. Информационная безопасность: курс лекций / Е.В. Михайленко, И.Н. Старостенко. – Краснодар: Краснодарская академия МВД России, 2005.
7. Павловская, Татьяна C/C++. Процедурное и объектно-ориентированное программирование. Учебник / Татьяна Павловская. – М.: Питер, 2015.
8. Шакин, В.Н. Объектно-ориентированное программирование на Visual Basic в среде Visual Studio. Net / В.Н. Шакин, А / В.Н. Шакин, Г.К. Сосновиков, З. – Москва: РГГУ, 2015.

Сведения об авторе

Епифанцева Виктория Александровна, преподаватель кафедры информатики и математики Краснодарского университета МВД России; e-mail: torohova_viktori@mail.ru.

Жилин Роман Андреевич

ЧИСЛЕННЫЙ МЕТОД ФОРМИРОВАНИЯ АЛЬТЕРНАТИВНЫХ КОАЛИЦИЙ ЭКСПЕРТОВ

При разработке математической модели в некоторой предметной области, являющейся слабоформализуемой, существует вероятность того, что у экспертов могут быть противоположные мнения. Для отдельных предметных областей оценка квалификации эксперта может быть неоднозначна, так как могут существовать несколько независимых подходов к оценке изучаемых объектов.Для таких ситуаций, характеризующихся несогласованностью мнений экспертов (например, в социально-экономической сфере), может оказаться эффективным метод формирования альтернативных коалиций экспертов.

Цель работы. Разработка численного метода формирования альтернативных коалиций экспертов в области решения слабоформализуемых задач.

В работах А.В. Мельникова [1], Е.А. Буркова [2], С.А. Бабкина [3], Н.П. Путивцевой [4], А.В. Старцева [5], В.В. Конобеевских [6], К.Е. Волковицкого [7] и В.В. Навоева [8]рассматриваются вопросы формирования и оценки качества согласованной группы экспертов.

В работах Е.А. Буркова и К.Е. Волковицкого рассматривались вопросы формирования альтернативных коалиций экспертов. Е.А. Бурковым предложено формирование альтернативной коалиции экспертов на основе методов математической статистики.

К.Е. Волковицкий утверждает, что коалиции образуются экспертами, которые либо полностью разделяют точку зрения, отражаемую признаками, либо полностью её отрицают. В его исследованиях группа экспертов разделялась на несколько коалиций, противоречащих друг другу.

В вычислительных экспериментах, описанных в научной литературе, формировалась только одна альтернативная коалиция. При этом авторами не учитывалась специфика объекта исследования, которая, в свою очередь, может влиять на необходимость использования альтернативных коалиций.

В данной работе авторами предложена методика формирования нескольких альтернативных коалиций экспертов с учетом различий в оценках для главных и второстепенных признаков.

Формирование альтернативных коалиций экспертов состоит из следующей последовательности шагов.

Шаг 1. Осуществим разделение экспертов на группы с использованием отношения дисперсий между ошибками в оценивании относительно средних значений. В основе данного метода лежит процедура проверки статистических гипотез, описанная в работах различных авторов [9, 10].

Так, метод Гольдфельда-Квандта [10] предполагает упорядочивание данных по переменной, относительно которой есть предположение о гетероскедастичности остатков, разбиение данных на части и сравнение суммы остатков m первых и m последних наблюдений.В работе предложено из-за малочисленности оцениваемых признаков делить их на 2 группы.

Для осуществления шага 1 необходимо построить матрицу L различий.

$$L = \begin{pmatrix} \Delta_{11} & \Delta_{12} & \Delta_{13} & \dots & \Delta_{1N} \\ \Delta_{21} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \Delta_{ij} & \dots \\ \Delta_{M1} & \dots & \dots & \dots & \Delta_{MN} \end{pmatrix} \quad (1)$$

где Δ_{ij} – разность значений рангов оценок экспертов (a_{ij}) и рангов, полученных по средним значениям $\overline{x}_i$.

Составим вектор-строку P, значения элементов которой можно получить по формуле (2):

$$p_j = \begin{cases} \dfrac{\sum\limits_{i=1}^{\frac{M}{2}} \Delta_{ij}^2}{\sum\limits_{i=\frac{M}{2}+1}^{M} \Delta_{ij}^2}, \sum\limits_{i=1}^{\frac{M}{2}} \Delta_{ij}^2 > \sum\limits_{i=\frac{M}{2}+1}^{M} \Delta_{ij}^2; \sum\limits_{i=\frac{M}{2}+1}^{M} \Delta_{ij}^2 \neq 0 \\ \dfrac{\sum\limits_{i=\frac{M}{2}+1}^{M} \Delta_{ij}^2}{\sum\limits_{i=1}^{\frac{M}{2}} \Delta_{ij}^2}, \sum\limits_{i=\frac{M}{2}+1}^{M} \Delta_{ij}^2 > \sum\limits_{i=1}^{\frac{M}{2}} \Delta_{ij}^2; \sum\limits_{i=1}^{\frac{M}{2}} \Delta_{ij}^2 \neq 0 \end{cases} \quad (2)$$

Упорядочим значения p_j и сформируем вектор-строку Z, в которой элементы расположим сначала по убыванию при выполнении второго условия формулы (2), затем по возрастанию для первого условия.

Для предварительной оценки согласованности экспертов по группам значимых и менее значимых критериев предложим функцию различия оценок по важности признаков $Z = Z(j)$.

Распределение экспертов на группы $Z_k (k = 1,\ 2, \dots, K)$ и формирование матриц ре-

зультатов A_k осуществляется на основе разделения экспертов на три группы в соответствие со значением $Z_{крит}$ – границы вхождения экспертов в группы согласованности по важности критериев.

Функция $Z = Z(j)$ достигает значение $Z_{крит}$ в двух точках, тогда области отнесения экспертов в соответствующие группы Z_k (при $K = 2$):

$$Z_1\, m[Z_{max1}, Z_{крит1}];\ Z_2\, m[Z_{крит1}, Z_{крит2}];\ Z_3\, m\,(Z_{крит2}, Z_{max2}]. \qquad (3)$$

Шаг 2. Для каждой группы Z_k определяем коэффициент конкордации (W) и среднее значение ($\overline{x}_i$) признака, а также осуществляем формирование расширенной корреляционной матрицы R^*.

Шаг 3. В каждой группе Z_k определяем согласованную группу экспертов с коэффициентом конкордации $W \geq 0.7$[11]. Для этого необходимо выполнить следующие действия: если $W < 0.7$, то из рассмотрения исключаем экспертов со значением коэффициента корреляции $\overline{r}_j < 0.5$и далее по одному эксперту с наименьшим значениемкоэффициента корреляции до выполнения условия $W \geq 0.7$[12]. Выбранных экспертоввключаем в коалицию Y_k.

Шаг 4. Исключаем из общего числа высококвалифицированных специалистов, участвующих в проведении опроса, тех, кто оказался в составе коалицийY_k. Выполняем алгоритм, начиная с шага 1, до тех пор, пока количество экспертов,не вошедших в состав коалиций не достигнет минимального значения.

Шаг 5. Для полученных коалиций формируем матрицу H – матрицу расстояний Хэмминга между рангами признаков в выделенных группах. Данная матрица обладает свойством обратной симметрии, а так же свойством однородности.

$$H = \begin{pmatrix} 1 & h_2 & h_3 & \dots & h_M \\ h_1/h_2 & 1 & h_3/h_2 & \dots & h_M/h_2 \\ h_1/h_3 & h_2/h_3 & 1 & \dots & h_M/h_3 \\ \dots & \dots & \dots & \dots & \dots \\ h_1/h_M & h_2/h_M & h_3/h_M & \dots & 1 \end{pmatrix} \qquad (4)$$

По полученным значениям h определяем расхождение рангов по признакам в группах и определяем, можно ли из нихформировать одну коалицию:

а) если $h \leq 4$, то экспертов формируем в одну коалицию;

б) если $h > 4$, то экспертов формируем в несколько коалиций.

Верификация данных. Осуществим верификацию полученных результатов на примере исследования признаков нарушителя общекриминальной направленности [13].

В ходе экспертного оценивания составлена прямоугольная матрица A размера 10×72, определен вектор средних значений признаков и рассчитана расширенная корреляционная матрица $R*$ [14].

Осуществим разделение экспертов на 3 группы. Для этого в соответствии с формулой (2) составим вектор-строку P и сформируем функцию различия оценок по важности признаков $Z = Z(j)$.

В качестве $Z_{кр}$в ходе вычислительного эксперимента подобрано значение 2, что соответствует ∝= 0,25; n = 5; k = 1 для F-распределения. В рамках дальнейших исследований предполагается аналитически описать закономерности и определить методику точной оценки параметров F-распределения.

Таблица 1.

Результат распределения экспертов на группы

Общее количество экспертов 72			
№ группы	Группа 1	Группа 2	Группа 3
Количество экспертов в группе	6	20	46
Ранг по оценкам всех экспертов	Ранг в группе, $\overline{v}_{i1}$	Ранг в группе, $\overline{v}_{i2}$	Ранг в группе, $\overline{v}_{i3}$
9	9	9	2
2	6	1	3
7	3	7	4
1	5	3	6
8	4	8	7
6	2	2	1
3	1	6	5
4	7	5	9
10	8	10	8
5	10	4	10

В каждой из трех групп выделим согласованную группу экспертов на основе сортировки по коэффициенту корреляции. Для сформированных групп экспертов определим степень согласованности и средние значения признаков. Полученные данные представлены в таблице2.

Так как в данных группах $W \geq 0,7$, а $h \geq 4$, то группы принимаются за альтернативные коалиции. Коалициями с мощностью множества менее 10% от общего числа экспертов можно пренебречь (группа 1). Окончательно получаем две альтернативные коалиции экспертов.

Таблица 2.

Результат формирования согласованных групп экспертов

№ группы	Группа 1	Группа 2	Группа 3
Количество экспертов	3	8	10
Коэффициент конкордации, W	0,71	0,73	0,74

Ранги признаков нарушителей общекриминальной направленности для альтернативных коалиций:

$$\overline{v}_{ak1} = (1, 3, 8, 9, 10, 2, 4, 6, 5, 7), (5)$$

$$\overline{v}_{ak2} = (10, 9, 2, 5, 4, 3, 7, 6, 8, 1). (6)$$

Вывод.Использование мнений альтернативных коалиций при разработке математических моделей позволяет получить более точное описание предметной области.

В работе с применением разработанного численного метода были выделены две альтернативные коалиции. Учет альтернативного мнения экспертов позволит точнее определять результаты экспертизы.Проведенные вычислительные эксперименты показали устойчивость данного метода к исходным данным (к экспертной информации).

Литература

1. Мельников А.В. Кластерно-иерархические методы экспертизы технических и экономических объектов [Текст]: дис. докт. техн. наук: 05.13.18: защищена 16.09.2014. Воронеж, 2014. 354 с.

2. Бурков Е.А. Методы и алгоритмы анализа и агрегирования групповых экспертных оценок [Текст]: дис.канд. техн. наук: 05.13.01: защищена 14.11.2011. Санкт-

Петербург, 2011.189 с.

3. Бабкин С.А. Оценка характеристик радиотехнических устройств с использованием экспертно-статистических методов [Текст]: дис.канд. техн. наук: 05.13.18: защищена 19.11.2009. Воронеж, 2009. 180 с.

4. Путивцева Н.П. Обработка экспертной информации при отборе экспертов в научно-технической сфере [Текст]: дис.канд. техн. наук: 05.13.01: защищена 16.05.2012. Белгород, 2012. 233 с.

5. Старцев А.В. Модели согласования экспертных оценок в процедурах группового выбора [Текст]: дис.канд. техн. наук: 05.13.01: защищена 02.06.2004. Воронеж, 2004.122 с.

6. Конобеевских В.В. Статистические методы экспертных систем оценки качества радиотехнических приборов уголовно-исполнительной системы [Текст]: дис.канд. техн. наук: 05.13.18: защищена 22.09.2006. Воронеж, 2006. 182 с.

7. Волковицкий К.Е. Исследование пространства ранговых оценок и разработка пакета прикладных программ классификационной обработки данных экспертного оценивания: дис.канд. физ-мат. наук: 01.01.09. Москва, 1984. 154 с.

8. Навоев В.В. Экспертно-статистический метод оценки характеристик информационно-измерительных систем [Текст]: дис.канд. техн. наук: 05.13.18: защищена 23.12.2003. Воронеж, 2003. 164 с.

9. Гмурман В. Е. Теория вероятностей и математическая статистика.Москва: Высшаяшкола, 2003. 479 с.

10. Goldfeld, S.M. SomeTests for Homoscedasticity. Journal of the American Statistical Association. 1965. – 60 (310). P. 539-547.

11. Kendall M. Rank correlation methods.London: Griffin, 1970. 202 p.

12. ДобровГ.М. Экспертныеоценкивнаучно-техническомпрогнозированииКиев: Науковадумка, 1974.

13. Жилин Р.А. К вопросу о классификации нарушителей безопасности охраняемых объектов. Охрана, безопасность, связь. 2019. № 4-2 (4). С. 115-120.

14. Жилин Р.А. Численный метод предварительной экспертизы альтернатив нарушителей охраны объектов общекриминальной направленности.Вестник Воронежского института МВД России, 2019, № 3. С. 46-54.

Сведения об авторе

Жилин Роман Андреевич,командир взвода радиотехнического факультетаВоронежского института МВД России; e-mail: zhilin99.zhilin@yandex.ru.

Жмурко Даниил Юрьевич

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МЕТОДОЛОГИИ ПРОГНОЗИРОВАНИЯ ПРИ АДАПТИВНОМ УПРАВЛЕНИИ СЛОЖНЫМИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМИ ОБЪЕКТАМИ

Определение перспективы развития комплексного прогнозирования в XXI в. является предметом углубленных исследований и разработок большого круга ведущих академических и отраслевых институтов, специализированных научных центров, отдельных коллективов ученых и специалистов.

«Практика моделирования, анализа и прогнозирования эволюционирующих процессов и соответствующих им временных рядов позволяет сделать вывод, что одного универсального, удовлетворяющего всем требованиям и не обладающего недостатками подхода не существует. Каждый из них имеет свои достоинства, недостатки, границы» [4] и области применения.

Наряду с этим существует проблема концептуального уровня, заключающаяся в разрозненности, узкой специализации научного знания, которое испытывает еще более серьезный кризис в области верификации, о состоятельности различных теорий. Существуют также трудности с их объяснительными возможностями, т.е. с предоставлением не субъективной, а объективной оценки происходящему и обоснования полезности той или иной парадигмы развития.

При этом, первостепенной становится необходимость окончательного перехода на синергетическую парадигму развития, которая создает условия для движения к объективно заданной цели развития осознанно, методом эволюционного непрерывного познания, и ее полную реализацию.

Естественно, в оценках на «долгосрочную перспективу должна присутствовать такая информация, с помощью которой удается отслеживать качественные изменения моделируемых процессов» [3]. Она представлена в перспективных расчетах с использованием предложенной методологии, позволившей определить и выявить общую консенсус-траекторию развития макроэкономической динамики в мировом сахарном производстве в среднесрочном и долгосрочном временных горизонтах (рисунок 1).

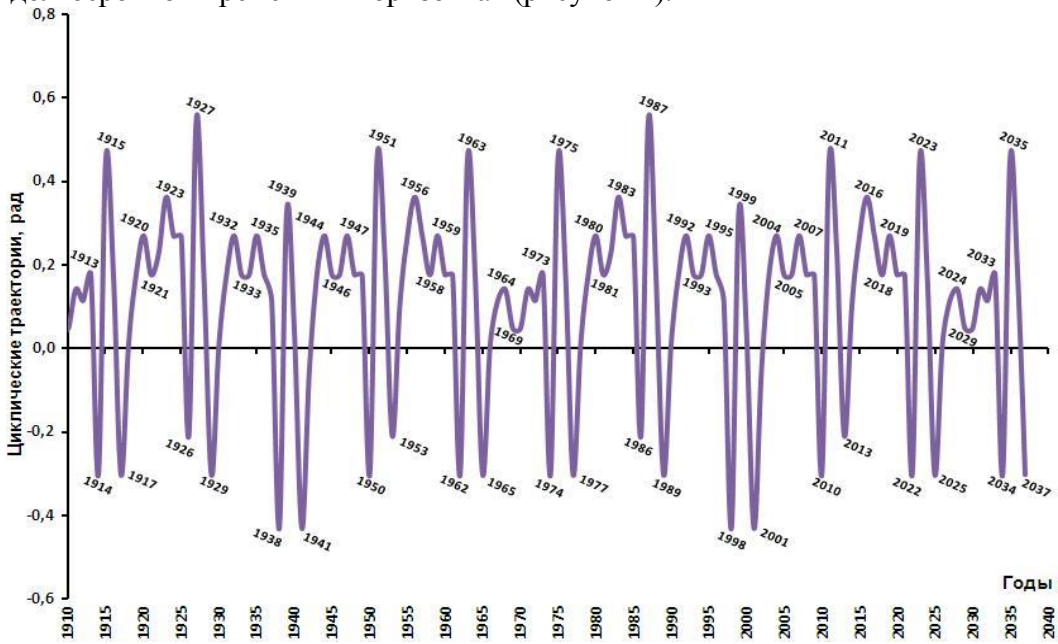


Рис. 1. Пример эталонной модели развития мирового сахарного производства.

Сложность получения достаточно реалистичных оценок такого рода связана с необычностью кризисной ситуации, в которой Россия пребывает в течение нескольких десятилетий.

Очень востребованной является процедура получения прогнозных оценок для тех перспективных периодов, в которых ожидается смена тенденций. На основе анализа, проведенного автором исследования, можно сделать следующий вывод: магистральная теория инверсивных полей (МТИП) и другие прогностические модели позволяют получать прогнозные оценки достаточно высокой точности. Особенно хотелось бы отметить композитные линии моделей, построенных на базе МТИП, результаты прогнозов по которым оказались наиболее точными.

Модели, в которых присутствуют индикативные механизмы, находят широкий круг применения как при осуществлении теоретических построений, так и при решении прикладных задач. Таким образом, с их «помощью удается построить эффективный механизм прогнозной модели в ситуациях, когда специфичность условий экономического развития проявляется в отсутствии полной и достоверной информации, по которой мож-

но было бы определить закономерность, лежащую в основе структурных изменений модели. С подобной ситуацией приходится иметь дело как в технических приложениях» [1], так и в экономических, для которых она более характерна.

Области применения комплексного прогнозирования

Прогнозирование реализует вполне понятную на интуитивном уровне идею рефлексии поведения моделируемого объекта, делающую его универсальным методом с позиций применения в разных сферах народного хозяйства и других предметных областях.

В таблице 1 представлены перспективные направления использования на практике МТИП и других элементов комплексного прогнозирования (вычисления возможны только на основе статистических данных).

Таблица 1.

Перспективные области применения комплексной методологии прогнозирования

Задача	*Полученные и ожидаемые результаты*
Прогнозирование количественных результатов выращивания сельскохозяйственных культур	Повышение прибыли и рентабельности производства сельскохозяйственных культур на 4–6 % за счет повышения адекватности принимаемых решений по выбору культур для выращивания
Прогнозирование количественных результатов при производстве сахара	Повышение прибыли и рентабельности производства сахара и его полуфабрикатов на 5–7 % за счет повышения адекватности принимаемых решений по выбору производственной стратегии
Прогнозирование продуктивности разных секторов АПК	Повышение уровня рентабельности за счет более рационального использования разных ресурсов отрасли АПК. Улучшение стратегического планирования, на основе которого можно построить отраслевые стратегии и программы
Анализ финансовых рисков при управлении портфельными инвестициями (для разных рынков) с выработкой рекомендаций	Уменьшение риска потери вложенных финансовых ресурсов при создании инвестиционного портфеля. Создание условий для подбора оптимальных объектов управления капиталом, конечной целью которых является получение прибыли и достижения положительных результатов от таких инвестиций. При рациональном управлении норма прибыли должна повыситься на 10–12 %
Оценка и прогнозирование уровня безработицы, инфляции, ВВП и других экономически важных показателей	Принятие органами исполнительной власти превентивных мер по снижению уровня безработицы и инфляции. Однако при этом индекс ВВП повышается за счет благосостояния граждан страны
Прогнозирование структуры и объема рынка сельскохозяйственной продукции	Выработка рекомендаций по реструктурированию производства с учетом прогнозируемой конъюнктуры рынка
Прогнозирование криминогенной обстановки в стране	Определение ориентиров вероятностного состояния (уровня, структуры) преступности в будущем и ее детерминант. Выработка рекомендаций по профилактике правонарушений, включая качественную и количественную оценки предполагаемых изменений, с указанием их примерных сроков
Оценка рисковых ситуаций для страховых компаний с выработкой рекомендаций	Снижение до минимального уровня страховых рисков, которые могут быть оценены с точки зрения вероятности наступления страхового случая и количественных размеров возможного ущерба
Прогнозирование военно-политической обстановки в России и мире	Выработка рекомендаций по мерам государственной политики и направлениям ее использования на основе анализа глобальных вызовов, связанных с ними угроз, возможностей государственного развития, перспективных направлений в геополитике, инновационных технологиях, в области научных исследований в военной сфере

Несмотря на то, что методология комплексного прогнозирования состоит из множества разработанных моделей и методов (в том числе и МТИП), которые дают практически одни и те же прогнозные оценки, условия их применения различны.

Перспективные направления в развитии методологии комплексного прогнозирования

Рассмотрим перспективы применения методик и технологий комплексного прогнозирования сахарной отрасли АПК, которые также актуальны и для других секторов экономики России. Реализация некоторых из представленных здесь методик и технологий описана в работах автора.

Целесообразно разделить их на две большие группы: первая основывается на механизмах реализации комплексного прогнозирования через принципы работы с большими данными, вторая – развивается в рамках некоторого экономического контура на базе теории конвергенции.

Ia. *Технология больших данных* (*англ.big data или economic data*) предполагаетработу с большим объемом структурированных данных.

Методы и техники анализа, применимые к большим данным:

– методы интеллектуального анализа данных (*англ.data mining*) составляют: всевозможные методы классификации, моделирования и прогнозирования, основанные на применении деревьев решений, эволюционного программирования, ассоциативной памяти, нечеткой логики и т.п. К ним нередко относят также статистические методы (анализ временных рядов, выживаемости и связей, методов A/B-тестирования, дескриптивный, факторный, кластерный, корреляционно-регрессионный, компонентный, дискриминантный анализ).

– смешение и интеграция данных – набор техник, позволяющих интегрировать разнородные данные из разнообразных источников для возможности глубинного анализа;

– краудсорсинг – категоризация и обогащение данных силами неопределенного круга лиц, привлеченных в рамках публичной оферты;

– машинное обучение, включая обучение с учителем и без него, а такжеансамбль методов (*англ. ensemble learning*), который использует несколько обучающих алгоритмов с целью получения более высокой эффективности прогнозирования, чем можно получить от каждого из них по отдельности;

– сетевой анализ, ИНС, оптимизация, в том числе генетические алгоритмы;

– распознавание образов;

– пространственный анализ – класс методов, использующих в данных топологическую, геометрическую и географическую информацию;

– имитационное моделирование;

– прогнозная аналитика;

– визуализация аналитических данных.

Ib. *Технология обработки глубоких данных* (*англ.deep data*), использующая сложные нейросети с множеством нейронов и слоев. Для обучения этих глубоких нейросетей, а также для обнаружения сложных закономерностей в огромных массивах данных используются повышенные вычислительные мощности и усовершенствованные методики. «Глубина» обеспечивается некоторым количеством скрытых слоев нейронов в сети, которые проводят математические вычисления.

Ic. *Технология обработки разноструктурированных данных* (*англ.diff data*), реализация которой происходит независимо от их форм и видов (количественных или качественных). В основе лежит наделение смыслом массивов данных, визуализация, сбор идей и принятие решений на основе этих данных.

Id. *Платформы, реализующие* т*ехнологии обработки больших данных*

1) Бизнес-разведка (*англ.business intelligence* или *BI*) – это обозначение компьютер-

ных методов и инструментов для организаций, обеспечивающих перевод транзакционной деловой информации в читабельную форму, пригодную для бизнес-анализа, а также средства, предназначенные для обработки больших массивов бизнес-данных.

Преимущество такой технологии заключается в том, что при сочетании поступающих внешних и внутренних сигналов на выходе получается более полная картина «структурированных» данных, т.е. аналитика, которую нельзя получить только от одного из этих источников.

2) Реляционные системы управления базами данных (СУБД) с поддержкой декларативных языков программирования, которые применяются для разработки, модификации и управления данными в реляционной БД, управляемой соответствующей СУБД (SQL и т.п.).

II. *Теория конвергенции экономических систем* (экономическая модель конвергенции, или конвергентная модель экономики).

Теория конвергенции предполагает, что происходит взаимное проникновение и дополнение капиталистической и социалистической модели развития общества тем самым предопределяется образование нового его типа, которое будет основываться на сочетании положительных сторон этих социально-экономических систем. В рамках такого общества предстоит развиваться нашей стране. Другими словами, происходит синтез моделей рыночной экономики и плановой. Ярким примером служат социально-экономические системы стран Скандинавии (как разновидность западного общества) и КНР (как разновидность коммунистического общества).

Первые упоминания о теории конвергенции относятся к 60–80-х гг. XX в. Авторами теории являются *Дж. Гэлбрейт, У. Ростоу, Ф. Перру, Я. Тинберген* и др. Доминирующим в научном сообществе стал подход *Я. Тинбергена*.

«Многие экономисты отмечали, что сближение и слияние двух СЭС состоится в результате развития одинаковой технологической структуры, которая имеет общие закономерности функционирования. В качестве факторов, способствующих их сближению, чаще всего выделялись общие признаки в управлении, методах государственного регулирования и т.п.

С распадом мировой системы социализма проблема конвергенции в такой ее трактовке в значительной степени утратила свою актуальность. Однако некоторые отечественные и зарубежные экономисты начали использовать понятие конвергенции применительно к процессу ускорения развития экономически отсталых стран и приближения их по уровню развития к передовым» [2].

Условием ускоренного и успешного развития конвергенционных процессов является проведение этими странами эффективной экономической политики, основанной, прежде всего, на разработке прогнозных моделей налоговых режимов и балансе международной торговли, в котором большую долю должна составлять продукция с высокой добавленной стоимостью.

Наряду с этой теорией существует отдельное научное направление, относящееся к конвергенции технологий (конвергентных технологий), под которым и понимается широкий круг процессов сближения – как отдельных областей наук, так и непосредственно технологий. Следует отметить, что этот процесс рассматривается с двух крайних точек зрения:

– простой междисциплинарной конвергенции, в основе которой лежит влияния горизонтальных нанотехнологий на другие технологии;

– появление инновационных направлений науки и технологии, которые в будущем будут развиваться по своим собственным траекториям.

Практическое использование конвергентных технологий будет характеризоваться такими особенностями, как повсеместное проникновение новых технологий, основу которой составит техническая инфраструктура и неограниченная информационная доступность (т.е. возможность получить информацию о любых процессах и явлениях за короткий промежуток времени).

«С большой вероятностью в рамках этой теории будет развиваться экономическая мысль XXI в. Методология комплексного прогнозирования также будет строиться на принципах конвергенции (с элементами дивергенции). Ключевым моментом для нее должна стать разработка оптимальных «критериев конвергенции» при верификации результатов исследования.

Будущее всегда многовариантно и в силу этого несет в себе неопределенность, однако в каждом моменте прошлого находит отражение только одна из разновидностей возможных альтернатив» [1]. Следовательно, многообразие будущего рождается из вариантов, распределенных случайным образом по всему горизонту прошлого. Для решения такого рода задач требуется постоянное совершенствование специальных приемов и методик при проектировании прогнозных моделей в контексте адаптивного и рационального подхода к управлению крупными отраслевыми образованиями, отражающего альтернативность моделируемых процессов.

В качестве перспективы или продолжения данного исследования интересной будет разработка таких научно-исследовательских проектов, которые смогли бы обогатить методологию комплексного прогнозирования:

1. Разработка методов статистики объектов нечисловой природы.
2. Совершенствование существующих и разработка новых исследовательских «платформ» синергетического прогнозирования, основанных на эвристических методах.
3. Описание возможных сценариев изменения структуры сахарного рынка.
4. Выявление циклов в структурных макроэкономических скачках.
5. Разработка моделей и методов формирования инвестиционных стратегий систем со сложной иерархической структурой в условиях кризиса (на примере сахарного рынка).

Указанные перспективы комплексного применения прогнозирования результативности крупных объектов экономики указывают на необходимость более глубокой проработки вопросов, связанных с инструментальным и математическим анализом переходных процессов и кризисных явлений вариативной экономики.

При прочих конкретных условий перспективным для комплексного прогнозирования и экономического развития является использование таких законов управления в макроэкономике, которые одновременно позволяют наряду с достижением высоких качественных и количественных показателей производительности сделать приемлемым уровень колебаний в рамках устойчивости системы управления.

Литература

1. Давнис В.В., Тинякова В.И. Адаптивные модели: анализ и прогноз в экономических системах. – Воронеж: Воронеж. гос. ун-т, 2006. – 380 с.
2. Красильников О.Ю. Теоретико-методологические основы исследования структурных сдвигов в современной российской экономике: дис. … д-ра экон. наук. – Саратов: СГУ, 2001. – 318 с.
3. Тинякова В.И. Модели адаптивно-рационального прогнозирования экономических процессов: монография. – Воронеж: Воронеж. гос. ун-т, 2008. – 336 с.
4. Яковенко В.С. Экономическая цикломатика: методология, практика: дис. … д-ра экон. наук: 08.00.13. – Ставрополь: СтавГУ, 2008. – 441 с.

Сведения об авторе

Жмурко Даниил Юрьевич, кандидат экономических наук, доцент, преподаватель кафедры информатики и математики Краснодарского университетаМВД России; e-mail: danis1982@list.ru.

Иванов Вячеслав Юрьевич,
Иванова Анастасия Вячеславовна

ТЕХНОЛОГИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Информация – один из самых ценных ресурсов, но только в руках того, кто умеет и может её правильно и вовремя использовать, недаром её считают одним из факторов производства. Как и любой другой ценный ресурс, информация требует постоянной и качественной защиты. Защита информации является одним из приоритетов современной государственной политики и бизнеса. Современные технические системы защиты информации на данный момент достигли той степени развития, когда в их работе можно не сомневаться ещё долгие годы, человек же так и остался человеком со своими привычками, стереотипами и слабостями или же просто самым слабым, ненадёжным звеном в системе безопасности, которую сам же и изобрел.

В современном мире идёт бурный процесс развития научно-технической базы, создаются новые науки и направления в них, которые в свою очередь порождают новые теории и подходы. Новые идеи требуют вложения больших денежных средств на их реализацию, разработку, исследования и испытания. В связи с тем, что в обществе происходит процесс усиления и укоренения коммерциализации и жёсткой рыночной конкуренции, поиск более новых способов и каналов сбыта своих товаров или услуг для получения максимальной прибыли, каждый стремиться сполна, окупить свои вложения как правомерными, так и неправомерными способами. Недобросовестная конкуренция вышла на новый уровень, когда экономические субъекты стали использовать коммерческую разведку и шпионаж для получения какой-либо информации о своих конкурентах. Любая информация прямо или косвенно связанная с конкретным субъектом, собранная в одном месте может оказаться очень солидной по своему содержанию. Из этого следует увеличение степени значимости и стоимости информации. Данные факторы не могли не отобразиться на желании экономических субъектов обезопасить себя от посягательств подобного рода. Все чаще экономические субъекты начинают учитывать информационные риски, как своими силами, так и с привлечением сторонних специализированных фирм. Информационные риски высчитываются исходя из таких факторов: размер предприятия, направление деятельности предприятия, законодательная база и степень экономического развития государства в котором находится экономических субъект. Одним из главных информационных рисков считается социальная инженерия.

Телекоммуникации и сети интернет технологий стали доступны каждому человеку, вести бизнес без данного сервиса очень сложно, это позволяет злоумышленникам, находясь в безопасности, добывать нужную им информацию. Существует масса интернет порталов, на которых можно найти множество технической информации и советов по теоретическим и практическим знаниям о краже информации. Для того, чтобы в полной мере осознавать всю информацию, полученную на данных ресурсах, человеку необходимо быть уверенным пользователем компьютера, знать его устройство представлять себе, как происходят те или иные процессы в его работе, знать технологию программирования и несколько языков программирования. На этих же порталах создаются открытые и закрытые сообщества, на которых возможен как обмен опытом и материалом, позволяющим использовать его для дальнейшего развития в данной отрасли, так и для координации действий при совместных атаках. Зачастую в подобных сообществах присутствует чёткая иерархия управления, её верхушку возглавляют те самые социальные инженеры, что научились не только эффективно управлять сознанием и действиями легальных интернет пользователей, но и стали делать на этом целый бизнес.

Издавна существовало только три способа заполучить что-то, что принадлежит другому человеку: обменять (купить), отобрать силой и обхитрить (обмануть). Первый

подход породил экономику, второй – породил гонку вооружений, третий целую науку, работающую на уровне подсознания. Она известна как социальная инженерия. Социальная инженерия(*social engineering*) – это объединение теоретических принципов и практических приёмов для осуществления манипулирования действиями человека без применения технических средств. Этот способ построен на применении знаний о слабости человеческого фактора[1].

Все техники социальных инженеров построены на систематических ошибках в мышлении и шаблонных уклонениях возникшие из-за дисфункциональных убеждений, отображающихся в анализе автоматических мыслей человека. Рассмотрим основные из них.

Нейролингвистическое программирование (НЛП) основанное в 60-х годах прошлого века считается псевдонаукой и может оказаться действенным способом для формирования положительного образа. НЛП – не признанное направление практической психологии, направленное на управление вербального и невербального поведения человека. Суть его заключается в том, чтобы выявить слабые и уязвимые точки личности с воздействием на них нейролингвистическими методами с целью достижения конкретных целей, таких как добыча информации или личная выгода. НЛП тесно связан с таким понятием как гипноз.

Обратная социальная инженерия – ситуация, когда жертва сама приходит к злоумышленнику и выдаёт ему все интересующую его информацию с помощью[2]. Этот способ намного сложнее предыдущих, ввиду знания особых знаний и навыков, но и эффект от него намного приятнее так как жертва сама отдаёт все ценную информацию. Диверсия – первая часть заключается в создании ошибки или проблемы, с которой объект не сможет полноценно пользоваться системой. Как правило, проявляется ошибка не сразу, а через какое-то время. Помощь – вторая часть обратной инженерии, в которой объект просит о помощи в исправлении ошибки или проблемы вызнаваемой заранее продуманной диверсией.

Реклама – рекламирование своих услуг на опережение настоящих представителей данных услуг. Идёт манипуляция таким качеством человека, как стадный инстинкт. Если человек увидит хорошо симулированные отзывы и похвалы пробельной работы, он в гораздо большем случае поддастся искушению приобрести данный товар или услугу.

Телефонный фрикинг– это один из видов хакинга. Злоумышленник эксплуатирует телефонные системы и работников телефонных компаний для получения сведений об их клиентах, а также для совершения, бесплатных звонков на большие расстояния.

Претекстинг – махинация целью, которой является поиск информации об объекте, после чего разрабатываться сценарий, по которому человек должен предоставить какие-либо сведения или сделать определённое действие. С развитием интернета для добычи такой «личной информации» социальному инженеру не нужно даже взламывать электронные почты или мессенджеры жертвы. Как показывает практика, пользователи халатно относятся к безопасности в сети, выкладывая в свободный доступ сведения, что могут быть использованы социальными инженерами. Люди сами стали выдавать о себе столько информации, сколько не выдали бы даже на допросе у спецслужб.

Кви про кво (Quid pro quo – от лат. «то за это» фразеологизм, обычно обозначающий недоразумение, связанное с тем, что кто-то или что-то принимается за кого-то или что-то другое). Например, злоумышленник находится в другом городе, стране или континенте, что в значительной мере усложняет идентификацию личности, сбор доказательств и фактов причастия человека к данной атаке. Далее он звонит в офис, какого-либо предприятия и, представившись системным администратором обслуживающим их компьютерную сеть, говорит, что ему нужно, чтобы вы сделали какие-либо действия со своего рабочего компьютера для оптимизации работы всей системы. Малограмотный

сотрудник офиса не станет проверять достоверность полученных указаний и будет делать то, что ему скажут, тем самым подвергая опасности всю компанию. Успешность звонка зависит от того заподозрит ли собеседник что его пытаются использовать или нет. Для этого социальный инженер прощупывает жертву при разговоре, и задаёт ей личный вопрос, который даёт понять по интонации и тону голоса, подозрительно ли собеседник относятся к разговору, если жертва отвечает на вопрос, то разговор продолжается. Далее проговаривается хорошо продуманная легенда максимально похожая на правду. Также в конце разговора следует спросить ещё 3-4 вопроса для того чтобы растворить подозрения в ненужной информации. Также для успешного развития событий социальному инженеру следует использовать претестинг для сбора информации о жертве, для более эффективного внушения.

Случайная встреча. Случайной встречей называют деятельность специальных нелегальных организаций деятельностью, которых является организация якобы случайной встречи. Первый этап, сбор всевозможной информации об объекте, просчет вариантов комбинаций, действий, которые в конечном итоге сведут объекта в той самой якобы случайной встрече. Для поиска информации используется претестинг, при подборе информации учитывается всё, вкусы, интересы и даже страхи объекта. Как правило, но не всегда, объектами становятся мужчины, происходит эксплуатация симпатии и чувства любви, исходя из первого этапа, определяется, какие девушки ему нравятся, цвет волос, характеристики тела, черты лица, цвет глаз и голос. После чего при помощи психологии прогнозируется действия объекта, в какой-либо ситуации. Второй этап, начало операции, предполагает в себе много вариантность развития событий, и каждый из них давно просчитан. Например, начальник влиятельной фирмы едет на личном автомобиле из дома в свой офис, на обочине стоит якобы «поломанный автомобиль» с девушкой вызывающей эвакуатор. Если объект проезжает мимо, у него «внезапно» повреждается колесо автомобиля, в след за ним едет автомобиль, за рулем которого находилась другая девушка, готовая помочь ему в сложной ситуации. Если не удаётся повредить колесо, автомобиль с девушкой совершает «намеренное дорожно-транспортное пришествие», что приводит к нужному результату, знакомству с объектом.

Рейдерские захваты. Рейдерский захват - захват бизнеса путём рейдерства и применения корпоративного шантажа или гринмэйла. Гринмэил – продажа пакета акций по цене значительно превышающую рыночную стоимость, под угрозой шантажа или обещанием провести рейдерский захват в их отношении[3]. Первый этап, сбор информации об организации (объекте), на данном этапе также используется все вышесказанные приёмы социальной инженерии для поиска такой информации как общее финансовое состояние предприятия, список акционеров, список конкурентов и т.д. Второй этап, скупка миноритарных акций предприятия путём гринмэйла. Одновременно со скупкой акций происходит так называемое «закошмаривание» предприятия путём нарушения его работы или дезорганизации управления. Все это ведёт к резкому увеличению количества акционеров желающих как можно быстрее избавиться от сомнительных акций. Третий этап. Раскол предприятия. Главной задачей первых двух этапов состоит в получении 30%+1 акций, дабы иметь свободный вход на предприятие, но консолидированный пакет всё ещё находиться в руках у руководства предприятия. Одновременно идёт процесс формирования оппозиции из остальных миноритарных акционеров и создание раскола интересов между руководителями предприятия. Действия руководства при этом сводятся к смягчению конфликта между руководителями, попытки задобрить оппозицию, выполняя из требования. Четвёртый этап, как только есть беспрепятственный вход на предприятие, т.е. возможность участвовать в управлении, рейдер инициирует внеочередное собрание акционеров. В случае игнорирования созыва со стороны руководства, рейдер в праве самостоятельно провести его, на нем принимаются решающие

вопросы, связанные с управлением предприятия. Последующий шаг является одним из важнейших, один из участников собрания акционеров, под руководством рейдера отправляет претензию к проведению того самого собрания в суд для признания его недействительным. Повод к претензии обязательно должен быть незначительным чтобы суд при рассмотрении претензии признал её формальностью и отказал рейдеру в его претензии, излагая свой ответ на официальном документе, этот документ и будет доказательством того что собрание было легитимным и государство в лице судьи это подтверждает и рейдер окончательно поглощает предприятие.

Волк в овечьей шкуре – один из популярных способов кражи информации у конкурентов считается отправление так называемого «волка в овечьей шкуре» т.е. специально обученного человека, который, проходит собеседование и трудоустраивается менеджером на якобы «продолжительное» время в конкурирующую фирму. После чего он прорабатывает испытательный срок, чаще всего его продолжительность не превышает 3-4 месяцев, и получает доступ во все интересующие его места хранения информации, оперативно копирует или же фотографирует её для дальнейшей передачи своим настоящим начальникам. После того как вся важная информация о конкурентах была собрана, сотрудник благополучно заявляет о своём увольнении из данной фирмы в связи с непредвиденными выдуманными обстоятельствами, не вызывающих подозрений со стороны руководства.

Литература

1. Орлова Л.В. Модель формирования инжиниринговых центров на базе социальной инженерии. Globus. 2019. № 10 (43). С. 30-32.

2. Артемов О.Ю., Овчинников С.А. Социальная инженерия как главная проблема обеспечения информационной безопасности. В сборнике: Проблемы управления безопасностью сложных систем. Материалы XXVII международной конференции. Под общей редакцией Калашникова А.О., Кульбы В.В. 2019. С. 208-214.

3. Пазухина А.П. Социальная инженерия, ее техники и меры противодействия. Молодой ученый. 2019. № 22 (260). С. 61-62.

Сведения об авторах

Иванов Вячеслав Юрьевич, кандидат технических наук, доцент, начальник кафедры информационной безопасности УНК ИТ Московского университета МВД России им. В.Я. Кикотя;e-mail:ivsl71@mail.ru.

Иванова Анастасия Вячеславовна, студентНационального исследовательского технологического университета«МИСиС»;e-mail:nastas1999@mail.ru.

Иванов Игорь Петрович

ПРОБЛЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ

Накопление и использование информатизации о лицах совершающих преступления всегда было и остается одним из основных источников раскрытия преступлений. С начала 90-х годов прошлого столетия, сотрудники органов стали заботиться о сохранности различных видов информации на компьютере, в том числе и об информации, качественно улучшающей процесс управления. Сотрудники органов внутренних дел, обладающие необходимой информационной культурой, считаются основой квалифицированных кадров МВД России. Учебный процесс образовательных организаций министерства внутренних дел России направлен в первую очередь на подготовку квалифицированных специалистов, освоивших в полном объеме и подтвердившие в процессе обучения свои квалификационные требования.

Количество информационных ресурсов в обществе регулярно растет, а приобретенные умения и навыки по производству поиска и использования информации в профессиональной деятельности регулярно изменяются. Государство обновляет концепции и стратегии развития информационного общества, на основе изменяющейся ситуации в мире. Задачи по привитию навыков работы обучающихся с информацией и с современными информационными технологиями в образовательных учреждениях на протяжении многих лет считаются приоритетными.

В 2014 году в органах внутренних дел внедрен электронный документооборот, который позволил сократить время от разработки нормативно правовых актов, до ознакомления сотрудников с ними на рабочих местах. За это время не был утрачен ни один документ. Развитие информационных систем и информационных технологий постоянно и быстро находит соответствующее внедрение не только в органах внутренних дел, но и практически во всех сферах жизнедеятельности человека. Это доказывает, что деятельность человека в значительной мере подчинена современным информационным технологиям.

В 2016 году органы внутренних дел перешли на новую ступень развития телекоммуникационных технологий, что имеет положительные тенденции развития скорости обработки и уменьшения времени обращения к информационным ресурсам банков данных МВД различных сфер деятельности. А вот учебные организации МВД России, некоторые новшества информационных технологий практически обошли стороной. Трудно представить современного юриста не умеющего пользоваться достижениями информационных технологий. Качественная организация учебно-познавательной деятельности – это основная функция образования. В 2020 году произошло одно из основных необратимых событий – переход всей сферы информатизации органов внутренних дел на новое современное отечественное программное обеспечение. Большинство сотрудников и преподавателей ранее не сталкивались с аналогом программного обеспечения. Только после установки программного обеспечения, пользователи компьютерной техники начинают задумываться о возникающих проблемах.

Программное обеспечение изменилось фундаментально. Те программные продукты, к которым привыкли сотрудники и обучающиеся, просто перестали работать на современном программном обеспечении. Необходимо срочно было искать альтернативу. Аналоги программного обеспечения, несомненно, существуют, но не в полной мере могут перекрыть все потребности образовательного процесса.

Нельзя сказать, что все сотрудники нормально и положительно восприняли этот переходный процесс. Только начали привыкать к особенностям нового программного обеспечения, как карантин заставил всех людей, кардинально изменить свой образ жизни. Курсанты, слушатели, преподаватели и весь персонал образовательных учреждений не в полной мере были готовы к переходу системы образования на дистанционную форму работы.

Кто-то освоился очень быстро и теперь качественно справляется с измененными профессиональными обязанностями.Преподавательскому составу в этой смене приоритетов повезло меньше. Преподавателям пришлось полностью изменять формат привычных занятий, вместе с освоением новых современных информационных технологий. Применяя возможности нового программного обеспечения, приходится маневрировать с вовлечением обучающихся и на основе «старого» программного обеспечения, чтобы качественно наладить и правильно организовать учебный процесс. В силу различных факторов, у обучающихся на домашних компьютерах не установлено отечественное программное обеспечение. За два месяца привыкания к дистанционному обучению, преподавательскому составу приходится регулярно корректировать и налаживать процесс обучения.

Преподаватели в процессе домашнего обучения столкнулись с массой проблем, которые значительно усложняют им работу. Обучающихся практически невозможно контролировать и следить за самостоятельным процессом выполнения заданий. Для этого приходится уменьшать время, отведенное для приобретения практических навыков и проводить онлайн опросы, позволяющие определить качество и самостоятельность выполненных работ.

Во время удаленного обучения преподаватели столкнулись с проблемами, которые усложняют им работу. Первая проблема – подготовка учебного материала. Некоторые обучающиеся перешли на программное обеспечение «AstraLinux», а большинство по разным объективным причинам остались на платформе «Windows7», «Windows8», а некоторые – на «Windows10». Вроде одноименные платформы и имеют не существенные отличия, хотя разрабатываемый материал иногда только на половину соответствует действительности. Данное направление дает возможность обучающимся импровизировать при выполнении разработанных заданий. Это повышает процесс нахождения соответствий и более осмысленно запоминается ими.

Вторая проблема – видеоуроки. Подготовка видео лекций практически стала прерогативой преподавателей. Для создания и обработки видеолекций, преподаватели быстро освоили все возможные программные продукты. Хотя существует возможность записи видеолекций онлайн,но тогда возникают дополнительные вопросы: качество изображения при передаче информации, или как записать содержимое презентации с ее озвучиванием. Программные продукты, которые используются преподавательским составом в настоящее время для записи видеофильмов, чаще всего работают на платформе «Windows». В связи с этим затруднена процедура просмотра некоторых форматов видеоизображений в «AstraLinux» или при работе с планшета без операционной среды «Windows».

Большинство преподавателей для объяснения нового материала или решения задач, не преминут воспользоваться видеосвязью. Данное действие аналогично восприятию обстановки в учебной аудитории и позволяет установить зрительный контакт с преподавателем. Проблема проведения видеозанятий в режиме онлайн, тоже имеет свои особенности и недостатки. После начала работы большинство преподавателей самостоятельно выбирали платформу для проведения занятий. Одни отдали предпочтение Zoom, другие выбрали Webex и другим. Эти две основные системы, которыми пользуются корпоративные клиенты для проведения вебинаров в настоящее время. К данным технологиям необходимо было привыкнуть. И вот когда все стало получаться, появилось нововведение – переходить на программу «TrueConf». И к чему мы пришли? Первое: для проведения большого количества занятий – необходимо иметь очень мощный сервер. Второе: качество изображения во время занятия практически невозможно прочитать на экране монитора. И третье – невозможно отслеживать процесс выполнения заданий обучающимися в онлайн режиме. Преподаватели и из данной ситуации нашли выход. Для совместного разбора задания преподаватель и курсант запускают одновременно одинаковое приложение. Затем в режиме диалога, один выполняет и рассказывает другому или всемсразу, что и как делает, а главное, что у него получается. Еще один не очень приятный момент – регулярная проверка заданий во время урока и выставление оценок. Данное действие отнимает возможность работы обучающихся с заданием до 20 минут занятия. Четверть урока (из 90 минут), преподаватель проверяет задания и комментирует найденные ошибки и недочеты. Прямые трансляции трудно контролировать, как преподавателю, так и обучающимся.Наличие маленьких детей в доме, тоже может поставить преподавателя в неловкую ситуацию.

Третья проблема – представление обратной связи. Часто бывают неполадки с подключением к конференции или невозможность устойчивой связи. Возникновение

вопросов у обучающихся – это тоже не совсем приятное действие, во время проведения занятий. Хорошо если вопросов немного, и они у разных обучающихся возникают в порядке очередности. Если вопросов много особенно по незнакомой тематике, тогда прподаватель только успевает давать пояснения. Одни спрашивают, другие ждут своей очереди, чтобы задать вопрос. Главное преподавателю не тратить много времени на ответ. Другое дело, когда требуется проверить и написать десятки комментариев к выполненным работам. Это отнимает много времени и не входит в процесс обучения.

Четвертая проблема – качество проверки заданий. Обучающихся трудно контролировать во время выполнения заданий: что и как он делает, и кто ему в этом помогает или делает задание за него. При сохранении выполненного задания в «Облако» у многих возникают проблемы с повторным доступом к области хранения информации. Некоторые обучающиеся не своевременно предоставляют задания для проверки, что дополнительно увеличивает время проверки заданий и выставления оценок. Положительное решение данной проблемы заключается в следующем: можно задавать задания на самостоятельную подготовку, а на занятии проводить защиту и объяснение выполняемых работ. Иногда обучающиеся представляют на проверку чужие работы. Для этого необходимо запоминать все проверенные результаты работ и типичные ошибки или разрабатывать индивидуальные задания.

Кроме основных проблем, существуют еще множество различных ситуаций: проспал, не включается компьютер, выключили свет, плохое Интернет соединение, не установлено программное обеспечение, не открывается или не запускается файл, антивирусная программа заблокировала установку программы или копирование исполняемых файлов из сети Интернети многое другое.

Несмотря на то, что общество живет современными технологиями, некоторые обучающиеся не имеют дома компьютера с доступом к Интернету, а со смартфона программы не работают или работают в онопользовательском режиме. Как в данном случае организовать обучение? Это риторический вопрос и ответ может быть совершенно разным. Одни практикуют индивидуальные беседы, тогда остальная аудитория остается без внимания педагога. Вторые – заставляют делать письменные работы и проверяютиллюстрации заданий, написанные вручную.

Несмотря на существующие проблемы, дистанционное обучение сегодня продиктовано действительностью, и хотим мы этого или не хотим, а нам всем придется подстраиваться к реалиям времени и совместно решать возникающие трудности.

Не новая, но совершенно неожиданная и непривычная форма обучения стала настоящим испытанием на прочность, не только среди педагогов, но и среди обучающихся и их родителей. Да существует множество претензий по поводу дистанционного обучения, но необходимо во всех ситуация, даже иногда неприятных, находить положительные моменты и эмоции, а также выбирать позитивные моменты из приобретенного неоценимого опыта.

Можно утвердительно сказать, что «новый формат» работы преподавателя – это не только определенные трудности, которые необходимо преодолевать, но и масса новых впечатлений и возможностей, привыкнув к которым обучение становится на новый виток развития. Озвученные и правильно решенные проблемы, позволят углубить информационную подготовку не только обучающихся, но и преподавателей, а также усилить ее практическую направленность.

Сведения об авторе

Иванов Игорь Петрович, кандидат педагогических наук, доцент, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: iv_on_off@mail.ru.

Ивличев Павел Сергеевич

НЕЗАКОННЫЕ МЕТОДЫ СНИЖЕНИЯ ИЗДЕРЖЕК В ПРОЦЕССЕ КРИПТОВАЛЮТНОГО МАЙНИНГА

Понятие криптовалюты появилось в обиходе в начале XXI века и довольно быстро приобрело известность в широких кругах, в том числе, далеких и от финансового мира, и от информационной сферы. Законодательного регулирования криптовалютного рынка на территории России, тем не менее, до сих пор не существует, что не мешает функционированию этого средства платежа в нашей стране.

Под термином криптовалюта в настоящее время понимают некий денежный суррогат (или электронные деньги), который функционирует на основе полностью автоматической децентрализованной системы[5]. В отличие от полностью легально функционирующих средств электронного перевода денег, ключевой особенностью криптовалютного рынка является отсутствие единого центра, который брал бы на себя подтверждение и обработку транзакций в системе.

Отсутствие единого центра порождает ряд проблем, главной из которых является подтверждение транзакций в системе.Проблема достоверности транзакций в криптовалютной системе достигается с помощью технологии блокчейн – технологии цепочки связанных между собой блоков, хранящих информацию о транзакциях в данном кошельке. Правила построения блоков используют криптографические алгоритмы необратимого шифрования, результат работы которых в виде значений хеш-функции хранится в заголовке блока[1]. Заголовок каждого блока содержит в себе хеш предыдущего блока, поэтому подделка одной транзакции неизбежно влечет за собой подделку и предыдущих транзакций. Технически такая процедура возможна, однако ее практическая реализация приводит к существенным затратам вычислительных мощностей, временных и энергетических ресурсов, поэтому подделка транзакций экономически нецелесообразна.

Кроме того, подделка транзакций может оказаться бессмысленной из-за особенностей функционирования технологии блокчейн, мошенническая транзакция может оказаться побочной в цепочке и быть отмененной уже после ее осуществления.

В технологии блокчейн предшественника не имеет первый блок, который имеет в заголовке только собственный хеш нулевой операции, которая в большинстве криптовалютных систем обозначает выплату вознаграждения (эмиссию криптовалюты). Вознаграждение получает тот, кто принял участие в формировании этого первого блока, являющегося подтверждением транзакций.

Поскольку в криптовалютах используется необратимое шифрование, алгоритмы которого являются на настоящий момент криптостойкими, единственным действенным способом формирования хеша, отвечающего требованиям криптовалютных систем является метод перебора[4]. Поскольку большинство алгоритмов необратимого шифрования разрабатывались с целью обеспечения невозможности восстановления исходной информации, такой перебор требует высокой вычислительной мощности. В случае отсуттсвия единой централизованной системы, достижение такой мощности может достигаться исключительно построением распределенной сети компьютеров, выполняющих операции по проверке и подтверждению транзакций. Процесс такого перебора и получение вознаграждения за его результат на специфическом жаргоне носит название майнинга.

Таким образом, между создателями криптовалютных систем и так называемыми майнерами, возникает некий союз, функционирующий на основе принципов взаимной выгоды: создатели систем пользуются необходимыми для них ресурсами майнеров, а майнеры получают вознаграждение за предоставление своих ресурсов.

Следует отметить, что майнинг криптовалют не является незаконным действием сам по себе, однако с ним связано немало схем откровенно криминальных действий, причем в силу инертности уголовного законодательства, ряд этих действий формально не является уголовным преступлением.

Основой криминального интереса к майнингу криптовалют является стремление лиц, занимающихся поиском первого блока снизить издержки и, как следствие, увеличить свою прибыль. С этой точки зрения майнер подобен предпринимателю, и как предприниматель, майнер нередко балансирует на грани закона.Ситуацию с криминальным интересом в сфере майнинга усугубляет тот факт, что рентабельность майнинга с каждым годом снижается. Это обусловлено следующими причинами:

1. Снижение вознаграждения для лиц, занимающихся майнингом. Так, в 2020 году планируется снижение вознаграждения за один блок популярной криптовалюты биткойн в два раза. В 2019 году размер вознаграждения за майнинг криптовалюты этериум снизился на треть.

2. Спекулятивный рост спроса на оборудование для майнинга. Всплеск интереса к криптовалюте породил спекулятивный спрос и на без того дорогое оборудование для майнинга. Как правило, для майнинга используются графические процессоры топовых настольных систем, стоимость единицы оборудования может достигать 700 долларов США, а для организации криптофермы необходимо несколько таких видеокарт. По разным оценкам, интерес к топовым видеосистемам для организации майнинговых ферм привел в росту цен на видеосистемы до 100%.

3. Высокие переменные издержки. Высокие переменные издержки обусловлены высокими затратами на оплату электрической энергии. Так, простейшая криптоферма на базе четырех видеокарт, может иметь мощность до 800 Вт. Функцирование такой фермы в течение месяца приведет к потреблению электрической энергии на уровне 500 кВтч, что в разы больше потребностей среднестатистической семьи. Этот факт приводит к снижению популярности так называемого домашнего майнинга.

4. Нестабильность курса криптовалют. Поскольку криптовалюта не имеет никакого обеспечения реальными ценностями, ее курс и обращение обусловлены исключительно спросом, который, во многом, носит спекулятивный характер[1].

5. Увеличение количества лиц, занимающихся майнингом криптовалют. Популяризация майнинга привела к значительному росту числа желающих заработать на этом процессе. Поскольку, как уже было сказано, фонд вознаграждений за майнинг регулярно уменьшается, то рост числа участников дополнительно приводит к снижению размера вознаграждения для каждого из них.

В силу этих причин в 2020 году индивидуальный майнинг криптовалют является неактуальным и большинство вознаграждений получаются участниками с помощью так называемого майнинга в пуле.

При таком способе майнинга вычислительная задача поиска первого блока распределяется между всеми участниками, которые регистрируются на специально организованном сервере.

Большинство серверов для майнинга в пуле при определении размера вознаграждения исходят из фактического объема выполненных вычислительных задач, количества участников. Большее вознаграждение получают участники, задействовавшие большие мощности, хотя встречаются и иные подходы.

Одним из способов снижения затрат на процесс майнингаявляется разработка механизмов перекладывания постоянных и переменных издержек на иных лиц.

Эффективным вариантом может являться использование организационной уязвимости серверов майнинга, которые предлагают участникам пула готовые программные решения для различных аппаратных платформ и операционных систем[6].

Такие организационные уязвимости могут возникать как из-за умысла создателей сервисов, так и из-за недоработки алгоритмов. Умысел организаторов может быть связан с тем, что на сервис, позволяющий снизить издержки, пусть даже и криминальным методом, будет привлечено больше желающих участвовать в программе, что приведет к росту комиссионных вознаграждений организаторам, при это все риски лягут на плечи пользователей сервиса.

Примером такого сервиса является сервис Coinhive, закрытый в 2019 году, а также сервисы CoinIMP и Crypto-loot. Следует отметить, что эти сервисы не занимаются какой-либо противоправной деятельностью, предлагая своим пользователям готовые коды программ для майнинга, пригодные для использования в качестве скриптов на веб-страницах. Легальное использование таких скриптов предполагает наличие у пользователя своего сайта или страницы сайта, при просмотре которых в браузере посетителя будет выполнен скрипт по проверке хеша.

Поскольку эти скрипты преимущественно используют технологию JavaScript, то выполнение скрипта будет происходить на ресурсах посетителя сайта. Скрипты имеют настройки, позволяющие регулировать уровень загрузки центрального процессора компьютера посетителя.

Упомянутые сервисы за предоставление кода взимают вознаграждение от 18 до 30% от результата майнинга. Как правило, существует минимальное количество хешей, которые должны быть проверены скриптом.

Указанные сервисы применяются для майнинга криптовалюты Монеро и используют мощности только центрального процессора. Поскольку для майнинга здесь используется обычное оборудование, количество перебираемых хешей в секунду (хешрейт) невелико и на типовых процессорах не превышает 400 хешей в секунду. Учитывая курс Монеро, на заработок одного доллара уйдет около 6 машино-дней. Для того, чтобы владелец сайта мог заработать на майнинге Монеро хотя бы один МРОТ, необходимо, чтобы его сайт в течение часа посещало не менее 14000 человек, что является очень высоким показателем.

Таким образом, желающий заработать на майнинге с помощью скриптов должен иметь сайт с высоким уровнем посещаемости. Однако в этом случае существуют намного более эффективные реферальные программы, обеспечивающие достаточную пассивную монетизацию сайта.

Казалось бы, нерентабельный способ заработка должен был сам сойти на нет в условиях рыночных взаимоотношений, однако, сервисы по скриптовому майнингу Монеро существуют на протяжении долгого времени. Этому способствует криминальный спрос на скрипты для майнинга.

Зарегистрировавшись в программе майнинга, злоумышленники, используя различные механизмы, осуществляют внедрение скриптов на сайты с высоким уровнем посещаемости. В качестве механизмов может выступать как взлом консоли управления сайтом, так и подкуп администратора сайта или использование своего служебного положения [3].

Для увеличения дохода и скрытия скрипта, злоумышленники отключают визуальные элементы и размещают скрипт в таблице стилей в разделах заголовков, чтобы скрипт выполнялся скрытно при открытии любой страницы сайта. Такой способ заработка на жаргоне получил название криптоджекинга, а используемые для него скрипты называют криптомайнерами.

Формально существование сервисов, распространяющих криптомайнеры, не является незаконным. По российскому законодательству криптомайнеры нельзя отнести к вредоносному программному обеспечению, поскольку он задействует ресурсы компь-

ютера, но не приводит к несанкционированному копированию, блокированию, модификации или уничтожению информации.

Вместе с тем ущерб для информационной инфраструктуры общества от использования криптомайнеров может быть значительным – до 70% ресурсов сети может быть использовано злоумышленником для несанкционированного майнинга.

Правовая борьба с сервисами криптомайнинга неэффективна и за рубежом. Так, сервис Coinhive был закрыт создателями только после сильного общественного давления, поскольку правоохранители оказались бессильны. Ответственность за криптоджекинг возникает только в случае, если удается доказать незаконность размещения скрипта на сайте, как это было в Орловской области в 2018 году. Вместе с тем, очевидно, что спрос на криптомайнеры является исключительно криминальным, из-за их экономической неэффективности. В настоящее время наличие криптомайнеров проверяется браузерами и рядом средств антивирусной защиты, однако, рубеж программной защиты здесь является первым, без традиционного и логичного прикрытия правовыми мерами [2].

В связи с этим целесообразной и логичной выглядит нормативное регулирование использования криптомайнеров, для чего может потребоваться корректировка информационного и уголовного законодательства.

Следует отметить также, что в последнее время в сфере крптовалютных систем начал наблюдаться отток лиц, занимающихся майниингом, что заставляет разработчиков этих систем искать другие способы подтверждения транзакций. О таких планах, к примеру, сообщили организаторы криптовалюты Etherium. Отказ от майнинга со стороны организаторов, разумеется, уберет угрозы, исходящие от недобросовестных участников этого процесса, но может породить иные методы мошенничеств на рынке криптовалют.

Литература

1. Давликанова Н.В., Здобникова Г.А. Экономика криптовалюты по технологии блокчейн // Инновационные исследования: проблемы внедрения результатов и направления развития: сборник статей Международной научно-практической конференции. – 2017. – С. 45-47.

2. Ивличев П.С. Анализ актуальных механизмов неправомерного доступа к компьютерной информации: / Ивличев П.С., Ивличева Н.А., Трофимов М.Н. – Рязань, 2019 – 132 с.

3. Ивличев П.С., Ивличева Н.А. Информационные технологии обеспечения безопасности платежных средств в свете современных тенденций в киберпреступности // Экономика и предпринимательство. 2017. № 2-1 (79). С. 135-139.

4. Ивличев П.С., Ивличева Н.А. Обеспечение информационной безопасности в условиях современной криминальной среды: учебное пособие. – Рязань, 2018 – 83 с.

5. Коваленко Д.А., Миллер Е.В. Преимущества, риски и актуальные проблемы криптовалют // Актуальные вопросы развития экономики: материалы Международной научно-практической конференции. – 2017. – С. 153-157.

6. Корнилович Р.А. Информационная безопасность населения как средство противодействия преступности в финансово-кредитной сфере: учебно-методическое (учебно-практическое) пособие / Корнилович Р.А., Ивличев П.С., Ивличева Н.А., Коноваленко С.А., Ребров А.А., Пинчук Л.В. – Рязань, 2017 – 61 с.

Сведения об авторе

Ивличев Павел Сергеевич, кандидат физико-математических наук, доцент кафедры экономической безопасностиМосковского университета МВД России имени В.Я. Кикотя; e-mail: psi940@mail.ru.

Ивличева Наталья Александровна

АНАЛИЗ НАРУШЕНИЙ И ЗЛОУПОТРЕБЛЕНИЙ НА РЫНКЕ КРИПТОВАЛЮТ

В настоящее время криптовалюты получили широкое распространение, несмотря на то, что признание со стороны государственных финансовых институтов, в частности, в России отсутствует.

Причиной популярности в немалой степени является использование технологии блокчейн, которая, с одной стороны, позволяет обеспечить полную прозрачность транзакций, а с другой, гарантирует анонимность и децентрализованность [5].

Блокчейн в криптовалютах представляет собой цепочку транзакций, содержащих сведения об операциях с кошельком криптовалюты. Сведения об операциях хранятся в виде хешей – результатов вычисления функций по алгоритмам необратимого шифрования. Формирование и подтверждение транзакции происходит по алгоритмам асимметричного шифрования, аналогичным тем, которые используются в электронных подписях. В отличие от традиционного механизма подтверждения электронной подписи посредством выдачи сертификатов, при реализации блокчейна в системах криптовалют удостоверяющий центр электронных подписей, а также единая база данных о состоянии криптовалютных кошельков отсутствуют.

Отсутствие единого центра управления кошельками криптовалют порождает явление так называемого майнинга – процесса, необходимого для функционирования криптовалюты.

Именно майнерами вносятся изменения в состояния счетов на основе выполнения вычислительных задач высокой интенсивности. Подтверждение транзакции достигается вычислением первого блока в цепочке транзакций для кошелька, с которого инициировано списание средств [6]. Все майнеры, зарегистрированные в криптовалютной системе, проводят подтверждение транзакций на основе своей локальной базы. Синхронизация баз проводится по мере обмена информацией между участниками майнинга на основе принципа простого большинства.

Исходя из принципа функционирования криптовалюты, возникает очевидное место уязвимости: открытость информации о транзакциях и доступ произвольного количества лиц к блокчейну. Теоретически, это открывает перед злоумышленниками возможность манипулирования данными в блокчейне.

Рассмотрим механизм возможной атаки злоумышленника на кошелек криптовалюты, имеющий целью несанкционированное списание средств.

Абсолютно легально злоумышленник может получить сведения о состоянии счета и блокчейн кошелька, зарегистрировавшись, например, в качестве майнера. Эти сведения доступны в его локальной базе данных, по которой и производится майнинг.

Фактически, злоумышленнику необходимо добавить в блокчейн один блок, причем сделать это легальным способом он не может, поскольку не обладает частным ключом цифровой подписи. В настоящее время все алгоритмы асимметричного шифрования являются абсолютно устойчивыми к операции восстановления частного ключа по публичному, поэтому задача вычисления частного ключа является заведомо невыполнимой [2].

Однако, технология блокчейна и процедура майнинга дают злоумышленнику возможность добавления транзакции путем подбора хеша нулевой транзакции и развертывания всей цепочки блокчейна. Данная операция вполне осуществима, поэтому теоретически в блокчейне может появиться мошенническая транзакция.

Такая транзакция, тем не менее, не приводит к немедленному хищения средств с криптовалютного кошелька, поскольку существует только в локальной базе данных

злоумышленника. Для того, чтобы транзакция была подтверждена, необходимо синхронизировать локальную базу данных с базами данных других майнеров. Попытка синхронизации обречена на провал: данные о транзакции хранятся только в базе данных злоумышленника, остальные базы данных сведения о ней не содержат, поэтому состояние криптовалютного кошелька будет установлено в соответствии с принципом большинства: мошенническая операция будет попросту отсечена от блокчейна [4].

В различных источниках упоминается так называемая «атака 51%», заключающаяся в том, что злоумышленники берут под контроль 51% вычислительной мощности в процессе майнинга системы криптовалюты. Теоретически это означает взятие всех криптовалютных кошельков под свой контроль, однако практическая реализуемость «атаки 51%» крайне маловероятна из-за ее нецелесообразности. Для того, чтобы получить 51% вычислительной мощности, необходимо вложить в майнинг денежные средства, исчисляемые сотнями миллионов долларов. Очевидно, что такие вложения не окупятся: по мере реализации атаки пользователи криптовалютных кошельков будут закрывать свои счета, что приведет к обвалу курса криптовалюты на бирже. Иной же стоимости, кроме спекулятивной, криптовалюты не имеют.

Таким образом, система криптовалюты, несмотря на теоретическую уязвимость, является вполне безопасной [3].

Понимая невозможность атаки на систему в целом, злоумышленники обращают свое внимание на ее составные части и процедуры функционирования.

Кошелек криптовалюты по сути является парой ключей асимметричного шифрования. Публичный ключ необходим для перевода криптовалюты на счет, частный – со счета. Практическая реализация кошельков может быть различной, распространены два варианта:

1. Локальный кошелек. Реализуется в форме программы, хранит всю информацию о блокчейнах системы (несколько гигабайт), требует синхронизации с базами майнеров. В этом случае частный ключ хранится на локальном компьютере пользователя и не доступен из глобальной сети.

В этом случае пользователь несет на себе риски утраты ключа, связанные с выходом из строя его оборудования. Локальные кошельки, как правило, не имеют механизмов восстановления доступа.

2. Веб-кошельки. Создаются на серверах глобальной сети. Доступ к веб-кошельку осуществляется с помощью пары логин-пароль, частный ключ хранится на сервере, публичный ключ может быть реализован различными способами, например, в форме QR-кода.

Данная система более надежна с точки зрения защиты от непреднамеренных угроз, поскольку базы данных серверов регулярно копируются, кошельки имеют средства восстановления доступа. К тому же веб-кошельки позволяют быстрее производить транзакции и синхронизировать базы данных.

К сожалению, именно веб-кошельки чаще всего становятся целью злоумышленников. В настоящее время существует масса способов незаконного получения пары логин-пароль, а многие популярные веб-кошельки до сих пор предлагают этот способ идентификации клиента по умолчанию.

Для получения данных идентификации разрабатываются вредоносные программы класса PSW, разрабатываются механизмы фишинга [1].

Популяризация криптовалют в мире привела к тому, что к операциям с ними стали привлекаться лица с низкой грамотностью в области информационных технологий, не понимающие принципов функционирования асимметричного шифрования. В настоящее время стали регистрироваться случаи, когда кошельки оформляются через посредника, который в качестве средства доступа передает клиенту не частный, а публич-

ный ключ, не сообщая иных данных идентификации. С помощью публичного ключа клиент имеет возможность просмотра состояния «своего» кошелька, может покупать криптовалюту на бирже, но правом вывода средств в данном случае обладает мошенник-посредник.

Также целью мошенников является процедура майнинга, без которой существование многих криптовалют невозможно.

В связи с ростом издержек на майнинг и постоянно сокращающимся размером вознаграждения за участие в этой процедуре, популярность получила так называемая облачная схема майнинга, в которой участники не покупают своего оборудования, а оплачивают издержки уже функционирующей фермы для майнинга.

Привлекательность облачного майнинга объясняется его понятностью для обывателя, доступностью и низкой стоимостью вхождения в проект. При этом немногие понимают размер реальной отдачи от таких инвестиций, что играет на руку злоумышленникам, которые организуют фальшивые облачные сервисы майнинга по принципу финансовых пирамид.

Мошенническая активность регистрируется также на сервисах майнинга в пуле. Особенностью такого майнинга является присоединение личного оборудования для майнинга к вычислительному серверу. Таким образом из локального оборудования участников создается распределенная сеть, вознаграждение в которой выплачивается пропорционально использованным мощностям. Мошенники различными способами искажают статистику для получения незаслуженного вознаграждения.

Следует отметить, что в настоящее время существуют и иные способы заработка криптовалюты, не связанные с трейдингом или майнингом. Речь идет о так называемых «кранах» – партнерских программах, предлагающих вознаграждение в криптовалюте за выполнение различных задач. Как правило, это несложные задания, похожие на опросы или лотереи. Доход владельцев кранов образуют рекламные отчисления от партнеров, часть из которых и распределяется среди участников.

Среди распространенных методов обмана наиболее популярным является отказ в выводе заработанных средств под различными предлогами. Также популярно среди злоумышленников выставление невозможных условий для перевода денег [7].

Более масштабные атаки связаны с атаками на криптовалютные биржи – частные организации, занимающиеся обменом реальных денежных средств на средства в криптовалюте. Деятельность таких организаций в большинстве случаев не регулируются законами, в силу непризнания или ограниченного признания понятия криптовалюты. Кроме того, организаторы валютных бирж берут на себя значительные риски, связанные с обвинением в отмывании денежных средств, поскольку на криптовалюты имеется сильный криминальный спрос.

Правовая незащищенность криптовалютных бирж приводит к тому, что вложения денежных средств на биржах довольно рискованы.

Первая группа рисков связана с возможностью манипулирования данными в таких системах. Все транзакции проводятся полностью в электронном виде, поэтому программное обеспечение для их осуществления должно отвечать высочайшим требованиям информационной безопасности, что далеко не всегда так. Программное обеспечение нередко содержит уязвимости программных компонентов, что позволяет проводить атаки различных типов, включая инъекции. Так, биржа BTC-E пострадала от действия злоумышленника, имитировавшего пополнение своего счета и осуществлявшего сделки за счет реально несуществующих денежных средств. В этом случае биржа, стараясь спасти свою репутацию, взяла возмещение ущерба на себя, однако это является скорее исключением из правил.

Вторая группа рисков связана с манипулированием сделками. Такое встречается и на легальных биржах, однако, в случае торговли сырьем или ценными бумагами, можно объективно оценить масштабы финансового пузыря, опираясь на знания в области экономики. В случае криптовалютных бирж специалистов, способных распознать манипулирование сделками с целью повышения или понижения курса, немного, что позволяет злоумышленникам на фоне созданного ими информационного шума проводить сделки, выгодные им и не соответствующие их реальной стоимости.

Наконец, третья группа рисков связана с возможностью полной утраты денежных средств из-за закрытия криптовалютной биржи. Причинами закрытия могут выступать как действия государства (блокирование сайта, уголовное преследование организаторов биржи), так и действия иных лиц (постоянные атаки на отказ в обслуживании, шантаж, угрозы). Из-за правовой незащищенности этого вида деятельности, конечными потерпевшими являются рядовые вкладчики, возмещение ущерба со стороны организаторов биржи, криминальных структур или государства в данном случае ожидать не приходится.

Резюмируя изложенное, можно сделать вывод. Механизм функционирования криптовалют достаточно стоек к глобальным воздействиям, однако, использование криптовалюты, участие в трейдинге и майнинге требуют от пользователя определенного уровня информационной культуры, без которого противостоять нарушениям в этой сфере будет достаточно проблематично. Кроме того, очевидно, требуется правовая регуляция деятельности криптовалютных бирж.

Литература

1. Ивличев П.С. Анализ актуальных механизмов неправомерного доступа к компьютерной информации: / Ивличев П.С., Ивличева Н.А., Трофимов М.Н. – Рязань, 2019 132 с.

2. Ивличев П.С., Ивличева Н.А. Обеспечение информационной безопасности в условиях современной криминальной среды: учебное пособие. – Рязань, 2018 – 83 с.

3. Колесникова Е.Н. Современные подходы к развитию форм и методов экономического контроля // Социально-экономические и правовые меры борьбы с правонарушениями: Материалы научно-практической конференции. – Рязань, РФ МосУ МВД России, 2012. – С. 35-43.

4. Корнилович Р.А. Информационная безопасность населения как средство противодействия преступности в финансово-кредитной сфере: учебно-методическое (учебно-практическое) пособие / Корнилович Р.А., Ивличев П.С., Ивличева Н.А., Коноваленко С.А., Ребров А.А., Пинчук Л.В. – Рязань, 2017 – 61 с.

5. Липатов Е.В., Лобудеев П.Д. Криптовалюта: понятие, сущность и классификация // Проблемы и перспективы развития современной науки: Материалы Международной (заочной) научно-практической конференции – 2017. – С. 118-126.

6. Целищев П.Б., Коречков Ю.В. Сущность криптовалюты. Процесс эмиссии криптовалют // Молодая наука-2015: Сборник материалов шестой региональной научной конференции студентов и аспирантов. – 2015. – С. 198-203.

7. Ивличев П.С., Ивличева Н.А. Информационные технологии обеспечения безопасности платежных средств в свете современных тенденций в киберпреступности // Экономика и предпринимательство. 2017. № 2-1 (79). С. 135-139.

Сведения об авторе

Ивличева Наталья Александровна, кандидат физико-математических наук, доцент кафедры экономической безопасности Московского университета МВД России имени В.Я. Кикотя; e-mail: ivlichevy@yandex.ru.

Михайленко Евгений Владимирович

ПРИНЦИПЫ АВТОМАТИЗАЦИИ ПОДБОРА И ПРОВЕРКИ ПРАКТИЧЕСКИХ ЗАДАНИЙ, ВКЛЮЧАЮЩИХ ОБРАБОТКУ ПОЛИНОМОВ

При изучении математических дисциплин курсантами, обучающихся по экономическим и информационно-техническим специальностям, часто решаются типовые задачи, включающие обработку полиномов одной или нескольких переменных различных степеней[1]. Разрабатывая аогоритмы компьютерных программ, не всегда удается построить прорстой и лаконичный вычислительный процесс. Часто для формирования заданий необходимо использовать массивы числовых и текстовых данных, разветвляющиеся и циклические структуры, учитывать ряд ограничений и связей [7, 8, 9].

Особенность генерирования таких заданий заключается в совместной обработке специальным образом структурированных числовых массивов, содержащих коэффициенты многочленов [6, 10]. Рассмотрим методы обработки многочленов на примере практической работы «Операции над многочленами» раздела «Многочлены».

Достаточно простой проблемой, с которой пришлось столкнуться разработчикам, оказался вывод многочленов на лист MSExcel [4]. На рисунке 1 представлено сгенерированное первое задание «Вычислить сумму многочленов».

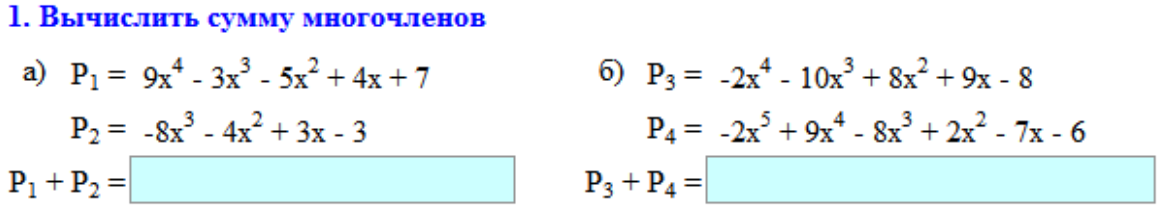


Рис. 1. Задание «Вычислить сумму многочленов».

Для генерации коэффициентов полиномов *P1* и *P2* четвертой и третьей степени соответственно (рис. 2) используем циклы, в которых рассчитываемые коэффициенты многочленов принимают значения в интервале от -10 до 10. С использованием нестандартной функции *pol* многочлены выводятся на лист [3].

```
' Задание 1
' Вычислить сумму многочленов
Erase P1
For i = 0 To 4
  P1(i) = Rnd(v) * 20 - 10
Next i
pol1 = pol(P1, 10, 3)
Erase P2
For i = 0 To 3
  P2(i) = Rnd(v) * 20 - 10
Next i
pol2 = pol(P2, 12, 3)
```

Рис. 2. Программный код задания «Вычислить сумму многочленов».

Рассмотрим процедуру вывода многочленов (рис. 3). Вызываемая в программе функция pol формирует строку, включающую коэффициенты многочлена, обозначения переменных, степени переменных и арифметические знаки «+» либо «–». Местоположение переменных в записи фиксируется в массиве *ms*, и после вывода полинома на лист определяется надстрочный шрифт для степеней переменных [2].

```
Function pol(p, R, c)
Dim ms(30) As Integer
t = ""
k = 0
For i = 30 To 1 Step -1
  If p(i) <> 0 Then k = k + 1

  If p(i) < -1 And k = 1 Then t = t + " " + Str(p(i))
  If p(i) < -1 And k > 1 Then t = t + " - " + st(-p(i))

  If p(i) = -1 And k = 1 Then t = t + " -"
  If p(i) = -1 And k > 1 Then t = t + " - "

  If p(i) = 1 And k = 1 Then t = t + " "
  If p(i) = 1 And k > 1 Then t = t + " + "

  If p(i) > 1 And k = 1 Then t = t + Str(p(i))
  If p(i) > 1 And k > 1 Then t = t + " + " + st(p(i))
  If p(i) <> 0 Then
    t = t + "x"
    If i > 1 Then
      t = t + st(i)
      ms(i) = Len(t)
    End If
  End If
Next i
If p(0) < 0 Then t = t + " -" + Str(-p(0))
If p(0) > 0 Then t = t + " +" + Str(p(0))
Cells(R, c) = t

For i = 30 To 2 Step -1
  If ms(i) > 0 Then Cells(R, c).Characters(ms(i), _
                    Len(st(i))).Font.Superscript = True
Next i
End Function
```

Рис. 3. Функция вывода полинома.

При проверке решения данного задания процедура генерации коэффициентов многочленов *P1* и *P2* остается без изменений (рис. 4).

```
' Задание 1 (Проверка)
' Вычислить сумму многочленов
Erase P1
For i = 0 To 4
  P1(i) = Rnd(v) * 20 - 10
Next i
Erase P2
For i = 0 To 3
  P2(i) = Rnd(v) * 20 - 10
Next i
p = polsum(P1, P2, Pr)
tz = Cells(14, 3)
tz = ubr_prob(tz)
t = poltext(Pr)
t = ubr_prob(t)
If t = tz Then mark = mark + 1 Else Cells(14, 3) = krest(14, 3)
```

Рис. 4. Проверка задания «Вычислить сумму многочленов.

С помощью функции *polsum* осуществляется сумма полиномов *PR = P1 + P2*. В строковую переменную *tz* считывается ответ обучаемого и из нее удаляются пробелы. С помощью функций *poltext* и *ubr_prob* происходит преобразование найденного решения. Затем происходит сравнение рассчитанного решения *t* и считанного *tz*. В случае

равенства значений *t* и *tz* к количеству набранных баллов *mark* добавляется балл, в противном случае поле с неверным решением зачеркивается.

Часто для подготовки заданий следует идти от обратного: сначала необходимо сгенерировать решение задачи, а затем на основе готового решения формировать условие задачи [5]. Рассмотрим процесс генерации и проверки задания 7.б «Разложить многочлены на множители» (рис. 5). Суть задания заключается в том, чтобы при разложении полинома *n*-й степени все *n* множителей-одночленов имели целые коэффициенты. Случайным подбором коэффициентов разлагаемого полинома здесь не обойтись, следовательно, их нужно специальным образом рассчитать.

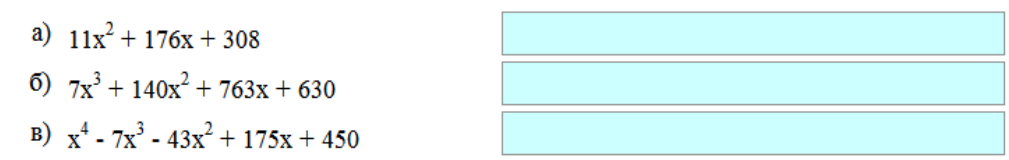


Рис. 5. Задание «Разложить многочлены на множители».

Для формирования выводимого полинома (рис. 6) после очистки массивов *P1*, *P2*, *Pr* и *R* в цикле *Do .. Loop Until* сгенерируем все его корни: x_1, x_2, x_3, а также коэффициент *a*. Осуществим проверку на то, чтобы кони не повторялись. Воспользуемся теоремой Виета для расчета коэффициентов искомого полинома. В случае многочлена третьей степени $ax^3 + bx^2 + cx + d$ его коэффициенты можно найти из произведения одночленов на старший коэффициент: $a(x - x_1)(x - x_2)(x - x_3)$. Результирующий полином *Pr* выводится на лист формы заданий.

```
'Задание 7.б. Разложить на множители
Erase P1: Erase P2
Erase Pr: Erase R
Do
  x1 = Rnd(v) * 20 - 15      '1-й корень
  x2 = x1 + Rnd(v) * 10 + 1 '2-й корень
  x3 = x2 + Rnd(v) * 10 + 1 '3-й корень
  a = (-1) ^ v * Rnd(v) * 10 + 2
Loop Until x1 * x2 * x3 <> 0 And Abs(x1) <> Abs(x2) _
                             And Abs(a) > 1 And x3 < 20

P1(1) = 1: P1(0) = -x1: R(0) = a
p = polmult(P1, R, P2)
R(1) = 1: R(0) = -x2
p = polmult(P2, R, P1)
R(1) = 1: R(0) = -x3
p = polmult(P1, R, Pr)
polr = pol(Pr, 58, 2)
```

Рис.6. Программный код генерации задания «Разложить многочлены на множители».

Произведение многочленов производится последовательно с помощью разработанной функции *polmult* (рис. 7). Функция предназначена для умножения двух многочленов. Степень множителей ограничена числом 15 только из потребностей обучения и ее легко можно увеличить. Итерационный процесс осуществляется в двух вложенных циклах, где параметры внешнего цикла *i* и внутреннего цикла *j* являются степенями мономов, входящих в первый и второй многочлены соответственно.

```
Function polmult(P1, P2, pm)
Erase pm
For i = 0 To 15
  For j = 0 To 15
    pm(i + j) = pm(i + j) + P1(i) * P2(j)
  Next j
Next i
End Function
```

Рис. 7. Функция произведения полиномов *polmult*.

Алгоритм расчета параметров условия задания во время проверки ничем не отличается от того, что был во время генерации (рис. 8) [11]. В вычислении коэффициентов полинома *b, cud* нет потребности, однако зная корни многочлена x_1, x_2, x_3 и коэффициент *a*, по теореме Виета сформируем строку произведений вида $a(x - x_1)(x - x_2)(x - x_3)$, и сравним ее с решением курсанта.

```
'Задание 7.б. Разложить на множители
Erase P1: Erase P2          'Проверка
Erase Pr: Erase r
Do
  x1 = Rnd(v) * 20 - 15     '1-й множитель
  x2 = x1 + Rnd(v) * 10 + 1 '2-й множитель
  x3 = x2 + Rnd(v) * 10 + 1 '3-й множитель
  a = (-1) ^ v * Rnd(v) * 10 + 2
Loop Until x1 * x2 * x3 <> 0 And Abs(x1) <> Abs(x2) _
                             And Abs(a) > 1 And x3 < 20
t = st(a) + "(x "
If x1 < 0 Then
        t = t + " + " + st(Abs(x1)) + ")(x"
    Else
        t = t + " - " + st(Abs(x1)) + ")(x"
End If
If x2 < 0 Then
        t = t + " + " + st(Abs(x2)) + ")(x"
    Else
        t = t + " - " + st(Abs(x2)) + ")(x"
End If
If x3 < 0 Then
        t = t + " + " + st(Abs(x3)) + ")"
    Else
        t = t + " - " + st(Abs(x3)) + ")"
End If
tz = Cells(58, 10)
tz = ubr_prob(tz): t = ubr_prob(t)
If t = tz Then mark = mark + 1 Else Cells(58, 10) = krest(58, 10)
```

Рис. 8. Программный код проверки задания «Разложить на множители.

Описываемый в статье программный продукт успешно используются в учебном процессе Краснодарского университета МВД России при изучении дисциплины математика для проведения практических занятий с курсантами, обучающимися по специальностям 38.05.01 Экономическая безопасность и 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

Литература

1. Булгаков, В.В. Структурно-методическая модель компьютерной программы контроля теоретических знаний курсантов /В.В. Булгаков // Открытое образование (Научный журнал). – М.: Российский экономический университет имени Г.В. Плеханова, 2018. – Том 22, №3. С. 4 – 13.

2. Лаптев, В.Н. О технологиях разработки программных приложений для генерирования и проверки практических заданий по математическим дисциплинам /В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2020. – №01(155). С. 164 – 177. – IDA [article ID]: 1552001013. – Режим доступа: http://ej.kubagro.ru/2020/01/pdf/13.pdf, 0,875 у.п.л.

3. Лаптев, В.Н. Некоторые аспекты применения среды Visual Basic for Application для создания учебных приложений по математическим дисциплинам /В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №09(103). С. 222 – 233. – IDA [article ID]: 1031409014. – Режим доступа: http://ej.kubagro.ru/2014/09/pdf/14.pdf, 0,75 у.п.л.

4. Михайленко, Е.В. О разработке программных приложений для генерации и проверки заданий к практикуму по разделу «Дискретная математика» дисциплины математика // Е.В. Михайленко // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина, – 2019. С. 20 – 27.

5. Михайленко, Е.В. К вопросу об использовании информационных технологий приорганизации самостоятельной работы обучающихся /Е.В. Михайленко, И.Н. Старостенко // Проблемы современного педагогического образования. – Сборник научных трудов. – Ялта: РИО ГПА, 2019. – Вып. 65. – Ч. 1. С. 257 – 262.

6. Михайленко, Е.В. Общие принципы автоматизации подбор заданий и проверки выполненных курсантами работ по математическим дисциплинам /Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XIV Всерос. науч.-практ. конф., 21 июня 2019 г. / редкол.: И. Н. Старостенко, Е. В. Михайленко, С.К. Ефремов, А. А. Хромых. – Краснодар: Краснодарский университет МВД России, 2019. С. 122 – 127.

7. Крыгин, С.В. Особенности преподавания дисциплин информационного цикла при реализации программ дополнительного профессионального образования /С.В. Крыгин С.В., С.Н. Сухов // Передовой опыт и проблемы профилизации учебной, учебно-методической и научно-исследовательской деятельности в образовательных организациях системы МВД России: доклады участников Всерос. Науч.-практ. конф. – Нижний Новгород: Нижегородская академия МВД России, 2019. С. 156 – 162.

8. Жукова, П.Н. Использование информационных технологий в системе ведомственного образования на современном этапе (на примере БЕЛ ЮИ МВД России имени И.Д. Путилина) /П.Н. Жукова, А.Н. Прокопенко, А.А. Гуржий // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 4-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина, – 2018. С. 3 – 12.

9. Старостенко И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

10. Старостенко И.Н. Место и роль электронного обучения в образовательном процессе / И.Н. Старостенко // Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности. –

Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2016. –С. 17-23.

11. Старостенко И.Н. Актуальные вопросы информатизации образования / И.Н. Старостенко // Общество и право. – Краснодар: Краснодарский университет МВД России, 2017. – №4 – С. 274-277.

Сведения об авторе

Михайленко Евгений Владимирович, кандидат физико-математических наук, доцент, заместитель начальника кафедры информатики и математики Краснодарского университета МВД России; e-mail: evmikhaylenko@mail.ru.

МорсаковаЮлия Владимировна

О СПЕЦИФИКЕ РАЗРАБОТКИ ДИСТАНЦИОННЫХ КУРСОВ В РАМКАХ ПЕРЕХОДА ОТ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ К ДИСТАНЦИОННОЙ

Дистанционное обучение – это получение образовательных услуг без посещения учебного заведения с помощью современных педагогических и информационных технологий, систем телекоммуникации.

Для создания дистанционных курсов, по нашему мнению, наиболее удачным выбором является электронная информационно-образовательная среда на платформе Moodle (модульная объектно-ориентированная динамическая учебная среда), ориентированная на организацию взаимодействия между преподавателем и обучающимся, и может быть использована, как для организации дистанционного, так и поддержки очного обучения) в интеграции с on-line трансляцией наиболее важных, с точки зрения содержания курса, занятий в режиме on-line видеоконференции (например, с использованием приложения TrueConf). Возможности среды Moodle позволяют создавать учебные материалы в режиме on-line или загружать ранее подготовленные файлы [1].

В первую очередь содержание каждого дистанционного курса должно полностью соответствовать рабочей программе учебной дисциплины, структура курса соответствовать расписанию, чтобы курсанты имели возможность отработать каждое занятие. Дистанционный курс должен содержать конспекты всех лекций (в том числе презентации), практические задания, обучающие и контролирующие тесты, другие учебно-методические материалы, а также ссылки на дополнительную литературу и информационные ресурсы сети [2].

Остановимся подробнее на структуре курса.

1. Лекции. Лекционные материал рекомендуется разбивать на отдельные блоки (учебные вопросы). Для контроля отработки лекционного материала предусмотреть наличие контрольных вопрос по каждому блоку.

2. Практические занятия. Перечень задач по теме, выбираемых из банка вопросов случайным образом для индивидуализации заданий, необходимых для закрепления основных изученных понятий.

3. Тестовые задания. Логическое завершение изучения каждой темы курса, их выполнение является важнейшим условием перехода к следующей теме курса.

4. Дополнительный материал. Сведения о применении, исторические справки об исследовании проблем в изучаемой области.

5. Итоговый контроль. Содержание раздела составляют тестовые теоретические задания по всем темам курса и контрольные работы, содержащие задачи, требующие знаний сразу по нескольким разделам курса.

6. Литература. В этом разделе представлен список основной, дополнительной литературы и информационных ресурсов сети для углубления и расширения знаний курсантов.

При переходе на дистанционную форму обучения кардинально меняется роль преподавателя, основными функциями которого становятся организация учебного процесса путем создания условий для успешной деятельности курсантов, консультирование, контроль и мониторинг. У преподавателя появляются возможности планировать и прогнозировать результаты учебного процесса, анализировать возможность достижения запланированных результатов; организовать систему оценки показателей эффективной работы курсантов; не только контролировать конечный результат, но и отслеживать динамику во времени (контролировать скорость и качество усвоения материала); своевременно выявлять негативные факторы в учебном процессе и вносить изменения в дистанционный курс.

Одна из задач дистанционного образования заключается в организации самообразовательной деятельности курсантов. Дистанционный курс призван не только обогащать знаниями, но и обучать будущих специалистов способам их эффективного усвоения, творческого применения в практической деятельности, нахождения нестандартных решений возникающих проблем и задач.

При разработке дистанционного курса необходимо учитывать разные технические возможности курсантов и разную обеспеченность оборудованием, необходимого для дистанционного обучения: компьютер (планшет, смартфон), сканер, веб-камера, гарнитура (микрофон, наушники) и т.п.

При создании дистанционного курса необходимо помнить, что работа с курсом не заканчивается на создании учебно-методических материалов. Во время всего процесса обучения преподаватель должен управлять учебной деятельностью курсантов, организовывать on-line консультации, систематически контролировать успеваемость и психологическое состояние курсантов, усиливать мотивацию, при необходимости вносить изменения в курс.

Итак, для достижения наилучшего результата обучения с использованием дистанционных курсов необходимо соблюдать требования к психолого-педагогическому, эргономическому, содержательно-методическому и технико-технологическому качеству педагогических дистанционных курсов, функционирующих на базе информационных и коммуникационных технологий [3].

Литература

1. Заяц Т.М., Заяц Ю.А. Технология внедрения в учебный процесс электронных средств обучения // Интернет как реальность: сборник докладов III-ей Международной научно-практической конференции. Под редакцией А.М. Грибкова, Л.А. Виликотской. – 2017. – С. 105-107.

2. Ивличева Н.А. Методика реализации электронного обучения при проведении аудиторных занятий по очной форме // Математические методы и информационно-технические средства: материалы XV Всероссийской научно-практической конференции. – 2019. – С. 78-82.

3. Роберт И.В. Теория и методика информатизации образования: психолого-педагогический и технологический аспекты. – М.: БИНОМ. Лаборатория знаний, 2014. – 398 с.

Сведения об авторе

Морсакова Юлия Владимировна, кандидат физико-математических наук, доцент кафедры экономической безопасности Рязанского филиала Московского университета МВД России имени В.Я. Кикотя; e-mail: jykos@mail.ru.

Остапенко Владимир Савельевич
Юршин Александр Дмитриевич

ПРИМЕНЕНИЕ МЕТОДОВ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ В ДИАГНОСТИКЕ ГРАЖДАНСТВЕННОСТИ БУДУЩИХ ОФИЦЕРОВ В ВОЕННОМ ВУЗЕ

Современноеэмпирическоеисследованиевпедагогике невозможнобез использования методов математической статистики, в том числе, и применительно к проблемам развития такого сложногомировоззренческого феномена как гражданственность будущих офицеров, формируемого в военном вузе.

Математическиеметоды активно используются для обработки экспериментальных данных, полученных в ходе проведения научных исследований в рамках педагогического эксперимента в вузах. Так, в работах А.А. Дьячук[1], Е.А. Михайлычевой [4], П.В.Середенко [5], М.Г. Сороковой [6]и других рассматриваются вопросы применения математических методов в целом, и методов математической статистики в частности, в педагогических исследованиях с целью повышения достоверности их эмпирических данных и формулировки практических рекомендаций для повышения качества образовательного процесса.

Исследователи педагогических проблем образовательного процесса с помощью методов математической статистики обеспечивают репрезентативность объектов изучения в педагогическом эксперименте с целью провести целенаправленную диагностику исследуемого объектаи на этом основании представить достоверные результаты и выводы.

Так, например, при исследовании проблемы формирования гражданственности будущих офицеров в военном вузе определяются критерии и их показатели, по которым будут проводится измерения с помощью методов математической статистики. В нашем случае такими критериями будут: гносеологический, аксиологический, мотивационный, праксиологический.

С помощью математических методов проводились измерения каждого критерия с целью определить уровень сформированности основных компонентов гражданственности (когнитивный, ценностный, мотивационный, деятельностный), соответствующих этим критериям. Сравнение полученных результатов в контрольных и экспериментальных группах с помощью методов математической статистики позволяет сделать обоснованный вывод о достижении определенного уровня сформированности того или иного компонента гражданственности и сделать вывод об эффективности или не эффективности применения образовательныхтехнологий.

По объему охвата педагогических явлений в образовательном процессе вуза статистика делит эмпирические исследования на сплошные, когда изучаются все факторы, условия изучаемого явления и выборочные, если рассмотрению подвергается только часть интересующей совокупности, взятая по какому-либо признаку применительно к теме исследования. Как правило в педагогических исследованиях выборочные измерения применяются чаще, так как не всегда представляется возможность изучить всю совокупность явлений, факторов по разным причинам.

В педагогическом исследованиифеномена гражданственности в образовательном процессе военного вуза мы широко применяли следующие методы.

1. Эмпирические используются при проведении анкетирования, тестирования, экспертных оценках, самооценки, интервьюировании, обобщении характеристик, оценки проектов и др. Методы математической статистики позволяют измерить как количественные, так и качественные характеристики гражданственности обучающихся при обработке анкет, тестов, экспертных оценок и т.п.

2. Диагностические используются при анализе результатов измерения компонентов гражданственности по выявленным критериям (их показателям) на констатирующем и формирующем этапах педагогического эксперимента, при диагностике уровней сформированности какого-либо качества рассматриваемого феномена, позволяют осуществить количественный и качественный анализ полученных результатов с использованием рангового критерия Вилкоксона, метода корреляционного анализа, статистического метода группировки, критерияχ^2 Пирсона и др. [1].

Для обработки результатов проведенной опытно-экспериментальной работы по формированию гражданственности будущих офицеров в военных вузах, мы применяли для обработки полученных данных методы математической статистики, и в частности, такой эффективно используемый в педагогических исследованиях, каккритерий χ^2Пирсона. Его конкретное использованиедля проверки достоверности выдвинутой гипотезы (стартовые позиции обучающихся контрольных и экспериментальных групп в педагогическом эксперимента примерно равны), рассмотрим на примере проведенной опытно-экспериментальной работы по заявленной теме в военном вузе.

Критерий согласия Пирсона– непараметрический метод, широко применяетсяв последние годы в педагогических исследованияхи позволяет оценить статистическую значимость различий двух или нескольких относительных показателей, представленных в нашем исследовании позициями контрольной и экспериментальной групппо уровням сформированности гражданственности будущих офицеров в военном вузе.

Наиболее часто данный критерий употребляется для проверки гипотезы о принадлежности наблюдаемой выборки.Критерий хи-квадрат для анализа таблиц сопряженности был разработан и предложен в 1900 году английским математикомКарлом Пирсоном(1857-1936)[2].

Педагогическая гипотеза (в нашем случае это стартовые позиции на констатирующем этапе педагогического эксперимента контрольной и экспериментальной групп с целью диагностики уровня сформированности гражданственности обучающихся), используяметоды математической статистки, предполагает формулировку двухосновных гипотез.

Первая (основная) называется *нулевой гипотезой* (H_0), в которой формулируется исходная позиция авторовпедагогического исследования в военном вузе: различия незначительны в стартовых позициях контрольной и экспериментальной групп в педагогическом эксперименте по изучению уровней сформированности гражданственности будущих офицеров в образовательном процессе.

В другой, *альтернативной гипотезе* (H_1) делается предположение о том, что, применяя некую новую, специально разработанную модель и созданные педагогические условия в экспериментальных группах, различия станут существенными и, таким образом, будет подтверждена выдвинутая в исследовании гипотеза об эффективность применяемой модели и условий. В отдельных случаях (в зависимости от цели исследования) могут предлагаться несколько альтернативных гипотез с соответствующими обозначениями и характеристиками.

Таким образом, критерий хи-квадрат для диагностики исходного состояния сформированности в военном вузе гражданственности в контрольной и экспериментальной группах, мы использовали в двух вариантах:

1. Как расчет согласия эмпирического значения и предполагаемоготеоретического. В этом случае проверяется гипотеза H_0 об отсутствии различий между теоретическим и эмпирическим распределением.

2. Как расчет однородности двух независимых экспериментальныхвыборок. В этом случае проверяется гипотеза H_0 об отсутствиираличий между двумя эмпирическими распределениями.

В ходе проведения опытно-экспериментальной работы по формированию гражданственности будущих офицеров в военном вузе, нами учитывались и существующие ограничения в применении критерия хи-квадрат, которые подробно рассмотрены в работе П.В. Середенко[5].

Все эти положения были нами учтены при организации опытно-экспериментальной работы в военном вузе по развитию гражданственности и диагностики уровня еесформированности с помощью методов математической статистики.

С целью проверки, можно ли считать различия в уровне сформированности гражданственности обучающихся в контрольной и экспериментальной группах до начала педагогического эксперимента статистически не значимыми, нами было выдвинуто две гипотезы:

H_0 – степень расхождения в распределениях по каждому уровню в экспериментальных и контрольных группах статистически не значима, следовательно, уровеньсформированности гражданственности в контрольных и экспериментальных группах в начале педагогического эксперимента можно считать примерно одинаковым;

H_1 – степень расхождения в распределениях по уровням в экспериментальных и контрольных группах статистически значима, следовательно, исходный уровень сформированности гражданственности обучающихся в начале педагогического эксперимента нельзя считать одинаковым [3,6].

Проверим достоверность гипотезы H_0 с использованием критерия χ^2 Пирсона, для чего рассчитаем для каждой эмпирической частоты оценок в экспериментальной и контрольной группахобучающихся соответствующее теоретическое значение с помощью выражения

$$Ft_i^{\text{экс}} = \frac{\left(F_i^{\text{экс}} + F_i^{контр}\right)\cdot \sum_i F_i^{\text{экс}}}{\sum_i F_i^{\text{экс}} + \sum_i F_i^{\text{контр}}},\ Ft_i^{\text{контр}} = \frac{\left(F_i^{\text{экс}} + F_i^{контр}\right)\cdot \sum_i F_i^{\text{контр}}}{\sum_i F_i^{\text{экс}} + \sum_i F_i^{\text{контр}}} \quad (1)$$

где $F_i^{\text{экс}}, F_i^{\text{контр}}$ – значения частот (количество) оценок для каждого уровня в экспериментальной и контрольной группах. Далее рассчитаем значения отношений квадрата разности эмпирических и теоретических частот к значению теоретической частоты для каждой категории частот в экспериментальной и контрольной выборкам по формулам

$$\Delta F_i^{\text{экс}} = \frac{\left(F_i^{\text{экс}} - Ft_i^{\text{экс}}\right)^2}{Ft_i^{\text{экс}}},\ \Delta F_i^{\text{контр}} = \frac{\left(F_i^{\text{контр}} - Ft_i^{\text{контр}}\right)^2}{Ft_i^{\text{контр}}} \quad (2)$$

и, просуммировав значения $\Delta F_i^{\text{экс}}$ и $\Delta F_i^{\text{контр}}$ с помощью выражения

$$\chi^2 = \sum_i \Delta F_i^{\text{экс}} + \sum_i \Delta F_i^{\text{контр}} \quad (3)$$

получим эмпирические значения величины $\chi^2_{\text{эмп.}}$ Результаты расчетов по формулам 1, 2, 3, используемым в педагогических исследованиях, приведены в таблице 1. Число степеней свободы при сопоставлении двух распределений оценок вычисляется по формуле:

$$\nu = (k-1)(c-1) = 3 \quad (4)$$

Гдеk = 4 – количество разрядов (категорий оценок);c = 2 – количество сравниваемых распределений.

Определяем критические значения величины χ^2для ν = 3:$\chi^2_{\text{кр. }0,01}$ = 11,3 и $\chi^2_{\text{кр. }0,05}$ = 7,8[2, с. 625].

Расчетные значения $\chi^2_{\text{эмп.}}$,полученные при сравнении уровней сформированности гражданственности обучающихся в экспериментальных и контрольных группах до начала эксперимента в военном вузепо основным критериям оценки (гносеологический, аксиологический, мотивационный, праксиологический), представлены в таблице 1.

Таблица 1.

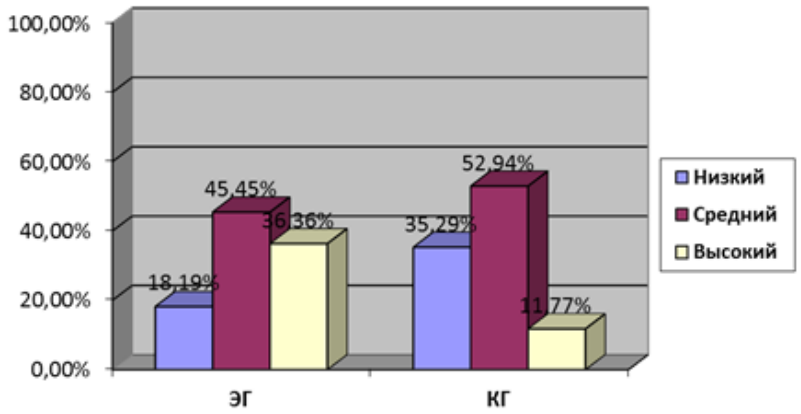
Критерийсформированности гражданственности	**Значения χ^2эмп.**
Гносеологический	0,05
Аксиологический	4,87
Мотивационный	1,34
Праксиологический	0,09

Поскольку все полученные значения $\chi^2_{эмп} < \chi^2_{кр,0,05}$, т.е. не лежат в критической области, то результаты наблюдения не противоречат гипотезе H_0. Следовательно, уровни сформированности гражданственности в экспериментальной и контрольной группах до начала эксперимента являются статистически однородными, что обеспечит «чистоту» педагогического эксперимента на следующем формирующем этапе. Такой результат был получен благодаря использованию методов математической статистики в диагностике уровней сформированности гражданственности будущих офицеров военном вузе.

Следует отметить, что применение методов математической статистики в педагогических исследованиях не ограничивается лишь вышерассмотренными положениями. Так, при проведении экспертизы представленной модели формирования гражданственности будущих офицеров в военном вузе, используется система экспертных оценок с выставлением баллов по конкретным блокам этой модели. Целевой блок имеет свою шкалу оценок по которой оценивается мнение каждого эксперта в соответствии с предложенной методикой. Далее с помощью методов математической статистики выводится усредненный показатель. По такой же методике проводится оценка методологического, структурно-содержательного, технологического и результативного блоков модели.

После реализации модели и завершения формирующего этапа педагогического эксперимента с помощью методов математической статистикипредставляется обобщенный вывод по полученным результатам.

Например, приведем конкретные результаты проведенного педагогического эксперимента по формированию гражданственности будущих офицеров в военном вузе. Так, низким уровнем сформированности обладают 35,29% опрошенных КГ и только 18,90% респондентов ЭГ, средний уровень характерен для большинства опрошенных: 52,94% испытуемых в КГ и 45,45% испытуемых в ЭГ; высокий уровеньвыявлен только у 11,77% опрошенных в КГ и у 36,36% опрошенных в ЭГ, что и представлено для сравнения в диаграмме.



Представленные результаты являются достоверными и доказывают результативность применяемых методов. Таким образом, использование методов математической статистики в педагогических исследованиях позволяет повысить достоверность полученных результатов и доказать эффективность конкретного педагогического экспери-

мента в целях повышения качества образовательного процесса в вузах по формированию конкретных качеств и характеристик обучающихся.

Литература

1. Дьячук А.А. Математические методы в психологических и педагогических исследованиях: учебное пособие / А.А. Дъячук. – Красноярск: Красноярский гос. пед. ун-т им. В.П. Астафьева, 2013. – 347 с.

2. Корн Г. Справочник по математике (для научных работников и инженеров) / Г.Корн, Т. Корн. — М.: Наука, 1973. – 832 с.

3. Математические методы в педагогических исследованиях: учебное пособие / автор. коллект.: С.И. Осипова, С.М. Бутакова, Т.Г. Дулинец, Т.Б. Шаипова. – Красноярск: Сиб. федер. ун-т, 2012. –264 с. – (электронный ресурс) URL: https://znanium.com/catalog/product/442057.

4. Михайлычев Е.А. Математические методы в педагогическом исследовании. Учебное пособие / Е.А. Михайлычев. –М.: Высшая школа, 2008. – 196 с.

5. Середенко П.В. Методыматематическойстатистикив психолого-педагогическихисследованиях: учеб. пособ. / П.В. Середенко, А.В. Дол-жикова. – 2-е изд., испр. и доп. – Южно-Сахалинск: СахГУ, 2009. – 52 с.

6. СороковаМ.Г. Математические методы в психолого-педагогических исследованиях: учебное пособие / М.Г. Сорокова. – М.: Неолит, 2020. – 216 с.

Сведения об авторах

Остапенко Владимир Савельевич, доктор педагогических наук, профессор,профессор кафедры гуманитарных и социально-экономических дисциплин Центрального филиала Российского государственного университетаправосудия (г. Воронеж);
e-mail: ostapenko-vl@mail.ru.

Юршин Александр Дмитриевич, старший преподаватель кафедры управления материально-техническим обеспечением ВВС ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж); e-mail: Yurshin.1975@yandex.ru.

Пекарская Ольга Анатольевна,
Насрулин Эдуард Рафаэльевич

УПРАВЛЕНИЕ КАЧЕСТВОМ ПРЕПОДАВАНИЯ МАТЕМАТИКИ В ВУЗЕ С ПОМОЩЬЮ КВАЛИМЕТРИЧЕСКИХ МЕТОДОВ

При преподавании математических дисциплин в вузе особое место занимает вопрос об измерении уровня сформированности компетенций у обучающихся, поскольку этот аспект оказывает непосредственное влияние на качество математического образования.

При разработке инновационных образовательных технологий большое значение имеют такие вопросы как:

–взаимодействие отечественной системы образования и мировой образовательной среды;

–динамика изменений в характере и качестве образования, вызываемых, в свою очередь,изменениями в общественной, социальной и экономической обстановке в нашем государстве;

–изменения, происходящие в нашей стране не просто в образовательной сфере, но и конкретно в области инновационных технологий обучения и воспитания;

– ограничения, налагаемые на различные виды ресурсов[1].

Особым вопросом является квалиметрическая оценка уровня сформированности компетенций. Такой подход порождает предъявление к текстам дополнительных требований. Во-первых, тесты должны быть универсальны, то есть мы должны иметь возможность использовать их для тестирования по разным дисциплинам. Это очень существенно потому, что разработанная методика должна быть пригодна для междисциплинарного тестирования. Тесты должны быть надежны, иметь высокое качество, позволять эффективно обрабатывать результаты.

При этом, конечно же, система тестирования, вне зависимости от ее качества, не является и не может являться фактором, определяющим качество образовательного процесса в целом. Здесь исключительно важна роль квалиметрического подхода. Это позволяет произвести оценку различных видов образовательных технологий на обобщенный показатель качества, а также моделировать образовательные процессы с применением информационных технологий.

В управлении качеством образования существенное место занимает система менеджмента качества (СМК), которая должна соответствовать положениям международных стандартов ISO9000 поколений 3 и 4. Такие стандарты уже действуют в образовательных учреждениях в качестве аккредитационных показателей [2].

Для повышения качества преподавания математических дисциплин необходимо обеспечить:

- для всех математических дисциплин - возможность текущего контроля успеваемости;
- для всех математических дисциплин - возможность сравнительной оценкиуспеваемости;
- для обучаемых - проведение выборочного текущего контроля успеваемости;
- для выпускников – проведение выборочного итогового контроляостаточных знаний.

Что касается текущего контроля успеваемости обучаемых, то это форма обучения давно известно и самым широким образом используетсяв области управления учебным процессом. [3].

Перейдем к математическому выражению показателей качества.

Во-первых, зачетную либо экзаменационную ведомость можно представить в текстовом формате (табл.1). Тогда комплексный показатель успеваемости можно рассчитать по следующей формуле:

$$Q_{\text{д}} = 1 - \frac{n_{\text{нз}}}{\text{m}}, \qquad (1)$$

где $n_{\text{нз}}$ – обучающиеся, которым не удалось сдать зачёт либо экзамен;

m – обучающиеся, которые смогли сдать зачёт либо экзамен.

Зачетная либо экзаменационная ведомость также может иметь цифровой формат. Такая ведомость включает реперные точки, обозначаемые цифрами 2, 3, 4, 5 (табл.1) В таком случае комплексный показатель качества может быть рассчитан по следующей формуле:

$$Q_{\text{д}} = 1 - \sum_{\text{i}=2}^{\text{i}=5} \frac{5-\text{i}}{3} \frac{n_{\text{i}}}{\text{m}} \qquad (2)$$

где i – показатель, характеризующий оценки в виде обозначений реперных точек;

n_{i} – число оценок с номером i;

m – число обучающихся, аттестованных по цифровой форме ведомости.

При цифровом формате ведомости зачета либо экзамена и использовании балльно-рейтинговой шкалы формула для расчета комплексного показателя качества образования принимает вид(табл. 1):

$$Q_{Д} = 1 - \frac{1}{m}\sum_{i=1}^{m}\frac{100 - Z_i}{60} \quad (3)$$

где Z_i–оценка[4, с.397].

Часто возникает необходимость впроведении внешнего аудита либо проверок. Тогда эксперты опираются на уровень освоения компетенций, требуемых согласно ФГОС, при этом ведомости предоставляются в буквенном формате (табл. 1). При этом комплексный показатель знаний, навыков и умений обучаемых рассчитывается по формуле:

$$Q_{гк} = 1 - \frac{n_н}{m} - 0{,}5\frac{n_с}{m}, \quad (4)$$

где $n_н$– оценки, обозначаемыелитерой Н;

$n_с$– оценки, обозначаемыелитеройС;

m– всего оценок, число которых должно быть равно числуобучающихся[4].

Таблица 1.

Буквенный формат ведомости успеваемости

№п/п	Обучающийся	Мнение	Пример расчёта $Q_{гк}$
1	Первый	С	
2	Второй	Н	
3	Третий	В	$Q_{гк} = 1 - \frac{2}{10} - 0{,}5\frac{6}{10} = 0{,}5$
…	…	С	
…	…	С	
…	…	В	
…	…	С	
…	…	Н	
…	…	С	
m=10	…	С	
$Q_{гк}$		0,5	

Литеры В, С, Н; которые соответствуютвысокому, среднему и низкому уровню знаний. При уменьшении значения $Q_{гк}$ требуется осуществить предупреждающее воздействие напроцессобученияДля данной математической дисциплины.

При соблюдении условия $Q_{гк} < 0{,}5$ происходит переход к корректирующим воздействиям.В качестве примера приведем некоторые из расчетов.

Таблица 2.

Сводная ведомость успеваемости для четырех дисциплин

№ п/п	Обучаемый	Учебные дисциплины				Формулы для расчета$Q_{Д}$
		Д1	Д2	Д3	Д4	
1	1-й	4	3	5	3	$Q_{д1} = 1 - \frac{5-4}{3}\cdot\frac{10}{10} = 1 - 0{,}33 = 0{,}66 \approx 0{,}7$
2	2-й	4	3	5	4	
3	3-й	4	3	5	4	$Q_{д2} = 1 - \frac{5-3}{3}\cdot\frac{10}{10} = 1 - 0{,}67 = 0{,}33 \approx 0{,}3$
4	…	4	3	5	4	
5	…	4	3	5	5	$Q_{д3} = 1 - \frac{5-5}{3}\cdot\frac{10}{10} = 1 - 0 = 1$
6	…	4	3	5	3	
7	…	4	3	5	4	
8	…	4	3	5	4	$Q_{д4} = 1 - \left(\frac{5-3}{3}\cdot\frac{3}{10} + \frac{5-4}{3}\cdot\frac{6}{10} + \frac{5-5}{3}\cdot\frac{1}{10}\right) =$ $= 1 - (0{,}2 + 0{,}2) = 0{,}6$
9	…	4	3	5	4	
10	…	4	3	5	3	
$Q_{д}$		0,7	0,3	1	0,6	

Текущую успеваемость по различным математическим дисциплинам можно сравнивать, используя сводные ведомости текущей успеваемости по различным математическим дисциплинам (табл. 2).

Проведение сравнения текущей успеваемости по 4-м дисциплинам показывает, что, когда речь идет о дисциплине Д2, то возникает необходимость корректирующего воздействия на образовательный процесс.

Иногда необходимо оценить степень владения обучающихся определенной компетенцией, формируемой определенными математическими дисциплинами. В этом случае составление комплексной сводной ведомости производится с учётом весовых коэффициентов для разных учебных дисциплин.

Использование буквенного формата представления измерительной информации дает возможность рассчитывать (табл. 3), комплексный показатель успеваемости для всех обучающихся (3).

Таблица 3.

Буквенный формат сводной ведомости успеваемости

№ п/п	Обучаемый	Учебные дисциплины				$Q_{стр}$	Пример расчёта $Q_{стр}$
		Д1	Д2	Д3	Д4		
		Весовые коэффициенты					
		0,2	0,1	0,4	0,3		
1	1-й	С	Н	В	С	0,66	$Q_{стр1}$ = 1-(0,1)-0,5(0,2+0,3)=0,66
2	2-й	С	С	С	С	0,51	$Q_{стр2}$ =1- 0,5(0,2+0,1+0,4+0,3) =0,51
3	3-й	С	В	Н	С	0,34	$Q_{стр3}$ =1-(0,4)-0,5(0,2+0,3) = 0,34
…	…	…	…	…	…	…	
m	…	…	…	…	…	…	

Включение в сводную ведомость дисциплин, имеющих зачеты согласно учебным планам, приводит к формуле:

$$Q_{кi} = 1 - \sum_{i=1}^{n_{нз}} g_i, \quad (5)$$

гдеg_i – весовой коэффициент дисциплины с номером i, для которой зачёт получить не удалось;$n_{нз}$ – общее число не полученных обучаемым зачётов [4].

При осуществлении внешних проверок, аудита и государственной аккредитации производится выборочный текущий и итоговый контроль компетентности выпускников образовательного учреждения, при котором применяется экспертный метод.

При проведении контроля эксперты либо проводят собеседования, либо осуществляют тестирование выпускников согласно группам компетенций. Мнение экспертов выражается в буквенном формате. Решения по каждому обучающемуся и в отношении всей генеральной совокупности, из которой сделана выборка, необходимо принимать в соответствии с правилами, применяемыми при выборочном статистическом контроле текущей успеваемости [3].

При цифровом формате представления измерительной информации с обозначениями реперных точек цифрами 2, 3, 4, 5 (табл.2), формула расчета комплексного показателя успеваемости обучающихся принимает вид:

$$Q_к = 1 - \sum_{i=2}^{5} \sum_{j=1}^{n_i} \frac{5-i}{3} g_{i,j}, \quad (6)$$

где $g_{i,j}$ – весовой коэффициент мнения с номером j, которому соответствует оценка с номером i[4, с.399].

Из показателей качества освоения отдельных групп компетенций, рассчитываемых по (4), можно сделать вывод о том, требуется ли корректирующее воздействие на учебный процесс согласно дисциплинам, которые данный процесс формируют.

Литература

1. Корбукова Н.А. Балльно-рейтинговая система как оценка функциональной подготовленности студента // Развитие современного образования: теория, методика и практика: материалы III Междунар. науч.–практ. конф. Чебоксары, 5 февр. 2015 г. - Чебоксары: ЦНС «Интерактивплюс», 2015. -С. 175–178.

2. Новикова Е.Ю. Балльно-рейтинговая оценка: мнение студентов // Высшее образование в России. - 2013.- №7. С.132-136.

3. О.О. Мартыненко, З.В. Якимова, В.И. Николаева. Методический подход к оценке компетенций выпускников // Высшее образование в России. - 2015. - № 12. С. 35-46.

4.Пекарская О.А. Интеграционные образовательные технологии, применяемые в дистанционном обучении студентов, - важнейший ресурс образования / Сборник научных статей V международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании».2016. -С. 396-400.

Сведения об авторах

Пекарская Ольга Анатольевна, кандидат экономических наук, доцент кафедры высшей математики и системного моделирования сложных процессов Санкт-Петербургскогоуниверситета ГПС МЧС России; e-mail: Pekarskaya.olga@mail.ru.

Насрулин Эдуард Рафаэльевич, магистрантСанкт-Петербургскогоуниверситета ГПС МЧС России; e-mail: nased@bk.ru.

Прокопенко Алексей Николаевич,
Дрога Андрей Анатольевич,
Гуржий Алексей Александрович

ОСОБЕННОСТИ ГОСУДАРСТВЕННОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА СОВРЕМЕННОМ ЭТАПЕ

Основы государственного регулирования в сфере применения информационных технологий установлены в статье 12 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ «Об информации…») [1]. В соответствии с указанной статьей государственное регулирование состоит из шести направлений деятельности:

1. Правовое регулирование отношений об обороте информации с применением информационных технологий.
2. Создание и развитие информационных систем для обеспечения информацией физических лиц и организаций всей страны, а также обеспечение взаимодействия между ними.
3. Обеспечение функционирования Интернет и других информационно-телекоммуникационных сетей.
4. Обеспечение информационной безопасности детей.
5. Разработка и реализация целевых программ применения информационных технологий.

6. Обеспечение доступа к информации в информационных системах на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Рассмотрим указанные направления государственного регулирования.

Государственное правовое регулирование об обороте информации с применением информационных технологий основано на положениях *Конституции Российской Федерации* [2]. Основные положения, имеющие отношения к информации и информационным технологиям сконцентрированы в статьях 29, 33, 41 и 42 Конституции РФ. Статья 29 Конституции РФ определила, что поиск, получение, передача, производство и распространение информации осуществляется свободно. Статья 33 Конституции РФ гарантирует гражданам и организациям возможность свободного получения в государственных органах необходимой им информации, а также обязывает государственные и муниципальные органы создавать информационные ресурсы (системы) для предоставления информации обращающимся гражданам и организациям. Статьи 41 и 42 Конституции РФ предусматривают свободное получение информации о фактах и событиях, угрожающих жизни и здоровью людей, а также об окружающей среде.

Развитие, установленных в Конституции РФ положений осуществляется путем принятия законодательных и нормативных правовых актов. Можно выделить следующие правовые акты, устанавливающие особенности применения информационных технологий и доступа граждан и организаций к информации.

Доктрина информационной безопасности Российской Федерации [3] - утвердила систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере, в том числе:

–по обеспечению и защите конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;

–обеспечению устойчивого и бесперебойного функционирования информационной инфраструктуры;

–совершенствованию деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности.

Доктрина информационной безопасности РФ определила, что к основным направлениям обеспечения информационной безопасности относятся, в том числе:

–повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов;

–повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

–развитие национальной системы управления российским сегментом сети «Интернет».

Законодательство о средствах массовой информации в целом и Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» [4], в частности, регулируют отношения, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий. Законодательство о СМИ устанавливает, как порядок распространения информации средствами массовой информации в электронном виде (через Интернет, телевидение и радио), так и право граждан на получение информации.

Законодательство о рекламе в целом и Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» [5], в частности, регулируют порядок распространения рекламной информации, социальной рекламы и ограничения на распространение рекламы. Подавля-

ющее большинство рекламной информации распространяется с помощью информационных технологий, через телевидение и радио, а также через Интернет.

Законодательство об информации ограниченного доступа основано на нормах ФЗ «Об информации…», Законе РФ от 21.07.1993 № 5485-1 «О государственной тайне» и Указе Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» [6]. В зависимости от вида информации меняются особенности ее распространения и доступа к ней, в том числе с использованием информационных технологий. В соответствии со статьей 9 ФЗ «Об информации…» информация ограниченного доступа подразделяется на информацию, относящуюся к государственной тайне, и конфиденциальную информацию. Указ Президента РФ от 06.03.1997 № 188 подразделил конфиденциальную информацию на 7 видов:

−персональные данные;

−сведения, составляющие тайну следствия и судопроизводства;

−служебная тайна;

−профессиональная тайна;

−коммерческая тайна;

−сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

−сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов.

Законодательно понятия профессиональной или служебной тайны не закреплены. Общее количество видов профессиональной и служебной тайны превышает пятьдесят видов (врачебная, банковская, налоговая, таможенная, нотариальная, адвокатская, журналистская, связи, усыновления, исповеди и т.д.).

Создание и развитие информационных систем для обеспечения информацией граждан и организаций осуществляется на основании следующих законодательных и нормативных актов: Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» [7], который предусматривает, в том числе, возможность обращений граждан в форме электронного документа и получение ими информации через Интернет. Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [8] и Федерального закона от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [9], которые устанавливают обязанности государственных органов, органов местного самоуправления и судов предоставлять физическим лицам и организациям информацию о своей деятельности. Для предоставления информации государственные органы, органы местного самоуправления и суды создают официальные сайты в сети Интернет.

Перечни информации о деятельности федеральных государственных органов, которая должна размещаться на официальном сайте, утверждаются Президентом РФ, Правительством РФ, Государственной Думой РФ и Советом Федерации РФ. Перечень информации о деятельности судов в Российской Федерации и особенности размещения судебных актов устанавливаются Федеральным законом от 22.12.2008 № 262-ФЗ. Перечни о деятельности государственных органов субъектов Российской Федерации утверждаются в порядке, определяемом субъектами РФ. Перечни информации о деятельности органов местного самоуправления утверждаются в порядке, определяемом органами местного самоуправления. Однако состав информации, которую должны размещать государственные органы субъектов РФ и органы местного самоуправления, установлен Распоряжением Правительства РФ от 10.07.2013 № 1187-р [10]. Постановлениями Правительства РФ и приказами министерств и ведомств установлен порядок

доступа к информации о деятельности конкретных министерств, ведомств и государственных организаций, а также к информации, содержащейся в информационных системах.

Для создания условий эффективного использования в России Интернет была проделана нормотворческая работа как внутри страны, так и на международном уровне. В целях государственного регулирования работы Интернет и других телекоммуникационных сетей в России был принят Федеральный закон от 05.05.2014 № 97-ФЗ, который направлен на упорядочение обмена информацией с использованием информационно-телекоммуникационных сетей. Указанным Законом установлены обязанности организатора распространения информации в Интернет и порядок ограничения доступа к ресурсам Интернет [11].

Были приняты другие федеральные законы, установившие обязанности оператора поисковой системы и владельца аудиовизуального сервиса, особенности распространения информации новостным агрегатором. Также был введен Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено и установлен порядок ограничения доступа к различным видам информации, распространение которой запрещено. Данные нормы были имплементированы преимущественно в ФЗ «Об информации…» и Кодекс РФ об административных правонарушениях.

На международном уровне был дважды принят Модельный закон об основах регулирования Интернета в 2011 и 2016 годах. Кроме того, был введен национальный кириллический домен верхнего уровня «.рф». 2-7 ноября 2008 года на 33-й конференции ICANN в Каире было принято решение о выделении России кириллического домена верхнего уровня. Домен действует с 16 ноября 2009 года. В настоящее время Координационный центр национального домена сети Интернет (Координационный центр доменов .RU/.РФ) является администратором и выполняет функции национальной регистратуры доменов верхнего уровня .ru и .рф. Техническим оператором реестров доменов .ru и .рф с 2018 года является «Ростелеком». Правовое регулирование российской национальной доменной зоны, а также контроль над ней, осуществляется Роскомнадзором и Минкомсвязи России.

Обеспечение информационной безопасности детей регулируется Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства РФ от 02.12.2015 № 2471-р [12], которая определяет стратегическую цель в данной сфере, как «обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России».

Основные положения обеспечения информационной безопасности детей закреплены также в Федеральном законе от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [13]. Указанным Законом установлен порядок классификации информационной продукции в соответствии с особенностями восприятия информации детьми определенной возрастной категории и вероятность причинения информацией вреда здоровью и (или) развитию детей. Вся информационная продукция подразделяется на пять видов – до шести лет, до 12 лет, до 16 лет, до 18 лет и без ограничений по возрасту.

Государственные органы и органы местного самоуправления участвуют в разработке и реализации целевых программ применения информационных технологий.

Целевые программы по созданию, модернизации и эксплуатации информационных технологий принимаются на федеральном и региональном уровне, уровне муниципалитетов, а также в министерствах и ведомствах. Из программ, принятых на феде-

ральном уровне можно выделить *Федеральную целевую программу «Электронная Россия (2002 - 2010 годы)»*, утвержденную Постановлением Правительства РФ от 28.01.2002 № 65 [14]. Продолжением ФЦП «Электронная Россия» стала *Государственная программа Российской Федерации «Информационное общество»*, которая действует с 2011 года и запланирована до 2024 года. Объем бюджетных ассигнований на реализацию Программы за счет средств федерального бюджета составляет более 2 триллионов 612 миллиардов рублей [15].

Также на федеральном уровне можно выделить концептуальные документы, определяющие порядок развития в Российской Федерации информационных технологий, информационных ресурсов и информационного общества в целом. Основным концептуальным документом в данной области является *Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы*, утвержденная Указом Президента РФ от 09.05.2017 № 203 [16]. Стратегия определила цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. До 2017 года действовала предыдущая Стратегия развития информационного общества в Российской Федерации, утвержденная Президентом РФ 07.02.2008 № Пр-212.

Вторым концептуальным документом является *Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года*, утвержденная Распоряжением Правительства РФ от 01.11.2013 № 2036-р [17]. В Стратегии под отраслью информационных технологий понимается совокупность российских компаний, осуществляющих следующие виды деятельности:

–разработка тиражного программного обеспечения;

–предоставление услуг в сфере информационных технологий, в частности заказная разработка программного обеспечения, проектирование, внедрение и тестирование информационных систем, консультирование по вопросам информатизации;

–разработка аппаратно-программных комплексов с высокой добавленной стоимостью программной части;

–удаленная обработка и предоставление информации, в том числе на сайтах в «Интернет».

Развитие отрасли информационных технологий в субъектах РФ осуществляется, в том числе на федеральные денежные средства, в соответствии с *Концепцией региональной информатизации*, утвержденной Распоряжением Правительства РФ от 29.12.2014 № 2769-р [18]. Положения Концепции распространяются на информатизацию региональных органов государственной власти, органов местного самоуправления и организаций, в которых размещается государственное задание или муниципальное задание (заказ) на предоставление государственных и (или) муниципальных услуг.

На региональном и муниципальном уровне также принимаются программы развития информационных технологий, программы развития информационного общества или программы информатизации. В качестве примера можно привести Государственную программу Белгородской области «Развитие информационного общества в Белгородской области» [19], Муниципальную программу муниципального района «Корочанский район» «Развитие информационных технологий в деятельности органов местного самоуправления» [20] или Муниципальная программа Алексеевского городского округа «Развитие информатизации в Алексеевском городском округе на 2015 - 2020 годы» [21].

Аналогичные программы развития информационных технологий и информатизации принимаются в министерствах и ведомствах. Например, Программа информатиза-

ции Федерального архивного агентства и подведомственных ему учреждений на 2011 - 2020 гг. [22]

Для организации деятельности информационных систем в Российской Федерации создана *государственная информационная система учета информационных систем*, разрабатываемых и приобретаемых за счет средств бюджетов бюджетной системы Российской Федерации [23]. Согласно информации Портала ФГИС КИ в 2019 году из федерального бюджета и бюджетов государственных внебюджетных фондов на создание новых информационных систем было израсходовано более 10 млрд. 800 млн. рублей, на эксплуатацию информационных систем более 74 млрд. рублей и на развитие информационных систем более 52 млрд. рублей [24]. Лидером в 2019 году по расходам на информационные системы является Федеральная налоговая служба РФ, израсходовавшая более 18 млрд. рублей.

Расходы регионов России на создание, развитие и эксплуатацию информационных систем в 2017 году составили более 85 млрд. рублей, а в 2018 году превысили 100 млрд. рублей. Безусловным лидером по расходам на информационные системы является Москва, расходы которой в 2017 году превысили 41 млрд. рублей, а в 2018 году практически достигли 50 млрд. рублей [25].

Государственные органы и органы местного самоуправления создают информационные системы для обеспечения доступа граждан к информации, в том числе на государственных языках республик в составе России.

Граждане получают доступ к информации или через официальные сайты государственных органов, организаций и органов местного самоуправления или через систему *электронного правительства.*

Портал государственных услуг (https://www.gosuslugi.ru/) функционирует на основании Федерального закона «Об организации предоставления государственных и муниципальных услуг» и предполагает объединение в одном ресурсе государственных услуг и функций, предоставляемых федеральными, региональными и муниципальными органами власти. Доступ к Порталу осуществляется гражданином или организацией, как самостоятельно, так и с помощью сотрудников многофункциональных центров (МФЦ). Часть государственных услуг и функций доступна полностью в электронном виде, часть через МФЦ и часть при обращении лично в государственный или муниципальный орган, но по электронной записи на Портале.

Перечень государственных услуг и функций, а также порядок их предоставления установлен:

–Постановлением Правительства РФ от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;

–Постановлением Правительства РФ от 27.09.2011 № 797 «О взаимодействии между многофункциональными центрами предоставления государственных и муниципальных услуг и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления»;

–Постановлением Правительства РФ от 06.05.2011 № 352 «Об утверждении перечня услуг, которые являются необходимыми и обязательными для предоставления федеральными органами исполнительной власти, Государственной корпорацией по атомной энергии «Росатом» государственных услуг и предоставляются организациями, участвующими в предоставлении государственных услуг, и определении размера платы за их оказание»;

–Распоряжением Правительства РФ от 25.04.2011 № 729-р «Об утверждении перечня услуг, оказываемых государственными и муниципальными учреждениями и дру-

гими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ), подлежащих включению в реестры государственных или муниципальных услуг и предоставляемых в электронной форме»;

–Распоряжением Правительства РФ от 19.02.2018 № 260-р «Об утверждении перечня государственных услуг, предоставляемых федеральными органами исполнительной власти, органами государственных внебюджетных фондов на основании комплексного запроса» и другими нормативными правовыми актами.

В соответствии с Законом РФ от 25.10.1991 № 1807-1 «О языках народов Российской Федерации» [26] допускается использование государственных языков республик для официального опубликования документов, проведения выборов и референдумов, работы государственных органов, организаций, предприятий и учреждений, а также в официальном делопроизводстве. Соответственно, официальные сайты органов государственной власти и местного самоуправления в республиках в составе Российской Федерации могут быть двуязычными. Например, двуязычными являются сайты Правительства Республики Татарстан (http://prav.tatarstan.ru/tat/) и Правительства Республики Башкортостан (https://pravitelstvorb.ru/ba/). Но не во всех национальных республиках государственные органы имеют двуязычные официальные сайты. Так, в Чеченской республике (http://chechnya.gov.ru/) и Республике Дагестан (http://www.e-dag.ru/) официальные сайты Правительств являются одноязычными – только на русском языке.

Таким образом, в России создана всеобъемлющая система государственного правового регулирования в сфере применения информационных технологий. Указанная система позволяет обеспечить функционирование государственных и муниципальных информационных систем, обеспечивающих граждан нашей страны информацией. Особое внимание государством уделяется области оказания государственных и муниципальных услуг населению и области информирования граждан о деятельности государственных органов.

Необходимо отметить, что созданная система позволяет информировать граждан, затрачивая минимальное количество человеко-часов, путем размещения на сайтах государственных органов большей части интересующих граждан сведений. Отдельно можно выделить созданную систему обеспечения информационной безопасности детей, которая позволяет разграничить информационные потоки и оградить детей от ненужной и вредной информации.

Кроме того, нужно обратить внимание, что в соответствии с Конституцией РФ и российским законодательством в России существует единое информационное поле, функционирующее на русском языке, что позволяет всем гражданам страны чувствовать себя членами одного единого государства.

Можно сделать вывод о необходимости дальнейшего развития интеграции различных государственных информационных систем, создания единого регистра населения и обеспечения получения гражданами максимального количества государственных услуг полностью в электронном виде.

Литература

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.12.2019) // Российская газета. № 165. 29.07.2006.

2. Конституция Российской Федерации (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. 04.08.2014. № 31. Ст. 4398.

3. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.

4. О средствах массовой информации: Закон РФ от 27.12.1991 № 2124-1 (ред. от 02.12.2019) // Российская газета. № 32. 08.02.1992.

5. О рекламе: Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 02.08.2019) // Российская газета. № 51. 15.03.2006.

6. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) // Российская газета. № 51. 14.03.1997.

7. О порядке рассмотрения обращений граждан Российской Федерации: Федеральный закон от 02.05.2006 № 59-ФЗ (ред. от 27.12.2018) // Российская газета № 95. 05.05.2006.

8. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон от 09.02.2009 № 8-ФЗ // Российская газета. № 25. 13.02.2009.

9. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22.12.2008 № 262-ФЗ // Российская газета. № 265. 26.12.2008.

10. О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных: Распоряжение Правительства РФ от 10.07.2013 № 1187-р (ред. от 24.03.2018) // Собрание законодательства РФ. 29.07.2013. № 30 (часть II). Ст. 4128.

11. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей: Федеральный закон от 05.05.2014 № 97-ФЗ (ред. от 29.07.2017) // Российская газета. № 101. 07.05.2014.

12. Об утверждении Концепции информационной безопасности детей: Распоряжение Правительства РФ от 02.12.2015 № 2471-р // Собрание законодательства РФ. 07.12.2015. № 49. Ст. 7055.

13. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) // Российская газета. № 297. 31.12.2010.

14. О федеральной целевой программе «Электронная Россия (2002 - 2010 годы)»: Постановление Правительства РФ от 28.01.2002 № 65 (ред. от 09.06.2010) // Собрание законодательства РФ. 04.02.2002. № 5. Ст. 531.

15. Об утверждении государственной программы Российской Федерации «Информационное общество»: Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 30.11.2019) // Собрание законодательства РФ. 05.05.2014. № 18 (часть II). Ст. 2159.

16. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 15.05.2017. № 20. Ст. 2901.

17. Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года: Распоряжение Правительства РФ от 01.11.2013 № 2036-р (ред. от 18.10.2018) // Собрание законодательства РФ. 18.11.2013. № 46. Ст. 5954.

18. Об утверждении Концепции региональной информатизации: Распоряжение Правительства РФ от 29.12.2014 № 2769-р (ред. от 18.10.2018) // Собрание законодательства РФ. № 2. 12.01.2015. Ст. 544.

19. Об утверждении государственной программы Белгородской области «Развитие информационного общества в Белгородской области»: Постановление Правительства Белгородской обл. от 16.12.2013 № 518-пп (ред. от 07.10.2019) // Сборник нормативных правовых актов Белгородской области. № 42 (том I). 13.01.2014.

20. Об утверждении муниципальной программы муниципального района «Корочанский район» «Развитие информационных технологий в деятельности органов местного самоуправления»: Постановление администрации муниципального района «Корочанский район» Белгородской обл. от 12.09.2014 № 651 (ред. от 29.03.2019) // Доступ из СПС «КонсультантПлюс».

21. Об утверждении муниципальной программы Алексеевского городского округа «Развитие информатизации в Алексеевском городском округе на 2015 - 2020 годы»: Постановление администрации муниципального района «Алексеевский район иг. Алексеевка» Белгородской обл. от 23.10.2014 № 724 (ред. от 28.03.2019) // Доступ из СПС «КонсультантПлюс».

22. Об утверждении Программы информатизации Федерального архивного агентства и подведомственных ему учреждений на 2011 - 2020 гг.: Приказ Росархива от 02.12.2011 № 104 // Доступ из СПС «КонсультантПлюс».

23. О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов (вместе с «Положением о федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов»): Постановление Правительства РФ от 26.06.2012 № 644 (ред. от 25.09.2018) // Собрание законодательства РФ. 02.07.2012.№ 27. Ст. 3753.

24. Портал ФГИС КИ. Бюджеты на информатизацию за 2019 год. [Электронный ресурс]. Режим доступа: https://portal.eskigov.ru/ (дата обращения – 24.05.2020).

25. Портал ФГИС КИ. Топ-5 регионов по объемам ИКТ-бюджетов. [Электронный ресурс]. Режим доступа: https://portal.eskigov.ru/er (дата обращения – 24.05.2020).

26. О языках народов Российской Федерации: Закон РФ от 25.10.1991 № 1807-1 (ред. от 12.03.2014) // Ведомости СНД и ВС РСФСР. 12.12.1991. № 50. Ст. 1740.

27. Прокопенко А.Н., Александров А.Н., Дрога А.А. Правовая защита информации (Информационное право): учебное пособие (2-е издание, переработанное и дополненное). – Белгород: Изд-во Бел ЮИ МВД России, 2012. 227 с.

28. Ищенко А.Н., Прокопенко А.Н., Страхов А.А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. № 2. С. 55-62.

29. Прокопенко А.Н., Кривоухов А.А. Правовая политика Российской Федерации в сфере государственных информационных ресурсов // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. 2007. № 1.С. 173-181.

Сведения об авторах

Прокопенко Алексей Николаевич, начальник кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат технических наук, доцент; e-mail: aprokopenko11@mvd.ru.

Дрога Андрей Анатольевич, заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: abullet@rambler.ru.

Гуржий Алексей Александрович, преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: aleksey.gurzhiy@yandex.ru.

Прокопенко Алексей Николаевич,
Жукова Полина Николаевна,
Насонова Валентина Афанасьевна

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ ИДЕНТИФИКАЦИИ ГРАЖДАН РОССИЙСКОЙ ФЕДЕРАЦИИ В СИСТЕМЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В декабре 2017 года в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ «Об информации…») [1] введена новая статья 14.1 «Применение информационных технологий в целях идентификации граждан Российской Федерации». Указанная статья является объемной (24 части) и затрагивает достаточно сложные вопросы, связанные с ведением государственными и муниципальными органами и организациями, а также банками информационных систем идентификации граждан Российской Федерации.

Принятие статьи 14.1 ФЗ «Об информации…» потребовалось в связи с разработкой и внедрением новой системы идентификации граждан России как в государственных информационных системах, так и в финансовых целях.

Часть первая статьи 14.1 ФЗ «Об информации…» установила, что размещение данных граждан Российской Федерации может осуществляться в двух информационных системах, которые предназначены для идентификации физических лиц:

Единой системе идентификации и аутентификации (далее – ЕСИА), созданной с соответствии с Постановлением Правительства РФ от 28.11.2011 № 977 [2].

Единой информационной системе персональных данных (Единой биометрической системе, далее – ЕБС), созданной в соответствии с Постановлением Правительства РФ от 30.06.2018 № 772 [3].

Необходимо отметить, что ранее существовала только одна система – ЕСИА, которая функционирует с 2011 года. Цель создания двух систем состоит в том, чтобы информация, содержащаяся в них, позволяла осуществлять процедуру идентификации граждан России не только сотрудникам той организации, которая внесла данные гражданина в систему, но и сотрудникам любой организации – пользователя информационной системы.

Для обмена информацией в форме электронных документов в указанных информационных системах используется электронная подпись, которая формируется в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» [4]. Причем, статья 11.1 ФЗ «Об информации…» установила, что для государственных органов и их сотрудников обязательно использование *усиленной квалифицированной электронной подписью*, которая формируется в результате криптопреобразования информации и состоит из открытого и закрытого ключей и создается с помощью средств криптозащиты, сертифицированных ФСБ России. А физические лица и организации подписывают направляемую в государственные органы информацию электронной подписью без каких-либо требований к ней, то есть *простой электронной подписью*.

Правила использования простых электронных подписей при оказании государственных и муниципальных услуг установлены в статье 21.2 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [5] и Постановлением Правительства РФ от 25.01.2013 № 33 [6]. В со-

ответствии с Правилами идентификатором простой электронной подписи на портале Госуслуги является страховой номер индивидуального лицевого счета (СНИЛС)заявителя - физического лица либо руководителя или уполномоченного им иного должностного лица заявителя - юридического лица, а паролем ключа - последовательность символов, созданная в соответствии с Правилами (формируется самим заявителем).

Анализируя функционирование указанных информационных систем, можно отметить, что ЕСИА входит в состав инфраструктуры электронного правительства и в соответствии с Постановлением Правительства РФ от 08.06.2011 № 451 является неотъемлемой частью инфраструктуры, используемой для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме [7].

Единая биометрическая система является цифровой платформой, которая позволяет гражданину проходить удаленную идентификацию по биометрическим образцам для получения некоторых финансовых услуг. В дальнейшем ЕБС станет национальной платформой для удобного и безопасного доступа граждан к государственным и коммерческим услугам. Размещение сведений в ЕБС осуществляется банками. В перспективе планируется размещение сведений в системе государственными и муниципальными органами и организациями (МФЦ).

Требования по осуществлению идентификации граждан России в Единой системе идентификации и аутентификации и в Единой биометрической системе установлены Постановлением Правительства РФ от 14.07.2018 № 820 [8]. В соответствии с Требованиями *идентификация* – это совокупность мероприятий по установлению сведений о гражданах Российской Федерации и подтверждению достоверности этих сведений с использованием оригиналов документов, надлежащим образом заверенных копий и (или) выписок из оригиналов документов. Возможно использование сведений из информационных систем государственных органов и организаций посредством Единой системы межведомственного электронного взаимодействия (далее – СМЭВ).

Согласие гражданина России, выраженное в письменной форме для размещения своих персональных данных в Единой системе идентификации и аутентификации и в Единой биометрической системе оформляется в соответствии с формой, утвержденной Распоряжением Правительства РФ от 30.06.2018 № 1322-р [9]. Форма содержит паспортные данные заявителя и перечисление сведений, которые он соглашается предоставить в системы. Кроме того, в форму включается информация об уполномоченном сотруднике и организации, которые осуществляют обработку персональных данных и ввод сведений в информационные системы. При идентификации заявителя государственными органами и организациями он лично представляет сотруднику государственного органа и организации следующие сведения:

–фамилия, имя, отчество (при наличии);

–дата рождения;

–место рождения;

–реквизиты документа, удостоверяющего личность (серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения);

–адрес места жительства (регистрации) или места пребывания;

–идентификационный номер налогоплательщика;

–информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (СНИЛС);

–контактная информация (номер абонентского устройства подвижной радиотелефонной связи и адрес электронной почты).

Изменение указанных сведений происходит в автоматизированном режиме в рамках СМЭВ. Изменение паспортных данных производится подразделениями по вопросам миграции МВД России, которые осуществляют выдачу и замену документов, удостоверяющих личность гражданина России. Сведения о всех выданных паспортах в течении одного дня размещаются в государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность (далее - система «Мир»). Система «Мир» функционирует на основании Постановления Правительства РФ от 06.08.2015 № 813 «Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность» [10] и состоит из ведомственных сегментов. Ведомственный сегмент МВД России обеспечивает автоматизацию механизмов сбора, хранения, обработки, распространения и анализа информации в сфере миграционного и регистрационного учета, оформления и выдачи документов, удостоверяющих личность.

Ведомственный сегмент Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации обеспечивает информационное взаимодействие ведомственных сегментов между собой, а также информационное взаимодействие ведомственных сегментов с иными информационными системами путем использования межведомственного резервированного центра обработки данных.

Таким образом, после замены или выдачи паспорта подразделениями МВД России сведения о новых документах, удостоверяющих личность гражданина России, вносятся в ведомственный сегмент МВД России в системе «Мир». Затем, через ведомственный сегмент Минкомсвязи России в системе «Мир», осуществляется автоматическая передача введенных данных посредством СМЭВ в Единую систему идентификации и аутентификации. После выдачи паспорта у гражданина появляется возможность в получении сведений о действительности/недействительности его паспорта с использованием сети Интернет через Единый портал (Портал Госуслуг).

В Единой биометрической системе размещаются следующие сведения:

1. Биометрические персональные данные физического лица - гражданина Российской Федерации следующих видов:

–данные изображения лица человека, полученные с помощью фото- видео устройств;

–данные голоса человека, полученные с помощью звукозаписывающих устройств.

2. Основной государственный регистрационный номер государственного органа, банка, иной организации, разместивших в электронной форме в системе биометрические персональные данные гражданина России.

3. СНИЛС сотрудника уполномоченной организации, разместившего биометрические персональные данные гражданина РФ в системе.

4. Идентификатор учетной записи в ЕСИА физического лица, биометрические персональные данные которого размещаются в системе. Таким образом, несмотря на то, что Единая биометрическая система является отдельной информационной системой, она непосредственно связана с Единой системой идентификации и аутентификации.

5. Контактные данные физического лица – номер телефона и адрес электронной почты.

Поясняя, почему в проекте используются вместе такие два типа биометрии, как голос и лицо, Ростелеком указывает, что сегодняшний день лицо и голос – самые распространенные и доступные для массового использования биометрические модальности, другие требуют специального считывающего оборудования. Пересдача биометри-

ческих данных для их актуализации предусмотрена внепланово при критических травмах или планово с периодичностью один раз в три года.

Использование отпечатков пальцев посредством сканера в смартфоне не применяется из-за низкой чувствительности сканера и закрытого программно-аппаратного обеспечения вендора смартфона (программное обеспечение произведено за пределами Российской Федерации и не может обеспечить должный уровень безопасности обработки биометрических персональных данных) [11]. Обработка биометрических персональных данных в государственных органах, банках и иных организациях осуществляется в соответствии с мерами по обеспечению безопасности персональных данных при их обработке, предусмотренными статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [12].

Распоряжением Правительства РФ от 22.02.2018 № 293-р функции оператора системы возложены на публичное акционерное общество междугородной и международной электрической связи «Ростелеком» [13].

Центральный банк Российской Федерации в целях контроля и надзора за выполнением банками мер по обеспечению безопасности персональных данных совместно с Публичным акционерным обществом «Ростелеком» издал Указание № 4859-У, № 01/01/782-18 от 09.07.2018. Указание утвердило перечень угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях [14].

Сведения, содержащиеся в Единой биометрической системе, могут предоставляться оператором ЕБС в МВД России и ФСБ России в целях обеспечения обороны страны, безопасности государства, охраны правопорядка и противодействия терроризму в соответствии с Правилами, утвержденными Постановлением Правительства РФ от 28.12.2018 № 1703 [15]. Предоставление сведений осуществляется Ростелекомом на основании мотивированного запроса МВД России и (или) ФСБ России и их территориальных органов посредством использования Единой системы межведомственного электронного взаимодействия.

Работа над созданием системы началась в 2017 году. Разработку системы полностью финансирует «Ростелеком», который планирует вложить в нее 1.5 млрд. рублей. Оборудование для снятия биометрических данных приобретают и обслуживают банки. С 29.12.2020 в соответствии с Федеральным законом от 27.12.2019 № 480-ФЗ «О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации» доступ в Единую биометрическую систему для идентификации граждан, а также заверения их личности при совершении юридически значимых действий в электронном виде, получают нотариусы [16].

Порядок предоставления биометрических персональных данных физического лица по каналам связи в целях проведения его идентификации без личного присутствия посредством сети «Интернет» установлен в главе 3 Методических рекомендаций, утвержденных Банком России 14.02.2019 № 4-МР [17]. Для обеспечения конфиденциальности передаваемой информации при взаимодействии с клиентом рекомендуется применять СКЗИ класса не ниже КС1 на стороне клиента и рекомендуется применять СКЗИ класса не ниже КС3 на стороне банка (пункт 1.1 Указания Банка России № 4859-У, Публичного акционерного общества «Ростелеком» № 01/01/782-18 от 09.07.2018).

Доступ в единую биометрическую систему осуществляется или на Едином портале госуслуг gosuslugi.ru или на портале Единой биометрической системы bio.rt.ru. Процедура удаленной идентификации гражданина с помощью Единой биометрической си-

стемы также осуществляется через мобильное приложение. Удаленный доступ осуществляется через встроенные криптографические средства защиты информации.

В соответствии с пунктом 3.1.2 Методических рекомендаций банкам рекомендуется разработать памятку для клиента, описывающую особенности работы программного обеспечения для удаленной идентификации физического лица с использованием биометрических персональных данных на мобильном устройстве клиента и описание возможных действий клиента в случае компрометации ключей аутентификации. Порядок получения банковских услуг дистанционно также указан на официальном сайте Единой биометрической системы https://bio.rt.ru.

Со стационарного компьютера с официального сайта ЕБС гражданин перенаправляется на сайт банка или торговой организации. На сайте банка, являющегося участником системы, организована специальная страница для доступа граждан к традиционным банковским услугам в удаленном формате. Например, на сайте Почта банка существует страница «Единая биометрическая система. Ключ к цифровой свободе» [18]. Далее клиент перенаправляется в личный кабинет, в котором осуществляется идентификация гражданина по биометрическим данным. Если клиент обращается в первый раз, то идентификация осуществляется в процессе создания личного кабинета (например, раздел «Давайте знакомиться» Интернет Банка Почта Банка). Далее гражданин входит с банковской страницы в свою учетную запись Госуслуг с использованием пароля в ЕСИА и подтверждает свою личность с помощью Единой биометрической системы. После прохождения процедуры сбора биометрических данных гражданин получает результаты идентификации, затем банк создает клиенту личный кабинет с биометрической идентификацией и доступом к банковским услугам.

С мобильного телефона гражданин входит на сайт банка, который предлагает ему установить мобильное приложение банка, воспользовавшись для осуществления идентификации мобильным приложением «Биометрия», разработанным ПАО «Ростелеком» и доступным для скачивания в GooglePlay и AppStore. Идентификация осуществляется также с использованием учетной записи гражданина на портале Госуслуги с использованием пароля в ЕСИА.

Гражданин для идентификации в системе снимает видео и направляет его в ЕБС. Видео проверяет специальный модуль системы, обрабатывая его алгоритмами двух вендоров - отдельно голос и отдельно изображение лица. После обработки определяется степень схожести с биометрическим контрольным шаблоном в процентах. Результат обработки направляется из ЕБС в банк с одновременной проверкой видео с помощью других биометрических алгоритмов. Если один или несколько из них не идентифицировал гражданина, то в работу включается «модуль аномалий», который анализирует причины расхождений и в случае обнаружения мошеннических действий направляет соответствующее уведомление в банк. При этом, не получает доступ к биометрическим данным пользователей. Банку направляется только результат сравнения биометрических данных пользователя - процент схожести образцов.

Таким образом, в настоящий момент невозможно предоставление гражданином России своих биометрических персональных данных для удаленной идентификации через мобильный телефон, смартфон или планшетный компьютер без использования специального мобильного приложения «Биометрия». Также невозможно предоставление биометрических данных гражданина через стационарный компьютер без использования для удаленной идентификации посредством специального программного обеспечения, размещенного на сайте ЕБС и пароля ЕСИА учетной записи гражданина на портале Госуслуг.

Осуществляя доступ или со стационарного компьютера, или с мобильного устройства, гражданин использует свою запись на портале Госуслуги и пароль в ЕСИА.

Другие способы доступа с использованием биометрических сведений в настоящий момент не предусмотрены.

Создавая личный кабинет, гражданин предоставляет банку право на использование его персональных данных, содержащихся на портале Госуслуги. К таким персональным данным относятся паспортные данные из общегражданского паспорта гражданина РФ, а также его СНИЛС. Гражданин подписывает согласие о предоставлении персональных данных путем ввода пароля ЕСИА учетной записи гражданина на портале Госуслуг, который является простой электронной подписью. В случае личного визита гражданина РФ в отделение банка согласие на обработку его персональных данных, в том числе биометрических персональных данных, должно быть подписано в «бумажной» форме.

Для клиентов – граждан РФ пользование Единой биометрической системой бесплатное, как на этапе сбора биометрических сведений, так и на этапе дальнейшего использования сведений. Для банков основные расходы по пользованию Единой биометрической системой заключаются в необходимости закупки оборудования фиксации биометрических данных. Кроме того, банки должны осуществить расходы по модернизации своих информационных систем и мобильных приложений. Пользование системой является платной для банков. Каждая успешная удаленная идентификация пользователя стоит для банка 200 рублей. Данная сумма распределяется между участниками системы - банком, который ранее зарегистрировал гражданина в Единой биометрической системе, оператором системы («Ростелекомом») и вендорами.

Единая биометрическая система вместе с логином и паролем от Госуслуг ЕСИА позволяет банкам осуществлять банковские операции без личного присутствия гражданина, но с его санкции. В дальнейшем планируется использовать ЕБС для оказания государственных и муниципальных услуг и выполнения функций, операций в финансовом секторе, в здравоохранении и образовании, электронной коммерции и других целях. После охвата системой большей части населения ее разработчики и оператор планируют сделать ЕБС национальной платформой, позволяющей участникам совершать юридически значимые действия, государству проводить выборы, транспортным компаниям идентифицировать пассажиров в транспорте, правоохранительным органам выявлять правонарушителей и обеспечивать безопасность граждан.

Таким образом, с внедрением, и самое главное полноценным законодательным и подзаконным закреплением, Единой биометрической системы, наше общество еще на один шаг приблизилось к всеобъемлющему информационному обществу в котором можно будет осуществлять подавляющее большинство действий, доступных в реальном мире.

Литература

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) // Российская газета. № 165. 29.07.2006.

2. О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»: Постановление Правительства РФ от 28.11.2011 № 977 (ред. от 20.11.2018) // Собрание законодательства РФ. 05.12.2011. № 49 (ч. 5). Ст. 7284.

3. Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина

Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации: Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 13.09.2019) // Собрание законодательства РФ. 09.07.2018. № 28. Ст. 4234.

4. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) // Российская газета. № 75. 08.04.2011.

5. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 27.12.2019) // Российская газета. № 168. 30.07.2010.

6. Об использовании простой электронной подписи при оказании государственных и муниципальных услуг (вместе с «Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг»): Постановление Правительства РФ от 25.01.2013 № 33 (ред. от 20.11.2018) // Собрание законодательства РФ. 04.02.2013. № 5. Ст. 377.

7. Об установлении требований к фиксированию действий при размещении в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также при размещении биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации: Постановление Правительства РФ от 29.06.2018 № 747 // Собрание законодательства РФ. 09.07.2018. № 28. Ст. 4210.

8. Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации: Приказ Минкомсвязи России от 25.06.2018 № 321 (ред. от 04.07.2019) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.07.2018.

9. Об утверждении формы согласия на обработку персональных данных, необходимых для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации: Распоряжение Правительства РФ от 30.06.2018 № 1322-р (ред. от 13.09.2019) // Собрание законодательства РФ. 09.07.2018. № 28. Ст. 4268.

10. Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность: Постановление Правительства РФ от 06.08.2015 № 813 (ред. от 17.12.2019) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.08.2015.

11. Сайт Единой биометрической системы. Раздел «Общие вопросы» [Электронный ресурс]. Режим доступа: https://bio.rt.ru/faq/project/ (дата обращения – 31.05.2020).

12. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) // Российская газета. № 165. 29.07.2006.

13. О возложении на публичное акционерное общество междугородной и международной электрической связи «Ростелеком» функций оператора единой информационной системы персональных данных: Распоряжение Правительства РФ от 22.02.2018 № 293-р // Собрание законодательства РФ. 12.03.2018. № 11. Ст. 1640.

14. О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе: Указание Банка России № 4859-У, Публичного акционерного общества «Ростелеком» № 01/01/782-18 от 09.07.2018 // Вестник Банка России. № 61. 08.08.2018.

15. Об утверждении Правил предоставления оператором единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, в МВД России и ФСБ России сведений, содержащихся в указанной системе: Постановление Правительства РФ от 28.12.2018 № 1703 // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 29.12.2018.

16. О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации: Федеральный закон от 27.12.2019 № 480-ФЗ // Российская газета. № 296. 31.12.2019.

17. Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации: Утв. Банком России 14.02.2019 № 4-МР // Вестник Банка России. № 12. 20.02.2019.

18. Единая биометрическая система. Ключ к цифровой свободе. Сайт Почта Банк. [Электронный ресурс]. Режим доступа: https://www.pochtabank.ru/service/ebs (дата обращения – 31.01.2020).

19. Прокопенко А.Н., Александров А.Н., Дрога А.А. Правовая защита информации (Информационное право): учебное пособие (2-е издание, переработанное и дополненное). – Белгород: Изд-во Бел ЮИ МВД России, 2012. 227 с.

20. Ищенко А.Н., Прокопенко А.Н., Страхов А.А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. № 2. С. 55-62.

21. Прокопенко А.Н., Кривоухов А.А. Правовая политика Российской Федерации в сфере государственных информационных ресурсов // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. 2007.

22. Старостенко И.Н., Шарпан М.В. Об организации электронного документооборота в органах внутренних дел // Вестник Краснодарского университета МВД России. 2013. № 2 (20).

Сведения об авторах

Прокопенко Алексей Николаевич, начальник кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат технических наук, доцент; e-mail: aprokopenko11@mvd.ru.

Жукова Полина Николаевна, профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, доктор физико-математических наук, доцент; e-mail:pnzhukova@mail.ru.

Насонова Валентина Афанасьевна, профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат физико-математических наук, доцент; e-mail: nasonova_valentina@inbox.ru.

Разбегаев Павел Витальевич

ЦИФРОВЫЕ ТЕХНОЛОГИИ В МВД РОССИИ

Новые средства компьютерной техники, программного обеспечения и программных продуктов открывают новые масштабные возможности. Понимание этого уже произошло на высшем государственном уровне, неслучайно Указом Президента Российской Федерации от 9 мая 2017 года № 203 утверждена «Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы»[3], в которой определены цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленных на развитие информационного общества, формирование национальной цифровой экономики, обеспечения национальных интересов и реализацию стратегических национальных приоритетов.

Представляется очевидным, что цифровая экономика не ограничивается сферой бизнеса. Развитие информационного общества затрагивает все ключевые аспекты жизни общества, в том числе правоохранительный сегмент. Кроме того, применение цифровых информационно-коммуникационных технологий открывает новые возможности для предупреждения преступлений и совершенствования правоохранительной деятельности в целом. Поэтому в октябре 2019 года Министерство внутренних дел Российской Федерации заявило в средствах массовой информации о своей готовности внедрять искусственный интеллект в работу. Как сообщил заместитель главы МВД России генерал-лейтенант полиции В.Д. Шулика на заседании круглого стола «Цифровая полиция» в рамках международной выставки «Интерполитех», ведомство готово сделать прорыв в области использования искусственного интеллекта: «Я думаю, что мы совместно с теми, кто готов к нам примкнуть, сделаем серьезный прорыв, потому что при огромном объеме информации нам нужны модели [искусственного интеллекта], которые сотрудники будут анализировать и выдавать рекомендации» [1], – сказал он.

По словам руководства МВД, ситуация в других странах, где используется искусственный интеллект на службе в органах внутренних дел, тщательно мониторится. Об этом на том же заседании сообщил руководитель Главного информационного-аналитического цента (ГИАЦ) МВД России В.В. Агеев: «На мой взгляд, у полиции и органов безопасности нет выбора, и в любом случае мы обязаны развивать искусственный интеллект и брать его на службу. Например, в США есть робот, который патрулирует улицы, в Дубае есть цифровой полицейский участок для приема заявлений граждан без участия сотрудников полиции. Мы в ГИАЦ стараемся все моменты, связанные с использованием искусственного интеллекта, мониторить, участвуем в различных отечественных и зарубежных конференциях» [1], – сказал он.

Очевидно, что на современном этапе внедрение и использование информационных технологий становится одной из приоритетных задач Министерства внутренних дел Российской Федерации и во многом характеризует качество его работы. В настоящее время становится всё более актуальным вопрос оснащения полицейских перспек-

тивными электронными средствами, обеспечивающими их деятельность в едином цифровом информационном пространстве МВД России. Хотя еще относительно недавно подобный процесс был возможен только в голливудских киносценариях.

Так, в 1987 году на широких экранах появился фантастический боевик режиссёра Пола Верховена «Робокоп». Слоганфильмагласит: «Part man. Part machine. All cop. The future of law enforcement» («Частичночеловек. Частично машина. Целиком полицейский. Будущее охраны правопорядка»). В фильме речь идет о проекте «RoboCop» – программе по роботизации полиции города. Затем, в 2002 году, появился американский фантастический триллер Стивена Спилберга, снятый по мотивам одноимённого рассказа Ф.К. Дика, – «Особое мнение». В этом фильме в работе полиции и других спецслужб активно используются инновационные технологии: система тотальной идентификации по радужной оболочке глаза (СканГлаз), система «Precrime» по предсказанию преступлений, анабиозные капсулы для заключенных, нейропрограммирование и т.д.

Сегодня все, что делало указанные фильмы фантастикой, стало реальностью, более того, внедрено в полицейские будни разных стран. По данным аналитиков Markets and Markets, общемировые затраты правоохранительных органов на программные средства и системы достигли по итогам 2018 года $11,6 млрд. Ежегодный среднегодовой темп роста рынка составит 9,3% и к 2023 году достигнет $18,1 млрд. Смарт-технологии становятся одним из основных объектов государственных инвестиций во всем мире.

Так, дубайский робот-полицейский, упомянутый В. В. Агеевым, не единственный пример использования инноваций в работе правоохранительных органов. В 2018 году полиция Дубая отчиталась о появлении в аэропортах робота-таможенника, который способен распознавать лица и отправлять предупреждения о подозрительных пассажирах. Он оснащен системами теплового и рентгеновского сканирования, поэтому может сразу проверять содержимое багажа. Кроме того, улицы городов будут патрулировать самоуправляемые дроны, оснащенные камерой с 360-градусным углом обзора. Они способны выявлять правонарушения и распознавать людей, находящихся в розыске. К 2030 году власти ОАЭ планируют заменить четверть полицейского состава на роботов.

Не отстает и Китай. В марте 2018 года полицейские из Пекина начали тестировать «умные» очки для распознавания лиц и автомобильных номеров. Гаджет, разработанный компанией LLVision Technology, впервые протестировали в китайской провинции Хэнань. С помощью «умных» очков полицейские из Хэнаня задержали 7 подозреваемых и выявили 26 случаев подделки документов менее чем за неделю. Также китайские власти содействуют развитию технологий на основе биометрических данных для выявления преступников. С 2017 года в Китае собирают образцы голосов граждан и отпечатки их пальцев для создания базы данных.

Сингапурская компания ST Kinetics разрабатывает квадракоптер, вооруженный стрелковым оружием. Разработку планируют завершить к 2019 году. На дрон установят легкий пулемет, камеру видеонаблюдения и тепловизор. Аппарат весит 60 кг. Успешные испытания квадракоптера прошли в 2017 году. Сейчас компания дорабатывает разработку: планируется, что дрон сможет находиться в воздухе не менее получаса.

В ряде стран получает активное развитие интеллектуальная аналитика преступлений – это технологии предиктивного анализа и искусственного интеллекта, которые трансформируют информацию в умные сведения, автоматизируют часть функций полицейских. Например, спецслужбы США совместно с компанией Palantir Technologies разработали программу предсказания преступлений, т.е. расчета вероятности того, что кто-то совершит преступление или станет его жертвой. Программа тестировалась с 2012 года полицией Нового Орлеана. Для прогнозирования программа анализировала базы данных, информацию из соцсетей и историю правонарушений человека. Похожую разработку используют в английском городе Дареме. Еще один недавний инновацион-

ный проект в США – искусственный интеллект, способный распознавать объекты и следить за передвижением людей с записи беспилотников. Американские военные работают над технологией совместно с компанией Google. Разработка активно используется с декабря 2017 года.

Возникает вопрос: насколько близка к этим технологиям российская полиция. Открытые источники сообщают, что близка и как никогда. Так, еще в 2010-х годах в МВД РФ начали использовать дроны. Например, летом 2016 года сотрудники Госавтоинспекции Хабаровского края использовали беспилотные летательные аппараты для патрулирования трассы Хабаровск–Владивосток. В первый же день дроны помогли выявить 11 нарушителей ПДД, пересекших двойную сплошную.

Для мониторинга социальных процессов общества, прогнозирования и предупреждения преступлений используются технологии работы с большими данными.

В октябре 2018 года мэр г. Москвы С. С. Собянин сообщил, что свыше 70% преступлений в Москве раскрывается с помощью систем видеонаблюдения. В столице России задействовано более 150 тыс. камер, а данные с них собираются в «Едином центре хранения и обработки данных».

МВД России ведет активную работу по разработке специального программного обеспечения, которое в автоматическом режиме будет искать пробелы и противоречия в законах, фактически выполняя функции юристов.

Институт проблем правоприменения при Европейском университете в г. Санкт-Петербурге проанализировал 4,4 млн сообщений о происшествиях, с которыми люди обращаются в полицию. Объем получился больше 450 экземпляров «Войны и мира». Человек такой объем мог бы осилить только при круглосуточной работе целый год. Работа была поручена самообучаемой нейросети, которая выявляла закономерности в данных и обобщала выводы. Работу технологий поделили на 40 распространенных категорий: «бытовые происшествия», «потери и кражи», «ДТП», «пожары». Это позволило лучше расследовать обстоятельства происшествий.

Наконец,МВД России давно использует роботов для разминирования. Недавно ведомство заявило о закупке робототехнических комплексов под названием «Сфера». Это оборудование может охватывать обзор в 360 градусов. Данные отправляются онлайн на расстоянии до 50 метров от пульта управления. Заряда «Сферы» хватит на час работы. Устройство не боится падений с высоты до трех метров. Оборудование необходимо размещать в непосредственной близости от источника. Внедряется также управляемый досмотровый робототехнический комплекс «Скарабей» взял лучшие характеристики «Сферы», но в отличии от нее он может сам добраться до места назначения. «Скарабей» внешне похож на радиоуправляемую игрушку, а управление ведется с джойстика. Функционал комплекса заключается в передачи видео на расстоянии.

Данные аппараты предназначены для разведки и передачи данных из условий, представляющих опасность людям или из труднодоступных мест. Информация об этом появилась на сайте государственных закупок.

Перечисленные выше технологии, а также другие научно-исследовательские изыскания в декабре 2018 года составили основу для «Концепции научно-технической политики МВД России до 2030 года», разработанной в соответствии с поручением генерал-лейтенанта полиции В.Д. Шулики [2]. В рамках этой Концепции появился проект «ИКТ “Цифровая полиция”» – ключевой инновационный результат НИР «Цифропол», определяющий концептуальный облик «цифровой полиции» будущего, предполагает создание многоуровневой информационно-аналитической системы, базирующейся на единой цифровой платформе, в том числе:

1. инновации в сфере информационно-коммуникационных технологий и цифровой связи МВД России;

2. инновации в сфере создания полицейской робототехники;

3. инновации в сфере создания специальных транспортных средств;

4. инновации в сфере создания специальных технических средств;

5. инновации в сфере создания специального (полицейского) вооружения и боеприпасов к нему.

Данный проект при условии должного кадрового обеспечения является стратегической целью развития облика «цифровой полиции».

Литература

1. Будущее России. Национальные проекты [Электронный ресурс] / Режим доступа: https://futurerussia.gov.ru/nacionalnye-proekty/mvd-rf-gotovo-ispolzovat-iskusstvennyj-intellekt-v-rabote (дата обращения: 21.05.2020).

2. Создание и развитие концептуального облика цифровой полиции // [Электронный ресурс] / Режим доступа: http://www.ormvd.ru/pubs/102/the-creation-and-development-of-a-conceptual-design-of-a-digital-police/ (дата обращения: 21.05.2020).

3. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

Сведения об авторе

Разбегаев Павел Витальевич, кандидат педагогических наук, доцент, начальник кафедры информатики и математикиВолгоградской академии МВД России; e-mail: pavel173@mail.ru.

Старостенко ИгорьНиколаевич

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В ПЕРИОД ПАНДЕМИИ COVID-19

В конце марта 2020 года все образовательные организации как в России, так и в других странах мира вследствие пандемии коронавируса перешли на дистанционное обучение. Индустрия дистанционного обучения очень быстро превратилась в одну из самых быстрорастущих и перспективных,пандемия показала, что информационные технологии станут неотъемлемым механизмом сферы образования.

Тенденция перехода от физического взаимодействия к цифровому, из офлайн в онлайн, не нова. Пандемия только ускорила эти процессы. В первую очередь она стала драйвером перехода всего мира в онлайн и явилась препятствием для традиционного образования. С одной стороны, изменилось многое, с другой, именно от самих участников образовательного процесса зависит принимать или не принимать произошедшие изменения. Было задействовано много технических решений, пришлось учить и учиться в непростых условиях.

В прошедшем локдауне было продемонстрировано, что благодаря развитию технологий люди практически по всему миру смогли физически находиться в изоляции достаточно долгое время, осуществляя при этом свою деятельность в онлайн. И сейчас можно утверждать: то, что доказало свою жизнеспособность в онлайн, теперь будет работать в онлайн, все, что может перейти в диджитал, туда перейдет.

По оценкам экспертов объем мирового рынка онлайн-образования к 2025 году увеличится почти на 70% в сравнении с показателями 2019 года. При этом самые большие темпы роста демонстрируют Юго-Восточная Азия и Россия. Аналитики прогнозируют ежегодный прирост российского сегмента в 20-25% в течение ближайших пяти лет.

Режим самоизоляции научил больше ценить традиционный формат обучения. В стандартных условиях онлайн образованиеявляется только дополнением к традицион-

ному. Безусловно, онлайн образование способно быть актуальным, гибким, доступным, быстрым. Обладает рядом очевидных преимуществ: предоставление широкого выбора образовательных траекторий и ресурсов, создание единой образовательной среды и ее масштабирование, повышение доступности качественного образования, обучение по удобному индивидуальному графику. Кроме того, такая форма существенно сокращает финансовые и временные затраты обучающихся. Однако, фундаментальные знания, основные интеллектуальные навыки развиваются в стенах учебного заведения. Особенно это важно учитывать, если речь идёт о первом – стартовом – высшем образовании.

Любой масштабный кризис приводит к изменению человеческого поведения. Пандемия очень четко продемонстрировала текущие возможности и потенциал как отдельно взятых сотрудников, так и подразделений в целом. Для преподавателя в первую очередь изменились требования к проведению учебных занятий. Нынешним обучающимся сложно долго удерживать внимание на одном предмете, они все хуже концентрируются на одной теме в течение продолжительного времени. Главная функция педагога в таких условиях – создавать среду для обучения и направлять, а не просто транслировать знания. Преподаватель в сложившейся ситуации должен был не просто готовить содержание лекции/практического занятия, а продумывать, как он будет управлять вниманием обучающихся на протяжении всего отведенного времени, меняя и чередуя разные режимы работы с учебным материалом. В этом смысле преподавательская работа в онлайн все больше отождествлялась с режиссерской – с точки зрения управления драматургией процесса.

Еще одним вызовом для профессорско-преподавательского стала адаптация к изменившимся условиям имеющихся и оперативная разработка новых методических материалов. К сожалению, из-за скорости перехода на дистанционное обучение, у преподавательского состава не было возможности перестроить свою работу – в онлайн пришлось перенести офлайновые практики. Очные лекции были заменены вебинарами, вместо письменного домашнего задания – такое же, но в электронном виде.Много времени у преподавателя уходило на работу с файлами в сети Интернет, электронной почтой, облачными хранилищами; установку и изучение принципов работы с новым программным обеспечением; разработку мультимедийных презентаций, компьютерных тестов; использование различных онлайн-платформ и электронных ресурсов.

Именно работа с различными онлайн-платформами, системами видеоконференцсвязи, электронными ресурсами и стала определяющей для всех участников образовательного процесса. Новой культурой в любом учебном заведении стала единая электронная образовательная среда – модель цифрового университета. В современных условиях простое приспособление цифровых инструментов и сервисов под нужды традиционного образования уже не является достаточным условием построения полноценной цифровой образовательной экосистемы ВУЗа. Требуется разработка и внедрение в образовательный процесс эффективной цифровой системы управления университетом, цифровизация образовательного процесса основного и дополнительного профессионального образования, цифровизация траекторий обучения и развитияобучающихся в условиях новой образовательной среды, структуризация цифровых компетенций [9]. Крайне важным представляется интеграция указанных электронных сервисов и модулей, а также успешных практик по разным направлениям в единую электронную среду.

Профессорско-преподавательским составом Краснодарского университета МВД России в период реализации образовательных программ с применением дистанционных технологий использовались различные электронные сервисы и платформы:

– для взаимодействия между участниками образовательного процесса, в том числе синхронное и асинхронное взаимодействие посредством сети Интернет – корпоратив-

ный портал на базе 1С-Битрикс, система управления обучением (СУО) «Moodle», системы видеоконференцсвязи, облачные хранилища;

– для фиксации хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы – система управления учебным процессом «Магеллан»;

– для доступа к электронным библиотечным ресурсам – официальный сайт, электронная библиотечная система IPRBooks.

Корпоративный портал на базе 1С-Битрикс является комплексным решением, позволяющим с одной стороны создать внутренний информационно-коммуникационный ресурс для сотрудников и обучающихся университета, с другой – построить закрытую социально-образовательную сеть для учащихся и преподавателей, интегрированную в учебный процесс.

Система управления обучением «Moodle» (с англ. модульная объектно-ориентированная динамическая обучающая среда) – свободное программное обеспечение, предоставляющее возможность создавать сайты для онлайн-обучения. В период применения дистанционных образовательных технологий Moodle являлся основным средством для создания электронных курсов по преподаваемым дисциплинам, проведения занятий семинарского типа, тестирований.

Преподавательским составом кафедры информатики и математики к моменту перехода на дистанционный формат обучения был разработан ряд собственных онлайн-курсов, которые активно используются в учебном процессе. Кроме того, для взаимодействия между участниками образовательного процесса по дисциплинам информационно-технического блока активно использовалась электронная образовательная среда сетевой академии Cisco. Программа академии включает материалы различных курсов, которые доступны через Интернет, инструменты оценки знаний, средства отслеживания успеваемости обучающихся, практические и тестовые задания. Курсанты получают доступ к интерактивной учебной среде Netspace, которая сочетает в себе качественные облачные сервисы для преподавания, обучения и совместной работы [5].

Для проведения занятий в онлайн-режиме и обратной связи на начальном этапе реализации учебного процесса в период пандемии преподаватели университета были вправе использовать различные инструменты виртуальной коммуникации. Наиболее популярными были такие программные продукты как Zoom, Skype, Youtube, мессенджеры. Преподавательским составом кафедры информатики и математики для проведения вебинаров использовался облачный сервис CiscoWebex. С помощью Webexобеспечивался упрощенный доступ к онлайн-сессиям: участникам конференции не требовалось предварительно инсталлировать программное обеспечение на свои электронные устройства, необходимые модули автоматически устанавливались при входе в конференцию. У каждого пользователя открывалось окно приложения Webex, в котором отображался демонстрируемый преподавателем материал, список участников, окно чата, панель с отображением web-камер. Кроме того, отсутствие сбоев и прерываний при проведении вебинаров, высококачественное видеоизображение в совокупности с функцией автоматического переключения на текущего выступающего, возможность выбора режима видеоконференции, высокий уровень безопасности при совместной работе позволяли осуществлять удаленное взаимодействие в комфортных условиях.

В зависимости от проводимых мероприятий использовались следующие решения CiscoWebex:

WebExMeeting – сервис позволявший обеспечить в режиме реального времени взаимодействие через Интернет до 25 человек одновременно;

WebExTraining – сервис дававший возможность качественно обучать курсантов и слушателей университета до 100 человек.

После введенного министерством внутренних дел России запрета на использование в образовательном процессе программных платформ размещенных или разработанных в иностранных государствах, профессорско-преподавательский состав университета для организации онлайн мероприятий перешел на использование программного продукта TrueConf. При определении модели внедрения ВКС-системы выбор был сделан в пользу выделенного решения. При таком подходе ВКС-система полностью функционировала на внутреннем сервере и контролировалась специалистами отдела информационно-технического обеспечения учебного процесса университета. По этой причине уровень надежности, отказоустойчивости, удобства и безопасности работы ВКС-системы существенно снизился. Периодически случались полное или частичное отсутствие доступа к виртуальным комнатам, прерывания сеансов связи при проведении занятий, низкое качество видеоизображения при предоставлении совместного доступа к учебным материалам, единственный режим проведения конференции – ролевой. В данном режиме не более четырех участников были видны и слышны остальным.

Для успешной организации самостоятельной подготовки обучающихся и предоставления им максимально возможного доступа к учебным, методическим, научным и иным материалам преподавательским составом кафедры активно использовалась электронная образовательная среда (ЭОС) «Виртуальный учебно-методический кабинет» (рис. 1).

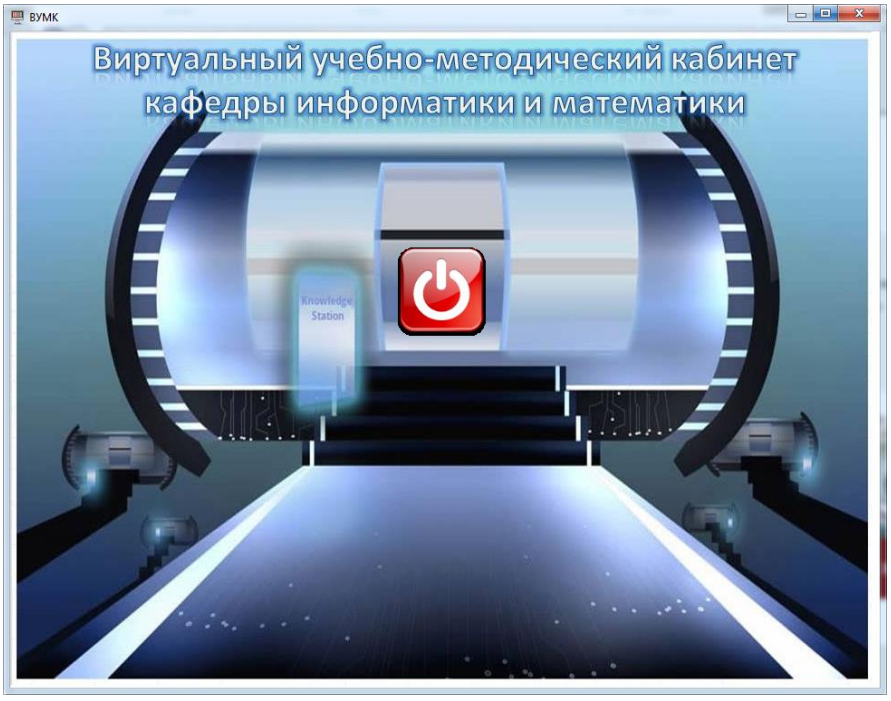


Рис. 1. Электронная образовательная среда «Виртуальный учебно-методический кабинет»

Виртуальная среда, выполняя роль электронного наставника, была призвана минимизировать недостатки присущие другим используемым электронным сервисам и системам, формировать у обучающихся способность воспринимать информацию в нужном месте, в нужное время, учитывать индивидуальные особенности обучающихся, задавать персональный темп обучения, обеспечивать самодиагностику.

В состав ЭОС «Виртуальный учебно-методический кабинет» (рис. 2) были включены учебно-методические комплексы по дисциплинам кафедры, мультимедийные презентации, тестовые задания, ссылки как на сайты глобальной сети Интернет, так и на компоненты электронной образовательной среды университета, различные ви-

деофрагменты, сюжеты, обучающее видео по дисциплинам кафедры, подготовленные на кафедре видеолекции [3].

Учебные материалы нового типа, реализованные в цифровой среде и с помощью цифровых элементов, предполагали, что обучающиеся не только общаются с преподавателем, но и взаимодействуют друг с другом, и делают это еще более качественно, чем в традиционной аудитории.

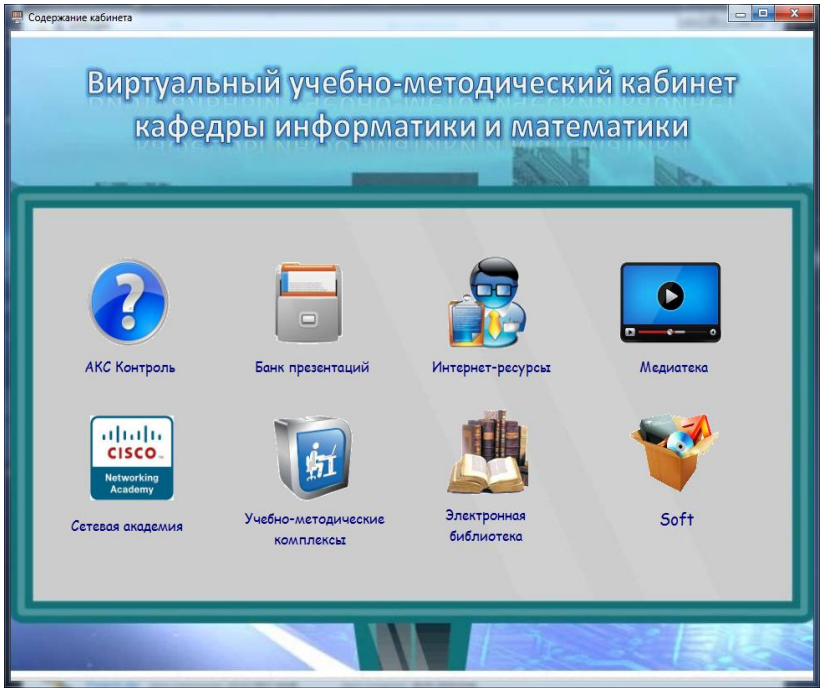


Рис. 2. Состав элементов ЭОС ВУМК

В такой образовательной модели обучающийся в меньшей степени является объектом педагогического воздействия, в большей степени становится субъектом познавательной деятельности, набор необходимых конкретному обучающемуся компетенций выбирает каждый для себя самостоятельно. В настоящее время человек уже не может развиваться в рамках одной образовательной программы. Будущее за обучением в сети образовательных организаций, цифровых платформ, технологических компаний.

Литература

1. Лаптев В.Н. Методы разработки тестовых заданий в автоматизированной контролирующей системе «Контроль» / В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2015. – С. 826-840.

2. Лаптев В.Н. Некоторые аспекты применения среды Visual Basic for Application для создания учебных приложений по математическим дисциплинам / В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2014. – С. 222-233.

3. Старостенко И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

4. Старостенко И.Н. Место и роль электронного обучения в образовательном процессе / И.Н. Старостенко // Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности. –

Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2016. –С. 17-23.

5. Старостенко И.Н. Актуальные вопросы информатизации образования / И.Н. Старостенко // Общество и право. – Краснодар: Краснодарский университет МВД России, 2017. – №4 – С. 274-277.

6. Шотыло Д.М. Информационное обеспечение цифровой трансформации университета / Д.М. Шотыло, В.А. Хвостикова, И.В. Логунова // ФЭС: Финансы. Экономика. – Воронеж: Воронежский государственный технический университет, 2019. – № – С. 58-68.

Сведения об авторе

Старостенко Игорь Николаевич, кандидат физико-математических наук, доцент, начальник кафедры информатики и математики Краснодарского университета МВД Росси; e-mail: staros80@mail.ru.

Трофимец Елена Николаевна,
Петриева Оксана Владимировна

МЕТОДОЛОГИЧЕСКИЕ ПРИНЦИПЫ ОЦЕНКИ И ВЫЧИСЛЕНИЕ ПОКАЗАТЕЛЕЙ ПОМЕХОУСТОЙЧИВОСТИ КАНАЛОВ РАДИОСВЯЗИ В УСЛОВИЯХ ЧС

Вычисление основных показателей, определяющих качество и эффективность систем (каналов) связи в условиях ЧС, таких как своевременность, достоверность и безопасность передаваемых сообщений является достаточно сложной задачей и возможно только при введении ряда упрощающих допущений и ограничений, которые, вместе с тем, не должны существенно искажать реальную картину процессов функционирования канала радиосвязи (КРС) и передачи по нему информации [1]. В качестве основных методологических принципов при разработке оценочных методик следует принять следующие:

1. Оценка показателей эффективности радиосвязи должна базироваться на имеющихся расчетных и статистических данных, характеризующих сигналы и помехи на входах радиоприемных устройств используемых диапазонов волн. Такими величинами, определяющими – помехоустойчивость приёма – информации, являются средние превышения сигнал/помеха в каналах приема и статистические характеристики их флюктуаций, измеренные экспериментально.

2. При оценке помехоустойчивости конкретной системы необходимо учитывать её структуру (число каналов и степень их назначения) и основные составляющие алгоритмов передачи и защиты информации от ошибок, реализованные в данной системе (метод приёма, способ объединении разнесенных каналов, систему синхрофазирования, систему кодирования информации и т. п.).

3. При оценке своевременности радиосвязи необходимо исходить из способа передачи сообщений и — помехоустойчивости используемого КРС, имея ввиду, что принятыми могут быть только достоверные сообщения. Неприём сообщений с требуемой достоверностью при квитанционном обмене всегда приводит к повторению передачи сообщения в той или иной форме и увеличению времени его радиопередачи и доставки. В итоге устанавливаются обменные соотношение между достоверностью и своевременностью связи, что позволяет в конечном итоге установить количественную взаимо-

связь между пространственно-энергетическими параметрами КРС и своевременностью передачи информации при их использовании [2].

Основные показатели помехоустойчивости, такие как своевременность, достоверность (надежность) и безопасность, могут вычисляться либо по эмпирическим данным, характеризующим работу реальных каналов связи, либо по их теоретическим моделям. При оценке эффективности планируемых мероприятий по улучшению качественных характеристик каналов радиосвязи второй путь более предпочтителен, однако требует разработки математических моделей реальных каналов автоматической связи. Линии радиосвязи, в первую очередь декаметрового диапазона, характеризуется быстрыми и медленными изменениями амплитуд напряженностей поля сигналов и помех.

Общепринятым способом учета быстрых замираний (интервал стационарности 5-7 мин.) при оценке эффективности автоматического приёма, является усреднение вероятности ошибочного приёма элементарной посылки за время передачи радиограмм определенного формата:

$P_i = \int_0^\infty P_i(h_i^2) \cdot \varphi(h_i^2) dh_i^2$ где:

$h_i^2 = \frac{P_{ci}}{P_{\text{пі}}}$ – отношение мощностеи сигнала и помехи в i-м канале приёма ($i = \overline{(1, Q)}$),

$\varphi(h_i^2)$ – плотность вероятностей h_i^2,

$P_i(h_i^2)$ – вероятность ошибочного приёма элементарной посылки в каналах с постоянными параметрами (КПсП).

В результате усреднения КПрП (каналы с переменными параметрами) приводится к эквивалентному КПсП с вероятностью ошибочного приема элемента. При этом предполагается, что изменение уровня сигнала из-за быстрых замираний происходит настолько быстро, что условия радиоприёма меняются случайным образом от одной посылки к другой [3, 4]. Это значит, что быстрые замирания влияют только на достоверность приёма сообщений.

Медленные замирания (интервал стационарности 1...2 ч.) учитываются либо путём усреднения результатов приема сообщений по множеству условий приёма, либо путем определения вероятности тех из них, в которых приём информации осуществляется с достоверностью не ниже заданной.

Экспериментально установлено, что распределение уровней сигналов $y_i (y_i = 20lgU_{ci})$ и помех $x_i (x_i = 20lgU_{\text{пі}})$, на входах радиоприемного устройства (РПУ) являются нормальными. Поскольку уровни y_i и x_i, как правило, независимы, то распределение их разности $z_i = y_i - x_i$(превышение сигнала над помехой) также является нормальным с параметрами $z_i = \bar{y}_i - \bar{x}_i$, $\sigma_z = \sqrt{\sigma_{yi}^2 + \sigma_{xi}^2}$.

Параметры уровней сигналов и помех определяются в результате расчета линий радиосвязи по существующим методикам, например ОСТ-В5.

На базе методики оценки надежности приёма дискретных сообщений с достоверностью не ниже заданной (надежностью радиосвязи), основана на рассмотренных способах учета быстрых и медленных замираний сигнала [5]. Недостаток такого подхода, по нашему мнению, состоит в том, что он, во-первых, применим по существу только к одноканальным системам и, во- вторых, не учитывает алгоритмы обработки принимаемых сообщений в конкретных каналах (трактах), поскольку требования по достоверности задаются через допустимую вероятность ошибки элемента на входе канала, а не сообщения в целом на выходе тракта приёма. Оценка эффективности приёма (радиосвязи) по рассмотренным выше показателям устраняют эти недостатки [6-8].

Как отмечено выше, вероятность $P_{\text{пр}}$ зависит как от структурытракта приёма и алгоритма обработки сообщений, так и от условийрадиоприёма, т.е. справедливо соотно-

шение:$P_{\text{пр}} = f\left(A, \vec{Z}\right), \vec{z} = \left\|z_1, z_2, \dots, z_Q\right\|$ – случайный векторпревышений(С/П) на входахканалов многоканального тракта, А – алгоритм обработки сообщения в многоканальном тракте (МТ).

В одноканальных трактах приема имеет место однозначное соответствие между величинами Z и $P_{\text{пр}}$, $P_{\text{ош}}$, p, то есть по заданному допустимому значению одной величины, например, $P_{\text{прд}}=\beta$, можно определить, путем последовательного пересчета $\beta \rightarrow P_{\text{ош}} \rightarrow p_{\text{д}} \rightarrow z_{\text{д}}$– граничное значение другой величины, например $z_{\text{д}}$.

Это позволяет определить надежность радиосвязи как вероятность выполнения условия $P_{\text{пр}}(t) \geq \beta$ по вероятности выполнения более простого условия $z(t) \geq z_{\text{д}}$ (закон распределения z, известен, а закон распределения $P_{\text{пр}}$ - неизвестен).

В многоканальных трактах такого соответствия нет; результат приёма зависит от совокупности величин $z_1, z_2, \dots, z_Q$ То есть одно и то же значение вероятности $P_{\text{пр}}$ может достигаться при различных наборах величин $z_1, z_2, \dots, z_Q$. Более того, из-за взаимного влияния каналов приёма, появляющегося при их объединении в групповой канал, пороговые значения превышений $z_{\text{д}}$, в каналах становятся функционально зависимыми и случайными. Это обстоятельство существенно усложняет вычисление показателей эффективности приёма дискретных сообщений при разнотипных каналах. Если изменение превышений С/П в каналах жестко коррелированы (синхронны), то многоканальная система ведет себя также как одноканальная с пороговым превышением $z_{\text{д}}(Q,\beta)$, зависящим от числа каналов Q и алгоритма обработки сообщения в тракте приёма [9]. Расчет эффективности МТ в этом случае в принципе не отличается от расчета эффективности одноканальной системы.

Литература

1. Киндеев Е. А. Надежность технических систем и техногенный риск: учеб. пособие / Е. А. Киндеев, Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2016, с.1-8.

2. Ермоленко А.А., Мансур И.А., Чемиренко В.П. Модель оценки структурной скрытности информационных сетей. - В сб.: Модели и методы исследования информационных сетей под ред. Буренина Н.И. Выпуск 4. - СПб: Лицей, 2000, с. 106-116.

3. Мансур И.А. Чемиренко В.П. Исследование влияния неоднородности структур на показатели структурной скрытности сетей связи. В сб.: Модели и методы исследования информационных сетей под ред. Буренина Н.И. Выпуск 4. - СПб: Лицей, 2000, с. 125-136.

4. Куделя В.Н., Привалов А.А., Петриева О.В., Чемиренко В.П Методы математического моделирования систем и процессов связи под общ. ред. В.П.Чемиренко. — СПб.: Изд-во Политех. ун-та, 2009. с. 94-105.

5. Батьковский М.А., Трофимец В.Я., Трофимец Е.Н., Фомина А.В.Программно-методическое обеспечение информационно-аналитической подготовки специалистов для оборонно-промышленного комплекса и силовых структур. Вопросы радиоэлектроники. 2016. № 9. С. 123-136.

6. Петриева О.В., Сикарев И.А. Информационные потоки, обрабатываемые информационно-диспетчерской системой. Программныепродуктыисистемы. 2007. № 3. С. 39.

7. Batkovsky A.M., Fomina A.V., Semenova E.G., Trofimets V.Ya., Trofimets E.N. Method for adjusting current appropriations under irregular funding conditions. JournalofAppliedEconomicSciences. 2016. Т. 11. № 5. С. 828-840.

8. Батьковский А.М., Трофимец В.Я., Трофимец Е.Н. Научно-методический аппарат решения аналитических задач в оборонно-промышленном комплексе. Вопросы радиоэлектроники. 2015. № 6. С. 173-193.

9. Ныpков А.П., Петриева О.В., Чистяков Г.Б.Автоматизированное управление высокоточной постановкой средств навигационного ограждения на ВВП РФ с использованием ГЛОНАСС. Методы и технические средства обеспечения безопасности информации. 2010. № 19. С. 44-45.

Сведения об авторах

Трофимец Елена Николаевна, кандидат педагогических наук, доцент, заведующая кафедрой высшей математики и системного моделирования сложных процессов Санкт-Петербургскогоуниверситета ГПС МЧС России; e-mail:ezemifort@inbox.ru.

Петриева Оксана Владимировна, кандидат технических наук, доцент, доцент кафедры высшей математики и системного моделирования сложных процессов Санкт-Петербургскогоуниверситета ГПС МЧС России; e-mail: oksenj_pet@mail.ru.

Тимофеев Виктор Владимирович,
Кирюшин Иван Иванович

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ

С развитием «всемирной паутины» практическикаждый человек ежедневно пользуется ее ресурсами. Известно, что глобальная сеть, преждевсего, является неиссякаемымисточником информации и полем для виртуального общения. Однако далеко не все знают, какойущерб может бытьнанесен персональному компьютеру и самому пользователю. Безопасность в интернете представляет собойпринятие необходимых мер, обеспечивающихзащиту от компьютерных вирусовразличной сложности, а также от взлома ПК злоумышленниками с цельюзавладения личной или корпоративной информацией.

Примером недостаточной информационной защищённости объектов информатизации образовательных организаций, в том числе высшего образования, могут служить несанкционированные трансляции постороннего контента, зачастую ненормативного содержания [1,2].

Информационная безопасность в сети предполагает, прежде всего, знакомство пользователя с основными источниками и алгоритмами действий, которые могут представлять реальную или потенцеальную угрозу.

Наиболее распространенными из них, как известно, являются:

- социальная инженерия, основанная на определенных психологических уловках и орентировланная надоверчивых пользователей;
- большинство вирусов скрыты в различных бесплатных программах загрузки;
- компьютерное заражение может происходить через так называемые программные дыры, которые умело используют хакеры;
- часто вирусы внедряются посредством фишинга (организация фальшивых сайтов, копирующих страницы популярных компаний), существует и множество других способов компьютерного мошенничества [1,5].

При более детальном рассмотрении вопроса обеспечения информационной безопасности, становится очевидным, что данная цель является многофакторной, комплексной задачей. Ее решение плотно связано с техническими характеристиками надёжности и устойчивости программно-аппаратного комплекса вычислиельных средств, задействованных в обработке информации конечного пользователя системы.

Сами угрозы информационной безопасности также имеют совершенно различный характер. Они могут быть преднамеренными и случайными, сам источник их возникновения может быть антропогенным, либо естественным. Очевидно, что и меры борьмы с ними должны радикально различаться.

Целями неправомерного доступа к информационным ресурсам являются кража учетных записей от авторизируемых ресурсов, паролей почтовых ящиков, различных сайтов, а также электронных кошельков; реализация рекламных рассылок со сторонних ПЭВМ.

Известно, что в процессе регистрации пользователю предлагается ввести свои персональные данные, а также, зачастую, предоставить фотографию, предлогается заполнить данные о месте учебы, работы, указать номер мобильного телефона, чтобы получать на него смс-сообщения.

В целях уменьшение угрозы утечки персональных данных рекомендуется использовать корректные настройки параметров конфиденциальности. Ваш профиль должен быть виден только вашим друзьям. Это также относится к публикации статусов и сообщений в ленте, на вашей стене и т. д.

Встречающийся во многих популярных источниках подход к реализации информационной безопасности вычислительных средств и систем исключительно путём использования антивирусного программного обеспечения является достаточно примитивистским, ориентированным на малоквалифицированных пользователей ПЭВМ [3,4].

Этот подход вреден ещё и тем, что неизбежно формирует в обществе большую массу пользователей, безосновательно уверенных в информационной защищённности своей вычислительной системы и, зачастую, узнающих, что что-то с безопасностьюих системы «не так», когда безвозвратно утеряны важные данные или нарушена работа этой самой системы.

Средство обеспечения безопасности, в том часле программные, не должны снижать производительность вычислительных устройств, в прортивном случае пользователь пудет игнарировать их использование.

Отдельного внимания заслуживает и сетевая инфраструктура организации или учреждения. Кабельное хозяйство, проложенное с нарушением требований по его монтажу в части топологии размещения, длины сегментов, а также норм электромагнитной совместимости, может в существенной степени снизить пропускную способность и даже, в отдельных случаях, полностью нарушить работу информационной системы. В то время, как сам кабель может быть и очень высокого качества, от известного производителя, заслуживающего абсолютного доверия. В этом случае постоянные сбои и задержки в работе локальной сети будут маскировать для пользователя деятельность вредоносных программ.

Свою лепту в сложившуюся ситуацию информационной незащищенности вычислительных средств и систем различного назначения вносят и, если сказать мягко, странные до нелепости технические стандарты электронных платёжных систем, например, размещения на обратной стороне банковских карт CVV-кода позволяющего реализовывать удаленные платежи, не используя PIN-код в то время, как PIN-код по своей сути – информация аналогичного назначения, выдается держателю карты в запечатанном конверте, содержание которого скрыто даже от сотрудников банка.

В отношении рассматриваемой проблемы сетевое оборудование также уязвимо для действий квалифицированного злоумышленника, поскольку передаваемая посредством его использования информация об учётных записях или ссылках для подключения к определённым информационным ресурсам содержится в служебной информации, сопровождающей пакеты данных пользователя, пересылаемым при работе в сети.

Отдельно следует отметить и определенную безнаказанность лиц, осуществляющих действия по распространению вредоносного программного обеспечения (ПО), нарушению работы сетей и систем ПЭВМ. Если громкие резонансные дела и факты как-то расследуются правоохранительными органами, то факты хулиганских выходок и тому подобные действия, не повлекшие тяжких последствий, сходят нарушителям, а зачастую и преступникам с рук.

Из сказанного можно сделать вывод, что основным фактором обеспечения необходимого уровня информационной безопасности является уровень информационной грамотности пользователя при работе на ПЭВМ, а особенно с сетевыми ресурсами и электронной почтой. При настройке и администрировании ПЭВМ и вычислительных систем необходимо оптимально настраивать параметры безопасности. При этом достаточно большое значение имеет этап постановки задачи администратору и необходимость наличия у него четкого представления о распределении функциональных обязанностей и полномочий между персоналом организации.

При обработке пользователем сообщений, связанных с денежными средствами и платежами, необходимо быть максимально внимательным, особенно обрабатывая почту от неизвестных адресатов.

Достаточно эффективным средством повышения информационной безопасности организации со стороны работодателя следует считать своевременное повышение квалификации персонала, связанного с обработкой данных на ПЭВМ.

Литература

1. Башлы П.Н. Информационная безопасность / П.Н. Башлы. – Ростов н/Д: Феникс, 2006. – 253 с.

2. Мельников В. П. Информационная безопасность: Учеб. пособие для сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. – М.: Издательский центр «Академия», 2005. – 336 с.

3. Тимофеев В.В. Особенности совершения и расследования отдельных преступлений, совершаемых с применением специальных технических средств.Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2018. № 1 (4). С. 118-123.

4. Тимофеев В.В. Проблемные вопросы обеспечения качества реализации образовательного процесса по дисциплине «Специальная техника ОВД». Вестник учебного отдела Барнаульского юридического института МВД России. Выпуск № 35 – Барнаул: БЮИ МВД России, 2020. С. 42-44.

5. Юрьева, Т. Ю. Словарь информационных продуктов и услуг / Т.Ю. Юрьева. - Кемерово: - РОСТИКС,2006.- 50 с.

Сведения об авторах

Тимофеев Виктор Владимирович,кандидат технических наук, доцент кафедры информатики и специальной техники Барнаульского института МВД России; e-mail: v.v.timofeev@bk.ru.

Кирюшин Иван Иванович,преподаватель кафедры информатики и специальной техники Барнаульского института МВД России; e-mail:kii22@rambler.ru.

Федосеев Алексей Эдуардович,
Федосеев Андрей Эдуардович,
Архипцев Иван Николаевич

АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СИСТЕМ ПРИ ПРОВЕДЕНИИ МОНИТОРИНГА В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Современный образовательный процесс неразрывно связан с использованием современных информационных технологий. Данная связь прослеживается на всем этапе обучения. Использование систем и ресурсов – необходимое составляющееинформационной сферы любой образовательной организации. Как правило, образовательная организация располагает сторонними информационными ресурсами и ресурсами, разработанными собственными силами. Ряд информационных систем образовательной организации используют как услугу по платной подписке. Все информационные ресурсы в той или иной степени необходимы. Но их порядок использования в образовательных организациях различен.

Методика информатизации образовательных организаций.

Мировые тенденции эффективного функционирования образовательной организации включают [1]:

1) устойчивость и эффективность управления вузом на основе информационных технологий;

2) обеспечение обучающихся информационными ресурсами по реализуемым образовательным программам.

Информатизация - это процесс разработки, создания и массового применения современных информационных средств и технологий для удовлетворения потребностей человека и общества. (в том числе телекоммуникационных, мультимедийных, интеллектуальных)[2].

Целью информатизации является обеспечение качественного доступа к различныминформационным ресурсам[2]. Мониторинг может выступать средством организации управления. С методологической точки зрения, с позиции работы Н.В. Абрамовских, мониторинг выступает мыслительной деятельностью, безразличной к предметному содержанию и научной специальности [3]. В.П. Савчук считает мониторинг методом научно-практической активности, цель которого состоит в получении и обработке упреждающей информации о состоянии системы и тенденциях ее развития [4]. Л.А. Чурина рассматривает мониторинг в виде системы исследования процесса, объекта с целью получения достоверной информации для эффективного управления средой, процессами, программами развития [5]. А.Н. Майоров с позиции образования даёт понятие мониторинга как процесса непрерывного научно обоснованного, диагностико-прогностического слежения за состоянием, развитием педагогического процесса в целях оптимального выбора образовательных целей, задач и средств их решения, основанный на сборе, обработке, хранении и распространении информации об образовательной системе или отдельных ее элементах [6].

Пути реализации эффективной информатизации в образовательной организации.

Данные мировые тенденции указывают на особую роль информатизации в современной образовательной организации. По мере развития информационных технологий данный фактор принимает различные формы. Информатизация на текущем этапе своего развития выступает мерой обеспеченности общественно значимого вида человече-

ской деятельности. В настоящий момент существуют различные программные продукты. Ряд систем направлены на обеспечение учебного процесса, управления образовательной организации, сопровождения научно-исследовательской деятельности. Подобно продолжающемуся развитию вычислительной техники, развитию программных решений для создания информационных ресурсов, продолжается и развитие программных решений для обеспечения образовательной организации.

Данное направление развития ставит основную цель к последующим разрабатываемым системам для образовательной организации, а именно: повышение эффективности активного воздействия на социальный процесс управления с последующим повышением качества оказываемых услуг образовательной организации. Данный фактор является актуальным, так как образовательные организации активно участвуют в борьбе на рынке оказания образовательных услуг. Фактор конкуренции в настоящий момент оказывает такое же влияние для образовательных организаций, как и для коммерческих организаций.

В процессе проведения информатизация должны быть решены задачи на различных уровнях:

- для руководителей образовательной организации необходимо предусмотреть эффективное обеспечение достоверной информацией о деятельности подразделений образовательной организации и обеспечить возможность поддержки принятия управленческих решений;

- для преподавательского состава актуальным является обеспечение информационными ресурсами учебного процесса и научной деятельности, а также полноценное использование мультимедийных технологий в учебном процессе;

- для обучающихся необходим доступ к учебно-методической и научной информации, необходимой для освоения реализуемой образовательной программы.

В итоге для повышения эффективности функционирования информационной структуры образовательной организации необходимо внедрить средства проведения мониторинга, которые призваны повысить эффективность применения управленческих решений и своевременного адекватного реагирования на возникающие ситуации.

Просматривая различные точки зрения понятия мониторинга можно выделить его фундаментальные составляющие. Мониторинг представляет собой процесс постоянного вычленения данных об исследуемом объекте. Данные анализируются с целью получения текущей оценки состояния и прогнозирования перспектив развития. Получаемые оценки призваны обеспечить информационные потребности в поддержке принятия управленческих решений и обеспечения информационных потребностей пользователей данных инструментальных возможностей.

Для полноценного внедрения мониторинга в образовательной организации с согласованием процессов информатизации необходимо решить ряд недостатков, которые присущи различным образовательным организациям:

- согласованная с программой развития образовательной организацией единой концепции информатизации;

- учет состояния главных проблем образовательной организации при распределении средств на решение важных задач информатизации;

- документальное регулированиеинформационного взаимодействия;

- сопряжение различных систем и подсистем образовательной организации в виде централизованной системы;

- обеспечение автоматизации важных процессов образовательной организации;

- обеспечение доступа к информационных ресурсам и системам образовательной организации.

Таким образом, в статье сформулирована важность информатизации образовательной организации. Выделены уровни обеспечения информатизации. Определена роль мониторинга вобразовательной организации. Определены задачи, решение которых призваны обеспечить повышение эффективности функционирования информационной структуры образовательной организации.

Литература

1. Тимченко В.В. Гарантии качества образования и информатизация вуза // Universum: Вестник Герценовского университета. 2007. №12. URL: https://cyberleninka.ru/article/n/garantii-kachestva-obrazovaniya-i-informatizatsiya-vuza (дата обращения: 11.06.2020).

2. Дубовская Л.В., Шикульская О. М. Концепция комплексной информатизации современного вуза // НиКа. 2010. URL: https://cyberleninka.ru/article/n/kontseptsiya-kompleksnoy-informatizatsii-sovremennogo-vuza (дата обращения: 11.06.2020).

3. Абрамовских Н. В. Педагогический мониторинг воспитания познавательной готовности старших дошкольников к обучению в школе: Дис. канд. пед. наук: 13.00.06. – Екатеринбург, 1999.

4. Савчук В.П. Мониторинг текущего состояния предприятия // Финансовый директор. 2004. № 1.

5. Чурина Л.А. Мониторинг учебной деятельности в инновационном образовательном учреждении как фактор рефлексивного управления: Дис. канд. пед. наук. 13.00.01. – М., 2002.

6. Майоров А.Н. Мониторинг в образовании. – М.: Интеллект-центр, 2005.

7. Федосеев А.Э., Михайликов В.Л., Баранов В.М. Архитектура взаимодействия модулей подсистемы сбора мониторинговой информации о деятельности в образовательной организации // В сборнике: Проблемы информационного обеспечения деятельности правоохранительных органов сборник статей 5-й Международной научно-практической конференции. 2019. С. 78-82.

8. Федосеев А.Э. Модель информационного процесса проведения рейтинга в образовательной организации как система обслуживания случайных потоков // В сборнике: Информационные технологии в науке, образовании и производстве (ИТНОП-2018) VII Международная научно-техническая конференция. Сборник трудов конференции. 2018. С. 352-354.

9. Маматов А.В., Немцев А.Н., Штифанов А.И., Загороднюк Р.А., Беленко В.А., Немцев С.Н. Разработка комплекса программных средств поддержки дистанционного обучения «Пегас» // Информационные технологии в науке и образовании. Материалы международной научнопрактической Интернет-конференции и семинара «Применение MOODLE в сетевом обучении». - Шахты: Изд-во ЮРГУЭС, 2007. - С.27-32.

10. Немцев С.Н., Штифанов А.И., Беленко В.А., Загороднюк Р.А., Федосеев А.Э. Автоматизированная информационная система мониторинга учебного процесса (Электронная школа) // Открытое и дистанционное образование. 2012. № 3 (47). С. 39-46.

11. Немцев А.Н., Штифанов А.И., Беленко В.А., Загороднюк Р.А., Немцев С.Н., Гальцев О.В., Федосеев А.Э. Автоматизированная информационная система предоставления электронных услуг в сфере образования // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2012. № 1 (120). С. 203-215.

Сведения об авторах

Федосеев Алексей Эдуардович, преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail:Alexs_Fedoseev@mail.ru.

Федосеев Андрей Эдуардович, инженер-электроник отделения планирования и контроля качества учебного процесса и практики учебного отдела Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: Andy_Fedoseev@mail.ru.

Архипцев Иван Николаевич, кандидат юридических наук, старший преподаватель кафедры уголовно-правовых дисциплин Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: arhiptsevin@yandex.ru.

Чубырь Наталья Олеговна,
Гудза Виталий Александрович,
Кириллова Евгения Вадимовна

АСИМПТОТИЧЕСКОЕ РЕШЕНИЕ КРАЕВОЙ ЗАДАЧИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ НЕСТАЦИОНАРНОГО ПЕРЕНОСА ИОНОВ 1:1 СОЛИ В ДИФФУЗИОННОМ СЛОЕ ВОЗЛЕ КАТИОНООБМЕННОЙ МЕМБРАНЫ ПРИ ДОПРЕДЕЛЬНЫХ ТОКАХ

Исследование структуры диффузионного слоя ионообменной мембраны является важным для понимания процесса переноса ионов в электромембранных системах. В данной работе рассматривается обедненный неподвижный диффузионный слой, примыкающий к ионообменной мембране. Основной целью является исследование структуры диффузионного слоя с течением времени. Исследуется одномерная нестационарная математическая модель переноса бинарного электролита в диффузионном слое в потенциостатическом режиме, с помощью уравнений Нернста-Планка и Пуассона. Построено новое асимптотическое решение. Оригинальной особенностью предложенного асимптотического метода является, то, что он основан не только на асимптотических упрощениях в уравнениях, но и на замене точного строения диффузионного слоя приближенным.

Система одномерных нестационарных уравнений нернста-планка и пуассона в безразмерной форме:

$$\frac{\partial C_i}{\partial x} = -z_i C_i \frac{\partial \varphi}{\partial x} - j_i, \qquad i = 1,2; \tag{1}$$

$$\varepsilon \frac{\partial^2 \varphi}{\partial x^2} = C_1 - C_2, \qquad x \in (0,1); \tag{2}$$

$$\frac{\partial C_i}{\partial t} = -D_i \frac{\partial j_i}{\partial x}, \qquad i = 1,2. \tag{3}$$

Краевые условия в безразмерной форме имеют вид:

при $x = 0$:

$$C_1(0,t) = 1, C_2(0,t) = 1, \varphi(0,t) = 0 \tag{4}$$

при $x = 1$:

$$C_1(1,t) = C_{1m}, \left(\frac{\partial C_2}{\partial x} - z_2 C_2 E \right)(1,t) = 0, \varphi(1,t) = \Delta_r \varphi \tag{5}$$

Начальное условие приТ=0:

$$C_1(x,0) = 1, C_2(x,0) = 1, \varphi(x,0) = 0 \tag{6}$$

Для решения этой задачи предлагается использовать некоторую модификацию метода погранслойных функций, которая заключается не только в использовании уравнений для регулярных и погранслойных функций[1-3], но и в асимптотическом упро-

щении области их решений. Это позволяет нам найти приближенное аналитическое решение краевой задачи.

На рисунке 1а показана точная структура диффузионного слоя, а на рис 1б) упрощенная структура.Вся левая граница области пространственного заряда является криволинейной. Она должна определяться в ходе сращивания асимптотических решений. Эта граница с большой точностью может быть аппроксимирована вертикальной асимптотой. В связи с этим, за левую границу квазиравновесной области с большой точностью, можно принять вертикальную асимптоту $x = x_c$.

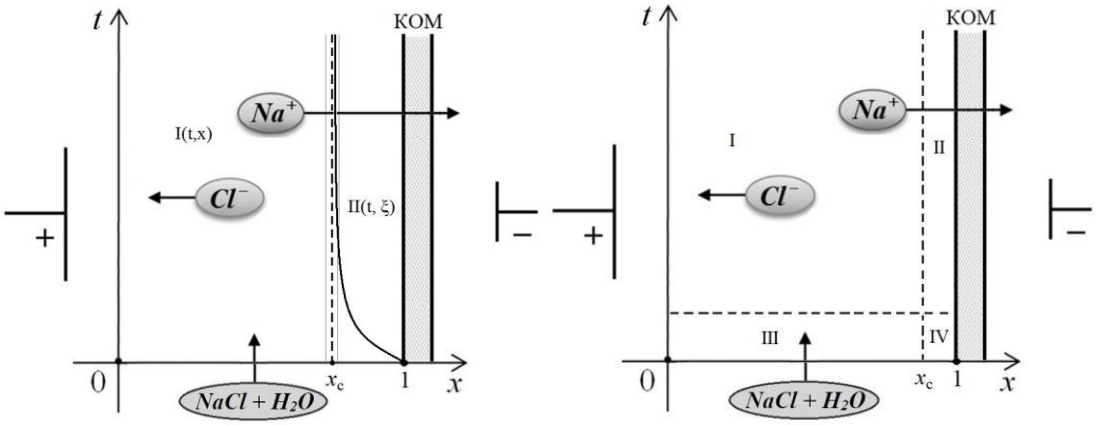


Рис.1 Схема строение области диффузионного слоя

Таким образом, при асимптотическом решении будем считать, что область $\Pi = \{(x,t) \in [0,1] \times [0,+\infty]\}$вдопредельном случае приближенно разбивается на две прямоугольные подобласти (рис. 1). Область I – область электронейтральности (ОЭН), область II – область квазиравновесного пространственного заряда (погранслой у КОМ).

Очевидно, что такое решение будет плохим приближением в окрестности криволинейной границы, но в остальной области оно будет хорошим приближением.
Будем искать решение в виде:

$$\begin{aligned} C_i(t,x,\varepsilon) &= \overline{C}_i(t,x) + \Pi C_i(t,\xi) + O(\sqrt{\varepsilon}) \\ j_i(t,x,\varepsilon) &= \overline{j}_i(t,x) + \Pi j_i(t,\xi) + O(\sqrt{\varepsilon}) \\ \varphi(t,x,\varepsilon) &= \overline{\varphi}(t,x) + \Pi\varphi(t,\xi) + O(\sqrt{\varepsilon}) \end{aligned} \qquad (7)$$

где $\overline{C}_i(t,x)$, $\overline{j}_i(t,x)$, $\overline{\varphi}(t,x)$ - регулярная часть, А $\Pi C_i(t,\xi)$, $\Pi j_i(t,\xi)$, $\Pi\varphi(t,\xi)$ - пограничные функции [1].

Подставляя (7) в уравнения (1) – (6) и приравняем отдельно регулярные и пограничные функции слева и справа при одинаковых степенях малого параметра находим уравнения и соответствующие краевые условия, решения которых имеют вид:

$$C_1(t,x,\varepsilon) = C(t,x) + \frac{\alpha\sqrt{2}ch(\sqrt{\alpha}\frac{1-x}{\sqrt{\varepsilon}} + d) - \alpha}{2sh^2(\sqrt{\alpha}\frac{1-x}{\sqrt{\varepsilon}} + d)} + \ldots \quad C_2(t,x,\varepsilon) = C(t,x) - \frac{\alpha\sqrt{2}ch(\sqrt{\alpha}\frac{1-x}{\sqrt{\varepsilon}} + d) + \alpha}{2sh^2(\sqrt{\alpha}\frac{1-x}{\sqrt{\varepsilon}} + d)} + \ldots$$

$$\varphi(t,x,\varepsilon) = -\frac{D_1 - D_2}{D_1 + D_2} lnC(t,x) + \frac{\partial\overline{\varphi}(t,0)}{\partial x}\int_0^x \frac{dx}{C(t,x)} + \frac{1}{2} ln\left|\frac{1 + e^{\sqrt{\alpha}(\frac{1-x}{\sqrt{\varepsilon}} + d)}}{1 - e^{\sqrt{\alpha}(\frac{1-x}{\sqrt{\varepsilon}} + d)}}\right| + \ldots$$

$$j_1(t,x,\varepsilon) = -\frac{2D_2}{D_1 + D_2}\frac{\partial C}{\partial x} + \sigma_1(t) + \ldots \quad j_2(t,x,\varepsilon) = -\frac{2D_2}{D_1 + D_2}\left(\frac{\partial C(t,x)}{\partial x} - \frac{\partial C(t,1)}{\partial x}\right) + \ldots$$

Таким образом, для того, чтобы найти эти функции достаточно решить краевую задачу для $C(t,x)$ и определить постоянные d, σ_1 и граничное значение $C(t,1)$.

$$\frac{\partial C}{\partial t} = D\frac{\partial^2 C}{\partial x^2} \tag{8}$$

$$C(t,0)=1, C(t,1)=k_c C_{1m}, C(0,x)=1 \tag{9}$$

$$C(t,1)\frac{ch^2 d+\sqrt{2}chd-2}{sh^2 d}=C_{1m} \tag{10}$$

$$-\frac{D_1-D_2}{D_1+D_2}\ln C(t,1)+\frac{\partial\overline{\varphi}(t,0)}{\partial x}\int_0^1\frac{dx}{C(t,x)}+\frac{1}{2}\ln\left|\frac{1+e^{\sqrt{\alpha}d}}{1-e^{\sqrt{\alpha}d}}\right|=\Delta_r\varphi \tag{11}$$

где $D=\frac{2D_1D_2}{D_1+D_2}$ – коэффициент диффузии электролита.

Задачу (8) – (9) можно решить методом фурье или численно, например, методом конечных разностей. система уравнений (10) – (11) не имеет точного аналитического решения, поэтому необходимо использовать для ее решения приближенные методы, устойчивые относительно ошибок округления, в качестве такого метода предлагается сочетание метода деления отрезка пополам и последовательных приближений, аналогичный методу [4,5].

Таким образом найдено новое асимптотическое решение задачи (1) – (6), которое основан не только на асимптотических упрощениях в уравнениях, но и на замене точного строения диффузионного слоя приближенным. Задачу можно решать асимптотически и без предположения об упрощении границы области электронейтральности и пространственного заряда, но при этом получается достаточно громоздкое решение, трудное для практического использования. Сравнение численного и асимптотического решения показывает совпадение их с хорошей точностью за исключением небольшой окрестности криволинейной части квазиравновесной области пространственного заряда.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-38-90314 Аспиранты.

Литература

1. Васильева А.Б., Бутузов В.Ф. Асимптотические методы в теории сингулярных возмущений. – М., 1990.

2. Chubyr N.O. About one particular solution of QECS tasks // Ion transport in organic and inorganic membranes. Book of abstracts. 2009. pp. 38-40.

3. ЧубырьН.О., КоваленкоА.В., УртеновМ.Х. Численные и асимптотические методы анализа переноса 1:1 электролита в мембранных системах / Краснодар, 2018,106 с.

4. Коваленко А.В., Уртенов М.Х., Чубырь Н.О., Хромых А.А., Узденова А.М., Барсукова В.Ю. Численное решение краевой задачи модели переноса бинарного электролита в приближении закона Ома / Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2012. № 77. С. 335-350.

5. Bulatnikova I.N., Gershunina *N.N.* Algorithmic support of problems of electronic kinematicsARPN Journal of Engineering and Applied Sciences. 2018. Т. 13. № 5.С. 1833-1837.

Сведения об авторах

Чубырь Наталья Олеговна, кандидат физико-математических наук, доцент кафедры прикладной математики, Кубанского государственного технологического университета; e-mail: chubyr-natalja@mail.ru.

ГудзаВиталий Александрович, аспирант кафедрыприкладной математики Кубанского государственного университета; e-mail: flash.wetal@mail.ru.

КирилловаЕвгения Вадимовна, ProfessorFachbereichArchitekturundBauingenieurwesenHochschuleRheinMain, университет Прикладных Наук Рейн-Майн; e-mail: evgenia.kirillova@hs-rm.de.

Шарпан Мария Владимировна

CISCOWEBEX В ДИСТАНЦИОННОМ ОБУЧЕНИИ

Дистанционное обучение сегодня – это вынужденная необходимость, с одной стороны, это престижно, перспективно и удобно, с другой стороны.

На первый взгляд кажется, что онлайн идистанционное обучение это одно и то же, но в действительности это не так. Под понятием онлайн-обучение принято понимать получение теоретических знаний и практических навыков при помощи компьютера или других современных гаджетов, подключенных к Интернету, «в данный момент времени». Такой формат обучения еще называют «e-learning». Оно считается логическим продолжением дистанционного обучения.

Дистанционное обучение – это форма получения образования, при которой преподаватель и обучаемый (школьник, студент, курсант, слушатель) взаимодействуют на расстоянии при помощи информационных технологий. При этом происходит смена привычного сенсорного канала на визуальный, из-за чего возникают новые ситуации и отношения[2]. В условиях этой новой реальности все участники образовательного процесса ведут себя иначе, чем при очном общении. Преподаватель вынужден искать инструменты и средства воздействия на дистанционных обучаемых. Также важным при дистанционном обучении является сотрудничество, доступность и четкость при формулировании заданий и требований и адекватные сроки их выполнения[3].

Основным сходством этих двух форм обучения является – процесс получения новых знаний и навыков без непосредственного контакта с преподавателем. На этом этапе и возникает необходимость выбора информационной технологии, с помощью которой будет осуществляться непосредственный визуальныйконтакт.Так как, на базе КрУ МВД России ведется обучение по различным направлениям и курсам академии Cisco, то было предложено использовать **Webex.**

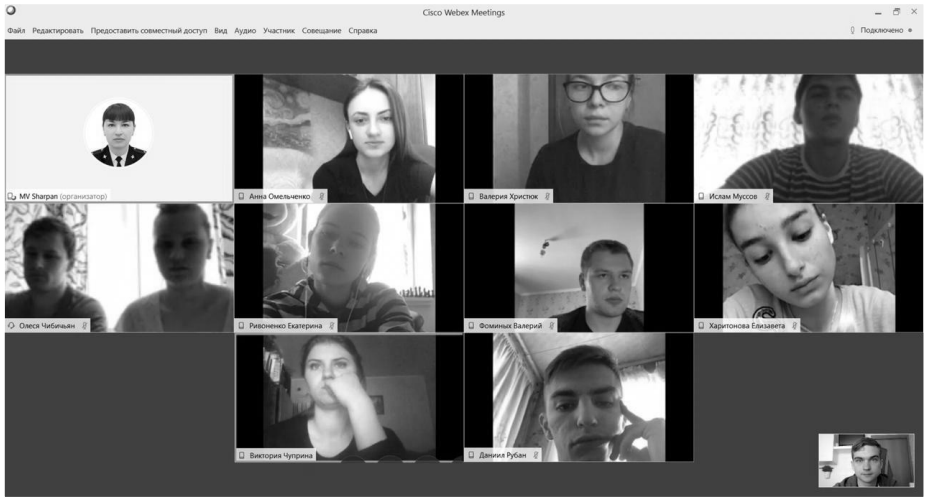


Рис. 1 Иллюстрация проведения группового занятия

Webex– это облачный сервис (платформа) для проведения любых web-конференций, позволяющий участникам обмениваться информацией в любой момент

времени из глобальной облачной среды, в любом месте, используя компьютер или мобильные устройства [1].

Webex отлично зарекомендовал себя при проведении лекционных, семинарских (одновременно до 35 человек) и практических занятий. Интересными и востребованными оказались такие функции как: возможность отключать звук у всех участников занятия, возможность самостоятельно предоставлять обучаемому роль докладчика (например, при устном опросе), возможность вести аудио и видео запись (например, при проведении зачета или экзамена). К сожалению, запись предоставляется не в универсальных форматах, а в собственном формате Webex.

Также, полезными функциями оказались возможность предоставлять совместный доступ к контенту как преподавателя (при объяснении нового материала или новых возможностей той или иной программы)так и к контенту обучаемого (при контроле выполнения практического задания).

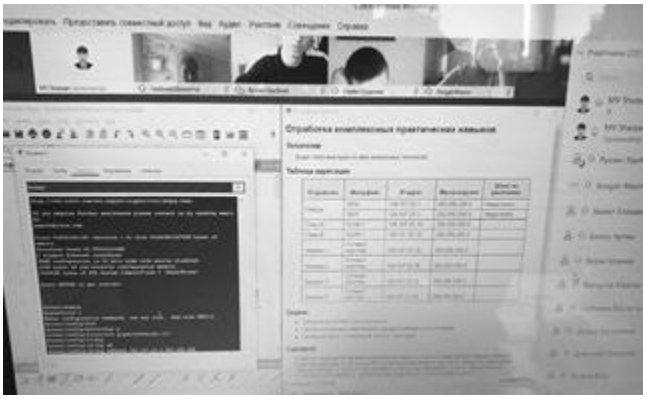


Рис. 2 Иллюстрация возможности предоставление совместного доступа к контенту

Помимо всего перечисленного, также стоит отметить кроссплатформенность, т.е. способность программного обеспечения работать с двумя и более аппаратными платформами и операционными системами.

Рис. 3 Иллюстрация возможности проводить опрос обучаемого с предоставлением совместного доступа к контенту

Единственным существенным недостатком указанного сервиса является то, что он является иностранным программным обеспечением.

Литература

1. https://help.webex.com/ru-ru/ (дата обращения: 01.05.2020 г.).

2. НикуличеваН.В. Использование коммуникаций при дистанционной деятельности тьютора для создания условий индивидуализации образовательногопроцесса// В сборнике: Тьюторство в открытом образовательном пространстве: образовательная ситуация и тьюторская деятельность (ГАОУ ВО Московский городской педагогический университет при участии Межрегиональной тьюторской организации) XII Международная научно-техническая конференция. Сборник трудов конференции. 2019. С. 311-321.

3. Старостенко И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

Сведения об авторе

Шарпан Мария Владимировна, кандидат физико-математических наук,старший преподаватель кафедры информатики и математики Краснодарского университета МВД России, e-mail: marusi2000@mail.ru.

Шкоркина И.В.,
Гудза В.А.,
Уртенов М.Х.

ПРОБЛЕМА РАСЧЕТА ПЛОТНОСТИ ТОКА ДЛЯ НЕСТАЦИОНАРНОГО ПЕРЕНОСА ИОНОВ 1:1 СОЛИ В СЕЧЕНИИ КАНАЛА ОБЕССОЛИВАНИЯ И МЕТОДЫ ЕЕ РЕШЕНИЯ

В данной работе исследуется одномерная нестационарная математическая модель переноса ионов бинарной соли в сечении канала обессоливания, которая описывается уравнениями Нернста-Планка-Пуассона. Новшеством нашей работы являются то, что, во-первых, рассматривается сечение канала обессоливания, а не диффузионный слой, как, например, в работах [1-3]. Это значительно усложняет задачу, но и повышает адекватность модели. Во-вторых, рассматривается потенциодинамический режим, когда разность потенциалов меняется во времени, что позволяет строить и анализировать вольтамперную характеристику (ВАХ).

Рассмотрены различные варианты расчета теоретической ВАХ. Показано, что усредненный ток описывает ВАХ с хорошей точностью. Для вычисления средней плотности тока необходимо использовать математическую модель для расчета тока проводимости.

В данном исследовании в качестве такой модели рассматривается краевая задача, описывающая перенос бинарного электролита через сечение канала обессоливания, образованного анионообменной (АОМ) и катионообменной мембранами (КОМ):

$$\frac{\partial C_i}{\partial t} = -\frac{\partial j_i}{\partial x} \text{ для } i = 1,2$$

$$j_i = -\frac{F}{RT} z_i D_i C_i \frac{\partial \varphi}{\partial x} - D_i \frac{\partial C_i}{\partial x} \text{ для } i = 1,2$$

$$\frac{\partial^2\varphi}{\partial x^2} = -\frac{F}{\varepsilon_a}(z_1C_1 + z_2C_2)$$

$$I_c = F(z_1j_1 + z_2j_2)$$

Здесь φ – потенциал, $E = -\frac{\partial\varphi}{\partial x}$ – напряженность электрического поля, C_i, j_i, D_i, I_c – концентрация, поток, коэффициент диффузии i-го иона, плотность тока. Константы: ε_a – диэлектрическая проницаемость раствора, F – число Фарадея, R – универсальная газовая постоянная. Положим $x = 0$ – соответствуетусловной межфазной границе «АОМ/раствор», а $x = H$ – условной межфазной границе «раствор/КОМ», и в этих точках зададим граничные условия:

При $x = 0$: $\left(\frac{F}{RT}C_1\frac{\partial\varphi}{\partial x} + \frac{\partial C_1}{\partial x}\right)\Big|_{x=0} = 0, C_2(t,0) = C_{2m}, \varphi(t,0) = \Delta_r\varphi = d\cdot t$

При $x = H$: $C_1(t,H) = C_{1m}, \left(\frac{F}{RT}C_2\frac{\partial\varphi}{\partial x} - \frac{\partial C_2}{\partial x}\right)\Big|_{x=H} = 0, \varphi(t,H) = 0$

где d – коэффициент скорости прироста во времени скачка потенциала, имеющий размерность B/c. Начальные условия должны быть допредельными для вычисления ВАХ: $C_{10}(x) = C_0, C_{20}(x) = C_0, \varphi_0(x) = 0$. В данном исследовании предполагается идеальная селективность ионообменных мембран.

Результаты. Для анализа токов, протекающих в системе, нами предложена принципиальная электрическая схема системы сечения канала обессоливания. Эту схему можно представить в виде электрической цепи, содержащей только сопротивление и конденсаторы, в соответствии с рисунком 1:

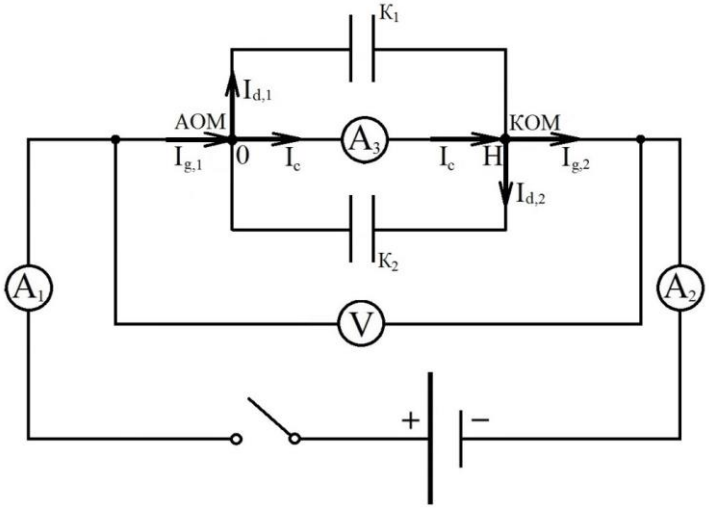


Рис. 1. Электрическая схема сечения канала обессоливания: A_1, A_2 и A_3 – амперметры, V – вольтметр, измеряющий скачок потенциала между точками $x = 0$ и $x = H$

На рисунке 1 изображена принципиальная электрическая схема сечения канала обессоливания. Рассматривается электрическая цепь, которая подключена к внешнему источнику тока. Цепь состоит из униполярного проводника, расположенного на отрезке $[0, H]$ с особыми свойствами, связанными с тем, что в проводнике ток определен переносом ионов, а также двух конденсаторов K_1и K_2, которые моделируют накопление заряда в области пространственного заряда (ОПЗ) у АОМ и КОМ, соответственно. Вольтметр измеряет разность потенциалов сечения канала

обессоливания. Будем считать, что амперметр A_3 имеет произвольное положение и может измерять плотность тока в любой точке отрезка $[0,H]$. Показания амперметров A_1 и A_2 могут не совпадать. Поскольку при замыкании цепи ток $I_{g,1}(t)$ дойдя $x=0$, разветвится на ток переноса $I_c(t,x)$, обусловленный потоком ионов соли, и ток смещения $I_{d,1}(t,x)$,связанныйс возникновением и развитием ОПЗ у АОМ, то точка $x=0$ является узлом и согласно первому правилу Кирхгофа [4],которое вытекает из закона сохранения заряда, справедливо равенство:

$$I_{g,1}=I_c+I_{d,1}$$

Аналогичное равенство справедливо и для узла $x=H$.

Проблемой является неудобство, связанное с использованием амперметра A_3 внутри интервала $(0,H)$, представляющего собой жидкую среду. В то же время вычисления плотности тока в точках $x=0$, и $x=H$ осуществляется со значительной ошибкой, так как для этого необходио вычислять производные концентраций катионов и анионов. Показано, что усредненная плотность тока[5], определенная по формуле:

$$I_{av}(t)=\frac{1}{H}\int_0^H I_c(t,x)dx \qquad (1)$$

позволяет решить эти проблемы.

С помощью платформы для моделирования COMSOLMultiphysics 5.5 были проведены расчеты для численного решения краевой задачи. В качестве исследуемого бинарного электролита был взят KCl для темпа роста скачка потенциала $d=0.01$. ВАХ была рассчитана по формуле (1):

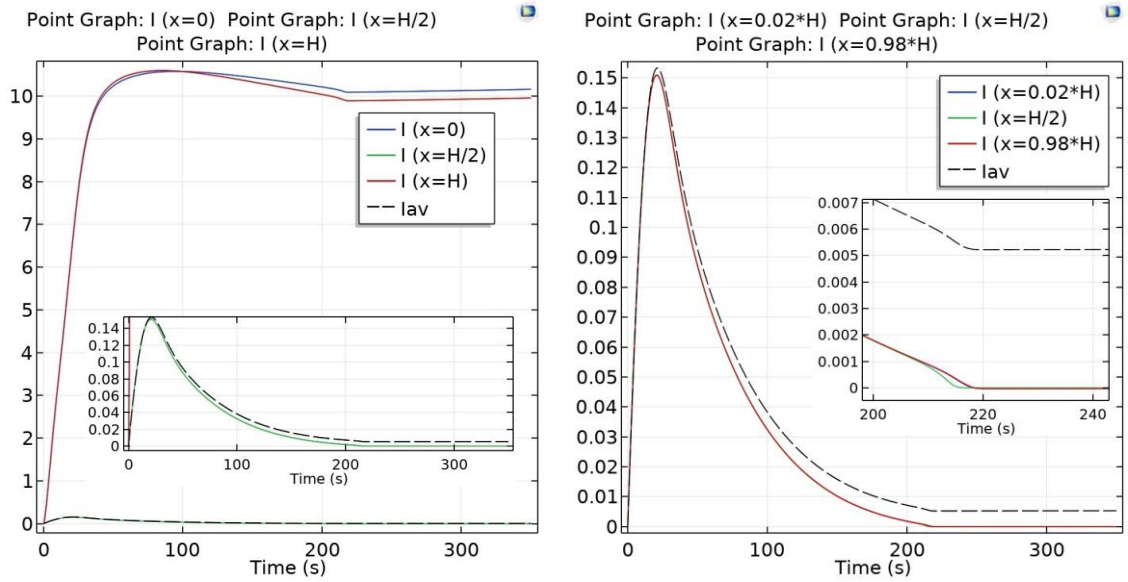


Рис. 2. Графики тока $I_c(t,x)$ в точках $x=0$, $x=0.02H$, $x=H/2$, и $x=0.98H$, $x=H$ и средней плотности тока $I_{av}(t)$, рассчитанной по формуле (1)

Как видно из рисунка 2а, графики функции $I_c(t,0), I_c(t,H/2), I_c(t,H)$ и $I_{av}(t)$ сильно отличаются друг от друга. Это связано с ошибками расчета производной концентрации при вычислении $I_c(t,0)$ и $I_c(t,H)$. В то же время, на рисунке 2б видно, что $I_c(t,0.02H)$, $I_c(t,H/2)$, $I_c(t,0.98H)$ и $I_{av}(t)$ близки друг другу. Следовательно, в ка-

честве плотности тока с хорошей точностью может быть взята средняя плотность тока $I_{av}(t)$, которая устойчива относительно ошибок округления.

Таким образом, в данной работе построена математическая модель переноса ионов бинарной соли в сечении канала обессоливания, принципиальная электрическая схема, и предложена формула для расчёта средней плотности тока. Полученные результаты позволяют строить и анализировать ВАХ для сечения канала обессоливания.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 19-08-00252 А «Теоретическое и экспериментальное исследование вольтамперных характеристик электромембранных систем».

Литература

1. Uzdenova A., Kovalenko A., Urtenov M., Nikonenko V. 1D mathematical modelling of non-stationary ion transfer in the diffusion layer adjacent to an ion-exchange membrane in galvanostatic mode // Membranes. 2018., Т. 8, № 3, С. 84

2. ЧубырьН.О., УртеновМ.Х., КоваленкоА.В., УзденоваА.М. Алгоритмрасчетавольт-амперной характеристикивдиффузионномслоедля мембранных систем в гальванодинамическом режиме / Современные наукоемкие технологии. 2019.№10. С. 92-96.

3. Коваленко А.В., Уртенов М.Х., Чубырь Н.О., Хромых А.А., Узденова А.М., Барсукова В.Ю. Численное решение краевой задачи модели переноса бинарного электролита в приближении закона Ома / Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2012.- № 77. С. 335-350.

4. Сивухин Д.В. Общий курс физики. Том III. Электричество. 4-е изд., стереот. – М.: ФИЗМАТЛИТ; Изд-во МФТИ, 2004. - 656 с

5. Urtenov M.Kh., Kovalenko A.V., Sukhinov A.I., Chubyr N.O., Gudza V.A. Model and numerical experiment for calculating the theoretical current-voltage characteristic in electro-membrane systems // IOP Conference Series: Materials Science and Engineering Collection of materials of the XV International Scientific - Technical Conference. DonStateTechnicalUniversity. 2019. С. 012030

Сведения об авторах

Шкоркина Инна Владимировна, аспирант кафедры прикладной математики Кубанского государственного университета; e-mail: shkorkina_inna@mail.ru.

Гудза Виталий Александрович, аспирант кафедры прикладной математики Кубанского государственного университета; e-mail: flash.wetal@mail.ru.

Уртенов Махамет Хусеевич, доктор физико-математических наук, профессор, заведующий кафедры прикладной математики Кубанского государственного университета; urtenovmax@mail.ru.

ЩербаковВикторАндреевич,
ВасинОлегИванович,
Рыскин Сергей Васильевич,
Кулаков Андрей Анатольевич

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Искусственный интеллект (ИИ) – это многообещающие, еще не осознанные возможности и трудно прогнозируемые сегодня угрозы.

Решимость в использовании новейших технологий и передовых методов управления для достижения и поддержания превосходства над соперником (противником) нашло свое отражение и в стратегиях развития ИИ ведущих государств мира. Последние достижения технологий машинного интеллекта и искусственных

нейронных сетей подают надежду на создание сверхспособной интеллектуальной системы. Начался очередной виток гонки среди более 30 государствза технологическое превосходство путем реализации своих национальных стратегий развития ИИ [1].

Человечество пока еще не осознало, что это за феномен ИИ, и какова его роль во всех областях нашей жизни, в том числе и в военной, к каким результатам и последствиям может привести монополия на его владение, особенно если он станет оружием кибер, психологической и информационной войн. Однако индустрия ИИ и машинного обучения сегодня стремительно растет и внедряется во все сферы деятельности государств, в том числе и в военную.

Искусственно созданный объект, который бы полностью копировал поведение человека, пока не создан, так как это связано с решением целого ряда, в том числе и научных (технологических) проблем. Этот искусственно созданный объект должен обладать разумом, рассудком, способностью отличать главное от второстепенного и принимать решения на основе ранее полученного жизненного опыта и анализа внешних воздействий. Интеллект и мышление для достижения конкретных целей неразрывно связаны с решением ряда задач: распознать, проанализировать, выбрать линию поведения, выработать новые понятия и знания, проявить творческое мышление. В процессе выполнения этих задач ИИ должен обладать способностью к обучению, обобщению, накоплению опыта, адаптации к меняющейся обстановке.

В настоящее время ИИ в военном деле характеризуется полным отсутствием способностей человеческого интеллекта и, по мнению многочисленных авторитетных экспертов, в ближайшее время его появление не предвидится. Сегоднякомпьютер управляется человеком и не может самостоятельно мыслить, самообучаться, проявлять волевые и эмоциональные качества. Поэтому пока об ИИ можно говорить только как о средстве (инструменте) решения военно – прикладных задач. В то же время, технологии ИИ ведущих государств мира в военной области развиваются настолько стремительно, что об ИИ уже принято говорить, как о третьей инновационной революции после изобретения пороха и создания ядерного оружия. Например, США в военной области стремятся занять лидирующее положение в мире в создании кибероружияи автономных видов вооружений с ИИ. В то же время, руководствуясь «Стратегией национальной обороны» и «Концепцией быстрого глобального удара», США постоянно ведут прокси-гибридную войну с Россией всеми доступными методами, в том числе с применением технологий ИИ, с целью вынудить страну к капитуляции еще задолго до применения вооруженных сил. Злонамеренное использование ИИ дает существенное преимущество за счет выбора наиболее эффективных форм воздействия на индивидуальное и общественное сознание.

В национальной стратегии развития ИИ в России до 2030 года дано следующее определение: «Искусственный интеллект-комплекс технологических решений, позволяющий имитировать когнитивные функции человека… и получать при выполнениии задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека» [1].Для этого предполагается развивать такие системы, как компьютерное зрение, обработка естественного языка, распознавание и синтез речи, рекомендательные и интеллектуальные системы поддержки принятия решений [2], перспективные методы и технологии ИИ (в первую очередь технологии автоматизированногомашинного обучения).

Одной из ведущих алгоритмических технологий машинного обучения считается технология искусственных нейронных сетей, так как она подает надежду на имитацию многих свойств, присущих мозгу человека (обучение на основе опыта, выделение главного из большого объема поступающей информации). При этом нейронные сети обладают самонастройкой, гибкостью конфигурирования, высокой эффективностью,

самообучаемостью, работой в условиях неполной информации. Сегодня технология нейронных сетей развивает свои способности в распознавании речи, изображений и осуществлении поиска информации. Жесткая конкурентная борьба ведется в области аппаратного обеспечения ИИ в таких сферах прорывных технологий, как мемристоры, графеновые и алмазные процессоры, оптические платы.

По сообщениям прессы, не так давно в ВКС России испытана АСУ средствами ПВО с элементами ИИ, которая позволяет средствам ПВО (ЗРК С-300, С-400, ЗПРК «Панцырь» и РЛС) реагировать на угрозы в масштабе реального времени с выдачей рекомендаций на боевое применение выбранного средства поражения воздушных целей.

Многие страны уже имеют на вооружении автономные оборонительные средства. В то же время ведутся работы по созданию автономных наступательных вооружений,при этом используются достижения технологий ИИ. Такие автономные наступательные вооружения (интеллектуальные, боевые и командные платформы) будут принимать участие в будущих операциях, выполняя свои конкретно поставленные задачи в космосе, в воздухе, на суше, в море и под водой.

При прочих равных условиях в военном противоборстве победу одержит тот, кто быстрее сможет обработать больший объем разведывательной информации, распознать и идентифицировать цели и первым применить оружие. Такой принцип «обнаружил-выстрелил-забыл») давно заложен и продолжает развиваться в разведывательно-ударных комплексах типа «Длинная рука» и другом высокоточном оружии. То есть, использование элементов ИИ позволяет опередить противника, обеспечить автономные действия без участия человека, как слабого звена (ведение разведки, идентификацию и классификацию целей противника, выбор применяемого оружия, средств и способов их огневого поражения, радио-электронного подавления, а также выбор и применение своих средств и способов защиты от действий противоборствующей стороны), проявляя при этом адаптивность к динамично меняющейся обстановке в масштабе реального времени.

Очень важные области применения элементов ИИ в стратегическом плане для исключения фактора внезапности и оперативного реагирования на военные угрозы – это постоянный анализ военно – политической обстановки, разработка сценариев ведения войны, строительства Вооруженных сил и их боевого применения, прогнозирование хода и исхода войны или военных действий, централизованное планирование и проведение операций (воздушно-космических, информационно-кибернетических, морских и наземных, антитеррористических операций), противодействие манипулированию общественным мнением, распространению дезинформации и проведению психологических операций.

Применение ИИ дают возможность обрабатывать большой объем информации за короткий промежуток времени, по возможности, без участия человека (автономно). Жесткая борьба за первенство в создании квантового компьютера дает шанс получить победителю огромные преимущества. Последствием для проигравшей стороны может быть взлом шифров во всей государственной, в том числе и военной инфраструктуре, утрата секретной информации и, возможно, полная потеря контроля над военно-политической и военной обстановкой, так как обладатель передовыми технологиями ИИ всегда и во всем будет упреждать, а значит побеждать.

В декабре 2019 года Сбербанк России и его дочерняя компания Sber Cloud в партнерстве скомпанией NVIDIA запустили в коммерческую эксплуатацию самый мощный суперкомпьютер «Кристофари», созданный для работы с алгоритмами ИИ.

Суперкомпьютер входит в 30 самых производительных суперкомпьютеров мира и занимает 29 место из 500. Эффективная производительность «Кристофари» составляет 6,7 PFLOPs (согласно тесту LINPACK), пиковая производительность — 8,8PFLOPs.

Имея в распоряжении такой мощный инструмент, значительно расширяются возможности для разработки и тестирования алгоритмов ИИ (например, протестировать крипкостойкость любого шифратора, провести исследования в области шифроанализа и т. д.).

Достижение военного превосходства над Россией, которая за время правления Д.Трампа возведена в ранг основных противников США, осуществляется с помощью быстрого внедрения результатов интенсивного развития научно-технологических разработок в области ИИ.

Основными направлениями применения ИИ в военной сфере США являются интеллектуальная обработка больших массивов данных, логистика, кибербезопасность, управление войсками, автономное управление подвижными объектами [3].

Технология интеллектуальной обработки больших массивов данных видеоизображений, поступающих с БПЛА (переферических систем-автоматизированных дронов, оснащенных системами компьютерного оптического зрения), в аналитический центр (центральный ИИ-гибкие модифицированные блоки нейронных сетей с машинным обучением, превосходящие человека в распознавании нечеткой оптической информации), успешно опробована в Ираке и Сирии, что позволило, по мнению по мнению американских экспертов, на 80% повысить оперативность обнаружения и классификации целей.

В области логистики элементы ИИ (интеллектуальные алгоритмы) анализируют-телеметрическую информацию и прогнозируют срок выхода из строя важных узлов отдельных образцов военной техники. По мнению Пентагона, внедрение такой технологии за счет своевременной поставки запасных частей, снижения затрат на ремонт и предотвращение ущерба позволит ежегодно экономить около одного млрд долларов.

Применение технологий ИИ в области управления подвижными объектами и обеспечения их взаимодействия друг с другом позволит робототехническим комплексам, летательным аппаратам, в том числе «роям» БПЛА, решать задачи навигации, разведки, связи, радиоэлектронного и огневого подавления и поражения целей противника. В целом, с меньшими затратами, такие «рои» могут противодействовать крупным силам противника (например, авианосным ударным группировкам).

Китай к 2030 году намерен стать мировым лидером в области технологий ИИ. В военной области основные направления использования ИИ в целом такие же, как в США и России. Россия в области применения новых технологий ИИ наверстывает упущенное и, по мнению американских экспертов, стремится создать свой ударный дрон дальнего радиуса действия и полностью уйти от зависимости иностранных компонентов. Кроме того, эксперты выделили два перспективных направления развития беспилотных систем в России – использование ИИ и «роев» дронов и размещение средств радиоэлектронной борьбы набеспилотных системах.

Таким образом, одним из основных направлений развития вооруженных сил ведущих стран мира являются исследования в области повышения эффективности систем управления войсками и оружием путем внедрения ИИ (высокоуровневых программ) в их программно-аппаратный комплекс. В целом, можно сказать, что совершенствование систем управления войсками и оружием ведущих стран мира (США, Китая, России) идет по пути развития прежде всего технических средств управления, связи, разведки, АСУ и РЭБ, их интеграции, взаимодействия и комплексного применения на основе использования технологий ИИ.

Следует подчеркнуть, что тенденция (закономерность) развития форм и способов боевого применения вооруженных сил в операциях (боевых действиях) на стратегическом, оперативном и тактическом уровнях будет характеризоваться обменом огромного количества информации в реальном масштабе времени по защищенным каналам связис

наращиванием возможностей ИИ для обработки, анализа этой информации и выработки решений.

Так, Lockheed Martin разработал и поставляет уже более 30 государственным организациям США программный продукт LV Wisdom, анализирующий интернет (социальные источники, СМИ и другие открытые источники) для прогнозирования военно-политической обстановки (уровень ее нестабильности) и террористических угрозв разных странах мира и регионах. Очевидно, что такая платформа может быть использована и для прогнозирования военно-политической обстановки с использованием не только открытой информации, но и закрытой (разведданные технических и агентурных источников) для своевременного реагирования на краткосрочные, среднесрочные и долгосрочные угрозы.

Последние достижения в области элементов ИИ касаются не только их применения в системах управления войсками и оружием, в активно развивающихся робототехнических комплексах и беспилотных системах вооружения, но и в дальнейшем развитии способов обнаружения и предупреждения компьютерных атак.

В области обеспечения компьютерной безопасности эффективно противодействовать компьютерным атакам, а также проводить свои (ведение боевых действий в киберпространстве) без применения элементов ИИ в ближайшее время, очевидно, будет просто невозможно. Именно ИИ обеспечивает мгновенное обнаружение аномалий и уязвимостей и обнаружение вторжения противника в сеть.

В этом направлении ведутся разработки средств, выявляющих уязвимости как собственного программного обеспечения, так и программного обеспечения противника для подготовки и проведения компьютерных атак и отражения атак противника. В целом ИИ, который действует по определенному правилу или алгоритму, пока только помогает эффективно решать задачи кибербезопасности, которые раньше решались традиционными способами. В тоже время его развитие идет по пути создания автономной интеллектуальной системы, способной к принятию самостоятельных решений в зависимости от ситуации и с высокой эффективностью обнаруживать и отражать компьютерные атаки. Подтверждением тому являются новые системы класса SIEM (security information and tvent management) с технологиями машинного обучения и ИИ. Такие системы предупреждают об опасности вторжения, объявляют тревогу, вычисляют типовые состояния работы системы, ищут отклонения (аномалии) – и все это без участия человека (он даже не в состоянии выполнить такую точную и скоростную работу). Кроме того, технологии машинного обучения и ИИ используются в системах обнаружения и предотвращения вторжений, управления идентификацией и доступом, в аналитических системах и современных системах антивирусной защиты. В таких системах точность и скорость являются критическими для защиты от кибератак.

Применение ИИ в кибератаках преступников уже факт, состоявшийся и бесспорный, имитация поведения человека на вебсайте уже происходит и противостоять атакующим роботам могут только роботы. Кибервойны уже идут в форме прокси-гибридных войн, и победу в них может одержать та сторона, которая действует быстрей с использованием более изощренных алгоритмов и технологий ИИ, имеет лучших специалистов для нападения и отражения атак. В докладе «Искусственный интеллект и национальная безопасность» вашингтонского Центра стратегических и международных исследований (Nhe Ctnter for Strategic and International Studies, CSIS) говорится: «ИИ и машинное обучение будет иметь преобразуюшее влияние на кибербезопасность и кибервойны… Кибератаки станут комплексными и крайне опасными» [4]. Очевидно, что противостоять такой системе с ИИ может только система, которая повысит уровень обнаружения угроз и сократит время реакции на их устранение вплоть до реального.

Таким образом, более 30 стран, в т.ч. ведущие мировые державы: США, Китай и Россия начали очередной виток гонки за технологическое превосходство путем реализации национальных стратегий развития ИИ во всех сферах своей жизнедеятельности, в том числе и военной.

Анализ состояния и перспектив развития ИИ в военной области показал, что в ближайшее время ИИ будет внедряться прежде всего в дальнейшее совершенствование СУВ и О, в т.ч. управление автономными оборонительными и наступательными системами, робототехническими комплексами и «роями», развитие технических средств управления-систем связи, разведки, АСУ и РЭБ и размещение их в т.ч. и на БПЛА. В то же время Россия уделяет большое внимание разработке собственной элементной базы для систем и технологий ИИ, дальнейшему развитию умных боеприпасов (высокоточного оружия), созданию кибероружия, экспертных систем и систем принятия решений, дальнейшему развитию способов обнаружения и предупреждения компьютерных атак.

Тенденция (закономерность) развития форм и способов боевого применения вооруженных сил в операциях (боевых действиях) на стратегическом, оперативном и тактическом уровнях будет характеризоваться обменом огромным количеством информации в реальном масштабе времени по защищенным каналам связис наращиванием возможностей ИИ для обработки, анализа этой информации и выработки решений.

Таким образом, возможные угрозы информационной безопасности в военной области от применения технологий ИИ и машинного обучения в принципе останутся теми же, но с более масштабными последствиями.

К таким угрозам можно отнести:

1. Взлом шифров в многочисленных каналах обмена закрытой информацией.
2. Охота за уязвимостями.
3. Кибератаки.

Очевидно, что укрепить свои позиции в информационной сфере в военной области путем нейтрализации существующих и отслеживания новых угроз возможно только с помощью систем ИИ, то есть, обеспечение кибербезопасности и информационной защиты в военной области предполагает широкое внедрение перспективных методов и технологий ИИ и, в первую очередь, технологий автоматизированного машинного обучения.

Литература

1. Национальная стратегия развития искусственного интеллекта до 2030 года. Утверждена Указом Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

2. Щербаков В.А., Васин О.И., Пидшморга Ю.В. Рекомендательная система подбора научных трудовна основе пользовательских оценок. // Информационная безопасность – актуальная проблема современности: сб. трудов XVII НТК, г. Геленджик 2018 г. / отв. ред. д.т.н., проф. А.В.Крупенин. – Краснодар: КВВУ, 2018. – С. 92–94.

3. Зарубежное военное обозрение. – 2019. – С. 11–15.

4. Доклад исследовательской службы конгресса США «Искусственный интеллект и национальная безопасность» (Artificial Intelligence and NationalSecurity)

Сведения об авторах

Щербаков Виктор Андреевич, кандидат технических наук, старший научный сотрудник НИЦ Краснодарского высшго военного орденов Жукова и Октябрьской революции Краснознаменного училища имени генерала армии С.М.Штеменко; e-mail: sherbakov_viktor@list.ru

Васин Олег Иванович, кандидат физико-математических наук, старший научный сотрудник НИЦ Краснодарского высшго военного орденов Жукова и Октябрьской ре-

волюции Краснознаменного училища имени генерала армии С.М.Штеменко; e-mail: ovassin@mail.ru

Рыскин Сергей Васильевич, кандидат технических наук, начальник лабораторииНИЦ Краснодарского высшго военного орденов Жукова и Октябрьской революции Краснознаменного училища имени генерала армии С.М.Штеменко; e-mail: ovassin@mail.ru

Кулаков Андрей Анатольевич, начальник отделаНИЦ Краснодарского высшго военного орденов Жукова и Октябрьской революции Краснознаменного училища имени генерала армии С.М.Штеменко; e-mail: Andrei9614@rambler.ru

Содержание

Научное издание

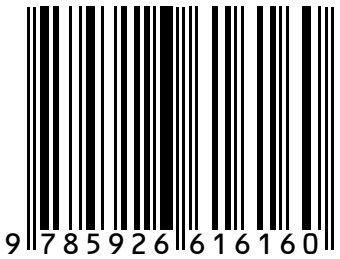
МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

XVI Всероссийской научно-практической конференции
(19 июня 2020 г.)

В авторской редакции

Компьютерная верстка *Н. А. Никитиной*

ISBN 978-5-9266-1616-0



Подписано в печать 25.08.2020. Формат 60х84 1/8.
Усл. печ. л. 15,3. Тираж 70 экз. Заказ 79.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.