ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(43) / 2022

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА

ЧУВАРДИН О. П.,
руководитель Управления Федеральной службы по техническому и экспортному контролю России по Уральскому федеральному округу

ГЛАВНЫЙ РЕДАКТОР

СОКОЛОВ А. Н.,
к. т. н., доцент, зав. кафедрой «Защита информации», Южно-Уральский государственный университет (национальный исследовательский университет) (г. Челябинск)

ВЫПУСКАЮЩИЙ РЕДАКТОР

СОГРИН Е. К.

ВЁРСТКА

ШРАЙБЕР А. Е.

КОРРЕКТОР

ФЁДОРОВ В. С.

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 1(43) / 2022

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,

Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,

Ph.D., Associate Professor, Head of Department "Information Protection", South Ural State University (National Research University) (Chelyabinsk city)

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SCHREIBER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ

ПЕТУХОВ А.Г., СТЕПАНЦОВА А.М., ДЕЛОГ А.Н.
Использование корректирующих кодов для повышения помехоустойчивости систем передачи информации. 5

ВОЙТОВИЧ Н.И., ЮНГАЙТИС Е.М., ЕРШОВ А.В.
Дифракция электромагнитных волн на полуплоскости применительно к системе посадки воздушных судов на аэродромы с высоким уровнем снежного покрова и сложным рельефом местности в зоне захода на посадку. 11

СТЕПАНЦОВА А.М., ПЕТУХОВ А.Г., ДЕЛОГ А.Н., СТЕПАНЦОВ С.В.
Анализ воздействия ионосферного луча на распространение радиоволн 22

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МИРВОДА С.Г., ПОРШНЕВ С.В., РЯБКО Н.Ю.
Автоматизация процедуры доступа к электоральным данным, размещенных на сайте Центральной избирательной комиссии Российской Федерации 28

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ШАМОНИН Е. Д.
Моделирование дисковой подсистемы ЭВМ на основе накопителя на жестких магнитных дисках в режиме чтения 35

ВИЛЬХОВСКИЙ Д.Э., ГУЦ, А.К.
Метод обнаружения LSB-вставок в искусственных цветных изображениях с градиентной заливкой с низким заполнением стегоконтейнера. 43

МАКСИМОВА Е. А., БУЙНЕВИЧ М. В.
Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры 50

МАКАРОВА О.С., ПОРШНЕВ С.В.
Методика прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя 64

СТАРУН И.Г., ЮГАНСОН А.Н.
Разработка алгоритма классификации шифрованного трафика на основе lightgbm 74

АСТАХОВА Л.В., УТОРОВ О.Р.
Будущий специалист по защите информации как субъект образовательной деятельности 84

ЛЕБЕДЕВ Д.В., ГУЗЕНКОВА Е.А.
Метод оценки эффективности обеспечения безопасности компьютерной сети системой предотвращения вторжений посредством проведения атак на уязвимую систему. 90

RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES

PETUKHOV A.G., STEPANTSOVA A.M., DELOG A.N.
The use of correction codes to increase the noise immunity of information transmission systems. 5

VOYTOVICH N.I., IUNGAITIS E.M., ERSHOV A.V.
Diffraction of electromagnetic waves on a half-plane in relation to the aircraft landing system on airfields with a high level of snow cover and difficult terrain in the approach zone 11

STEPANCOVA A.M., PETUKHOV A.G., DELOG A.N., STEPANCOV S.V.
Analysis of the effect of the ionospheric beam on the propagation of radio waves 22

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

MIRVODA S.G., PORSHNEV S.V., RYABKO N.YU.
Automation of the procedure for accessing electoral data posted on the website of the Central Election Commission Russian Federation. 28

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

SHAMONIN E. D.
Simulation of a computer disk subsystem based on a hard disk drive in read mode 35

VILKHOVSKY D.E., GUTS A.K.
Method of detecting LSB insertion in low stego-payload artificial color images of a gradient fill 43

MAKSIMOVA E. A., BUYNIVICH M. V.
The method of assessing the infrastructural stability of the subjects of critical information infrastructure 50

MAKAROVA O.S., PORSHNEV S.V.
Predicting methodology of the probability dynamics of a computer attack from the point of view of the intruder 64

STARUN I.G., IUGANSON A.N.
Development of the algorithm for classification of encrypted traffic based on lightgbm 74

ASTAKHOVA L.V., UTOROV O.R.
Future security specialist as a subject of educational activity 84

LEBEDEV D.V., GUZENKOVA E.A.
Method for evaluating the effectiveness of ensuring the security of a computer network by an intrusion prevention system through attacks on a vulnerable system 90

УДК 621.37.037 Вестник УрФО № 1(43) / 2022, с. 5–10

Петухов А.Г., Степанцова А.М., Делог А.Н.

DOI: 10.14529/secur220101

ИСПОЛЬЗОВАНИЕ КОРРЕКТИРУЮЩИХ КОДОВ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Передавая какие-либо сведения по каналу связи, абсолютно любая кодовая комбинация несет полученную информацию. В связи с тем, что не исключено возможное внешнее воздействие, либо внутренние сбои в работе аппаратуры, могут возникать помехи, которые искажают кодовые комбинации. Одним из способов повышения помехоустойчивости систем передачи информации является применение корректирующих кодов, которые позволяют обнаруживать или исправлять ошибки, возникающие при передаче информации из-за влияния помех. На сегодняшний день известно огромное количество корректирующих кодов, разных по строению и отличающихся друг от друга своими основными характеристиками. В данной статье рассматривается их классификация, принцип обнаружения ошибок и помехоустойчивого кодирования, геометрическая модель кода.

Ключевые слова: *корректирующий код, разрешенные и запрещенные комбинации, кодовое расстояние, бинарный код, помехоустойчивость.*

Petukhov A.G., Stepantsova A.M., Delog A.N.

THE USE OF CORRECTION CODES TO INCREASE THE NOISE IMMUNITY OF INFORMATION TRANSMISSION SYSTEMS

Transmitting any information over the communication channel, absolutely any code combination carries the received information. Due to the fact that possible external influences or internal failures in the operation of the equipment are not excluded, interference may occur that distort the code combinations. One of the ways to increase the noise immunity of information transmission systems is the use of correction codes that allow you to detect or correct errors that occur during the transmission of information due to the influence of interference. To date, a huge number of corrective codes are known, different in structure and differing from each other in their main characteristics. This article discusses their classification, the principle of error detection and noise-resistant coding, the geometric model of the code.

Keywords: *correcting code, permitted and prohibited combinations, code distance, binary code, noise immunity.*

Корректирующие коды подразделяются на два класса: обнаруживающие и исправляющие. Первые позволяют установить факт наличия искажения кодовых комбинаций. Вторые (корректирующие) позволяют обнаружить ошибку и установить ее место в кодовой комбинации, что дает возможность ее исправить.

Принцип обнаружения ошибок состоит в следующем. Если число возможных кодовых комбинаций

при заданном основании m и значности кода n равно $N = m^n$, то для передачи сообщений используется некоторая часть их $N_р < N$.

Используемые в данном коде комбинации называются разрешенными, а остальные $N - N_р$ неиспользуемые комбинации – запрещенными [1,11].

На рисунке 1 представлена диаграмма вероятностных переходов при передаче $N_р$ сообщений. Символами A_i обозначены разрешенные, а символами B_j – запрещенные комбинации, в которые могут перейти разрешенные в результате различного сочетания ошибок при приеме.

Очевидно, что каждая из разрешенных комбинаций при воздействии помехи, приводящей к ошибкам при приеме, может превратиться в любую из N возможных комбинаций, за исключением самой себя (в последнем случае ошибка отсутствует). Таким образом, общее количество ошибочных комбинаций при передаче $N_р$ сообщений равно $N_р (N-1)$. Из этого количества ошибки могут быть замечены только в том случае, если разрешенная кодовая комбинация переходит в запрещенную [2]. Следовательно, количество фиксируемых ошибок при передаче одного сообщения будет равно $N–N_р$, а при $N_р$ сообщениях будет $N_р (N– N_р)$.

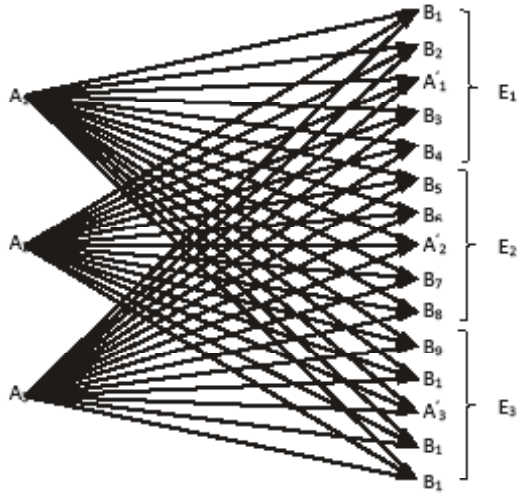


Рис. 1. Диаграмма вероятностных переходов для корректирующего кода

Доля обнаруженных ошибок $\eta_{об}$ составляет:

$$\eta_{об} = \frac{Np(N-Np)}{Np\,(N-1)} = \frac{N}{N-1} - \frac{Np}{N-1}.$$

Так как обычно N>>1, то:

$$\eta_{об} = 1 - \frac{Np}{N}.$$

Как следует из последнего, доля обнаруживаемых ошибок возрастает с увеличением числа избыточных кодовых комбинаций.

При использовании кода в качестве исправляющего в приемнике производится разбиение всего множества возможных кодовых комбинаций N на $N_р$ непересекающихся областей E_i (непересекающиеся подмножества), причем каждая из областей E_i приписывается к одной из разрешенных кодовых комбинаций A_i, Если принятая кодовая комбинация находится в области E_i, то при приеме считается, что передано сообщение A_i. Очевидно, что количество исправляемых ошибок при передаче одного сообщения будет равно числу запрещенных комбинаций, входящих в данную область E_i а общее количество исправляемых ошибок при $N_р$ разрешенных кодовых комбинаций равно общему числу запрещенных кодовых комбинаций $N– N_р$.

Отношение числа исправляемых ошибочных комбинаций к числу обнаруживаемых ошибочных комбинаций составляет:

$$\eta_{и} = \frac{N- Np}{Np\,(N-Np)} = \frac{1}{Np}.$$

Таким образом, обнаруживающая и исправляющая способность кода зависит прежде всего от количества избыточных (запрещенных) кодовых комбинаций. Практически увеличение количества кодовых комбинаций по сравнению с требуемым для передачи определенного числа сообщений при данном методе кодирования может быть достигнуто увеличением значности кода, т. е. удлинением кодовых посылок [3]. В настоящее время хорошо разработаны только бинарные корректирующие коды. Поэтому в дальнейшем будем полагать m = 2.

Если в системе связи необходимо передать $N_р – 2^h$ сообщений, то для придания коду корректирующих способностей необходимо увеличить число кодовых комбинаций до $N = 2^n$, причём n>k. Следовательно, комбинации корректирующего кода должны содержать n символов, из которых k являются информационными, а (n – k) – дополнительными контрольными или проверочными символами.

Выше было установлено количество комбинаций, которые можно исправить данным корректирующим кодом, из общего числа возможных ошибочных комбинаций. Естественным критерием при выборе типов исправляемых кодовых комбинаций является минимизация средней ошибки. Если ошибки при приеме каждого символа независимы, то их вероятность убывает с повышением кратности. Следовательно, для уменьшения средней вероятности ошибки необходимо в первую очередь исправлять ошибки низшей кратности.

Установим связь между кратностью исправляемых ошибок и количеством контрольных символов в кодовой комбинации. Предположим, что код используется для исправления ошибок кратности от 1 до r включительно. Так как количество ошибок кратности i в комбинации, состоящей из n символов, равно числу сочетаний из n элементов по i, то общее количе-

ство ошибок λ_r кратности от 1 до r, возможных в одной комбинации, равно:

$$\lambda_r = \sum_{i=1}^{r} c_n^i.$$

Тогда общее количество ошибок, исправляемых в N_p комбинациях, составляет $N_p\lambda_r$.

С другой стороны, код может исправить не более $N–N_p$ ошибочных комбинаций. Следовательно, величины N и N_p должны выбираться так, чтобы выполнялось неравенство:

$$N_p\lambda r \leq N - N_p,$$

откуда $N \geq N_p (1 + \lambda_r)$.

Поскольку $N = 2^n$ и $N_p – 2^k$, то подставляя значение λ_r и логарифмируя последнее неравенство по основанию 2, получим:

$$n-k \geq \log_2 \sum_{i=0}^{r} c_n^i. \qquad (1)$$

При выводе формулы (1) было использовано тождество $C^0_n = 1$. С помощью формулы (1) можно определить количество контрольных символов в кодовых комбинациях, необходимое для придания коду определенной исправляющей способности [4,5]. Знак «$\geq$» в ней означает, что округление величины log должно производиться в сторону увеличения до ближайшего целого значения. На практике обычно известной является величина k, так как она связана с количеством передаваемых сообщений. Однако формула непосредственной связи величин n и k оказывается сравнительно громоздкой, особенно при высокой кратности исправляемых ошибок. Поэтому для определения необходимого количества символов корректирующего кода обычно прибегают к составлению таблиц (таблица 1) зависимости между n и k для определенной кратности исправляемых ошибок.

С помощью подобной таблицы можно легко определить количество необходимых символов в комбинациях корректирующего кода n при заданном k и r. Например, пусть количество информационных символов k = 5, а код должен исправлять все однократные ошибки. По этим данным в таблице находим значение n = 9.

Таблица 1

Таблица зависимости для определения кратности исправляемых ошибок

k		1	2	3	4	5	6	7	8	9
n	$r = 1$	3	5	6	7	9	10	11	12	13
	$r = 2$	5	7	9	10	12	13	15	16	17

Из таблицы 1 следует, что в большинстве случаев неравенство (1) выполняется с запасом. Это свидетельствует о том, что исправление ошибок кратности до r часто не исчерпывает всех возможностей данного кода. При этом $N – N_p = 2^n – 2^k > N_p\lambda r$. Так, для вышеприведенного примера n = 9, k = 5, r = 1 код способен исправить $2^9 – 2^5 = 480$ ошибочно принятых кодовых комбинаций, в то время как количество однократных ошибок равно $2^5 – 9 = 288$. Следовательно, кроме однократных ошибок код способен исправить 480 – 288 = 122 кодовые комбинации, например, двукратных.

Реализация корректирующих способностей зависит от принципа построения кода [6]. Код, который полностью использует возможности по исправлению ошибок, называется оптимальным, причем оптимальность рассматривается в смысле полноты использования корректирующей способности при данном числе контрольных символов.

Для объяснения сущности процесса обнаружения и исправления ошибок при приеме кодовых комбинаций введем понятие кодового расстояния. Под кодовым расстоянием d_{ij} между двумя комбинациями понимают число идентичных позиций с несовпадающими символами. Например, расстояние между комбинациями A_1= 10111, A_2=01100 равно 4, так как они различаются символами в четырех позициях. Можно заметить, что кодовое расстояние равно числу единиц в сумме комбинаций по модулю 2^1. Так, для приведенных комбинаций имеем:

$$\begin{array}{r} \oplus\ 10111 \\ \underline{\ \ 01100} \\ \ \ 11011 \end{array}$$

Понятию кодового (хэммингового) расстояния можно придать геометрический смысл [12].

Бинарный код представляет собой последовательность нулей и единиц, общее число которых равно значности кода n. Если в n-мерной системе координат по каждой оси отложить значение определенного разряда, то геометрической моделью бинарного n-разрядного кода будет n-мерный единичный куб. При этом каждая вершина куба представляет комбинацию, входящую в данный код.

На рисунке 2 для наглядности изображена геометрическая модель трехзначного кода. Из рисунка видно, что кодовое расстояние равно расстоянию, измеряемому вдоль ребер куба от одной вершины до другой. Например, кодовое расстояние между комбинациями A_1 = 000 и A_6 = 101 равно 2, так как при перемещении из A_1 в точку A_6 необходимо пройти вдоль двух ребер куба [7, 8]. Перейдем к пояснению процесса обнаружения и исправления ошибок.

Если для передачи сообщений используются все возможные для данного кода комбинации $N = N_p$, то минимальное кодовое расстояние между комбинациями равно 1 и обнаружение ошибок невозможно, так как при воздействии помех происходит транс-

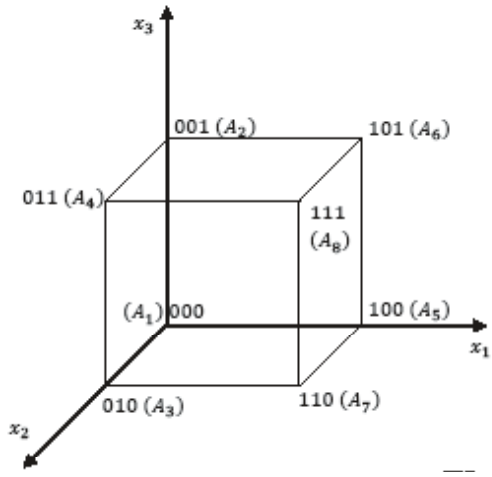


Рис. 2. Геометрическая модель кода

формация одной разрешенной комбинации в другую.

Пусть теперь минимальное расстояние между кодовыми комбинациями $d_{min} = 2$. Например, используются комбинации $A_1 = 000$, $A_4 = 011$, $A_6 = 101$, $A_7 = 110$. При воздействии помех, приводящих к однократной ошибке, расстояние между переданной комбинацией и любой другой из разрешенных изменится на единицу. Но при этом принятая комбинация преобразуется в запрещенную, и ошибка будет обнаружена. Таким образом, для обнаружения одиночных ошибок необходимо, чтобы $d_{min} \geq 2$. Это условие. реализуется, например, в коде с четной защитой. Принцип построения такого кода состоит в том, что к кодовым комбинациям обычного бинарного кода без избыточности добавляется один разряд. Знак этого разряда (1 или 0) выбирается так, чтобы сумма единиц во всех кодовых комбинациях была четной. Однократная ошибка при приеме кодовой комбинации нарушает четность числа единиц и легко обнаруживается с помощью простейшего счетчика числа единиц в комбинации. Кроме того, код с четной защитой способен обнаруживать все ошибки нечетной кратности.

Рассуждая аналогично, можно получить следующее соотношение между минимальным кодовым расстоянием d_{min} и кратностью обнаруживаемых ошибок:

$$d_{min} > r_{об} + 1.$$

Для исправления ошибок необходимо, чтобы кодовое расстояние между принятой ошибочно комбинацией и переданной было меньше, чем между принятой и любой другой разрешенной кодовой комбинацией. По этому правилу производится разбиение множества возможных комбинаций N на области E_i при приеме (рисунок 1). Для исправления одиночных ошибок область E_i должна содержать по крайней мере три комбинации, из которых одна разрешенная, а две других стоят от разрешенной по обе стороны на d = 1 и являются запрещенными [9].

Таким образом, минимальное кодовое расстояние для исправления одиночных ошибок должно быть не менее трех, а для ошибок кратности $r_и$:

$$d_{min} \geq 2r_и + 1.$$

Произведем оценку эффективности. использования корректирующих кодов для повышения помехоустойчивости систем передачи информации. Воспользуемся для этого формулой для вероятности r-кратных ошибок (2):

$$P_n(r) = C^r_n p^r (1 - p)^{n-r}. \qquad (2)$$

Если корректирующий код исправляет все ошибки кратности до r включительно, то вероятность безошибочного приема кодовой комбинации Q_r, состоящей из n элементов, будет выражаться суммой вероятностей ошибок с кратностью от 0 до r включительно:

$$Q_r = \sum_{i=0}^{r} c_n^i p^i (1 - p)^{n-i}.$$

Вероятность ошибочного приема Pr как событие противоположное будет равно:

$$P_r = 1 - \sum_{i=0}^{r} c_n^i p^i (1 - p)^{n-i}.$$

Повышение помехоустойчивости при использовании корректирующих кодов достигается за счет введения избыточности, которая определяется как разность между количеством элементов n в комбинациях данного кода и количеством информационных элементов k. Чаще употребляется понятие относительной избыточности:

$$R = \frac{n-k}{n} = 1 - \frac{k}{n}.$$

Введение избыточности при кодировании приводит к необходимости увеличения времени передачи одного сообщения, что влечет за собой увеличение энергии, необходимой для передачи сообщения. Но при увеличении длительности передачи уменьшается также вероятность ошибочного приема элемента комбинации при кодировании без избыточности. Поэтому при одинаковой скорости передачи информации вероятность ошибочного приема элемента обычно больше в коде с избыточностью [10]. В сряди с этим возникает вопрос о том, каким условиям должен удовлетворять код с избыточностью, чтобы его применение позволило повысить достоверность приема информации по сравнению с кодом без избыточности при том же времени передачи сообщения и одинаковой мощности сигнала.

Применение корректирующих кодов целесообразно в том случае, если выполняется неравенство:

$$r > \frac{n}{k} - 1,$$

где r – наибольшая кратность ошибок, полностью исправляемых данным кодом.

Для того чтобы повышение достоверности корректирующим кодом окупало усложнение кодирующей и декодирующей аппаратуры, знак неравенства необходимо усиливать.

[1] Сложение по модулю 2 производится по следующему правилу: $1 \oplus 0 = 1$, $1 \oplus 1 = 0$, $0 \oplus 1 = 1$, $0 \oplus 0 = 0$.

Литература

1. Борисов В.И., Зинчук В.М., Лимарев А.Е. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2000. 20 с.

2. Вернер М. Основы кодирования: Учебник для вузов: Пер. с нем. М.: Техносфера, 2004. 288 с.

3. Гриценко В.М., Недвоичные арифметические корректирующие коды, Проблемы передачи информации, 1969. С. 19 – 27.

4. Злотник Б.М. Помехоустойчивые коды в системах связи. М.: Радио и связь, 1989. 232 с.

5. Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник. М.: Горячая линия - Телеком, 2004. 126 с.

6. Ковалгин Ю.А., Вологдин Э. И. Цифровое кодирование звуковых сигналов. Издательство: Корона-Принт, 2004. 240 с.

7. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. М.: Наука, 2006.

8. Микропроцессорные кодеры и декодеры / В.М. Муттер, Г.А. Петров и др. М.: Радио и связь, 1991. 184 с.

9. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. 320 с.

10. Питерсон У. Коды, исправляющие ошибки, пер. с англ., М., 1964.

11. Пучков Ю.И., Корректирующий код с повторением [Международный журнал информационных технологий и энергоэффективности], Смоленск, 2020, 8 - 13 с.

12. Рыжов А.А., Гончаров С.Н., Одинцов М.В., Устройство формирования корректирующего кода [XIII всероссийской молодежной научно-инновационной школы], Саров, Издательство: Интерконтакт, 2019, 98-100 с.

References

1. Borisov V.I., Zinchuk V.M., Limarev A.Ye. i dr. Pomekhozashchishchen-nost' sistem radiosvyazi s rasshireniyem spektra signalov metodom psevdo-sluchaynoy perestroyki rabochey chastoty. M.: Radio i svyaz', 2000. 20 s.

2. Verner M. Osnovy kodirovaniya: Uchebnik dlya vuzov: Per. s nem. M.: Tekhnosfera, 2004. 288 s.

3. Gritsenko V.M., Nedvoichnyye arifmeticheskiye korrektiruyushchiye kody, Problemy peredachi informatsii, 1969. S. 19 – 27.

4. Zlotnik B.M. Pomekhoustoychivyye kody v sistemakh svyazi. M.: Radio i svyaz', 1989. 232 c. 5. Zolotarev V.V., Ovechkin G.V. Pomekhoustoychivoye kodirovaniye. Me-tody i algoritmy: Spravochnik. M.: Goryachaya liniya - Telekom, 2004. 126 s.

6. Kovalgin YU.A., Vologdin E. I. Tsifrovoye kodirovaniye zvukovykh signalov. Izdatel'stvo: Korona-Print, 2004. 240 s.

7. Kolesnik V.D., Poltyrev G.SH. Kurs teorii informatsii. M.: Nauka, 2006.

8. Mikroprotsessornyye kodery i dekodery / V.M. Mutter, G.A. Petrov i dr. M.: Radio i svyaz', 1991. 184 s.

9. Morelos-Saragosa R. Iskusstvo pomekhoustoychivogo kodirovaniya. Metody, algoritmy, primeneniye. M.: Tekhnosfera, 2005. 320 s.

10. Piterson U. Kody, ispravlyayushchiye oshibki, per. s angl., M., 1964.

11. Puchkov YU.I., Korrektiruyushchiy kod s povtoreniyem [Mezhdunarod-nyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti], Smo-lensk, 2020, 8 - 13 s.

12. Ryzhov A.A., Goncharov S.N., Odintsov M.V., Ustroystvo formiro-vaniya korrektiruyushchego koda [XIII vserossiyskoy molodezhnoy nauchno-innovatsionnoy shkoly], Carov, Izdatel'stvo: Interkontakt, 2019, 98 - 100 s.

ПЕТУХОВ Александр Георгиевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: putnik0879@mail.ru

PETUKHOV Alexander Georgievich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: putnik0879@mail.ru

СТЕПАНЦОВА Алёна Михайловна, студентка, «Сибирский государственный университет телекоммуникации и информатики». Россия, 630102, Сибирский федеральный округ, Новосибирская область, г. Новосибирск, ул. Кирова, д. 86. E-mail: alena169vega@yandex.ru

STEPANCOVA Aljona Mihajlovna, student, "Siberian State University of Telecommunications and Informatics". Russia, 630102, Siberian Federal District, Novosibirsk region, Novosibirsk, Kirova str., 86. E-mail: alena169vega@yandex.ru

ДЕЛОГ Андрей Николаевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: delog_mga@mail.ru

DELOG Andrey Nikolaevich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: delog_mga@mail.ru

УДК 621.371.33 + 621.396.6 Вестник УрФО № 1(43) / 2022, с. 11–21

Войтович Н.И., Юнгайтис Е.М., Ершов А.В.

DOI: 10.14529/secur220102

ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНЫХ ВОЛН НА ПОЛУПЛОСКОСТИ ПРИМЕНИТЕЛЬНО К СИСТЕМЕ ПОСАДКИ ВОЗДУШНЫХ СУДОВ НА АЭРОДРОМЫ С ВЫСОКИМ УРОВНЕМ СНЕЖНОГО ПОКРОВА И СЛОЖНЫМ РЕЛЬЕФОМ МЕСТНОСТИ В ЗОНЕ ЗАХОДА НА ПОСАДКУ[1]

Работа направлена на обеспечение пилота или автопилота воздушного судна безопасной информацией о траектории захода на посадку на аэродромы со сложным рельефом местности. Получены равномерные по угловым координатам источника и точки наблюдения коротковолновые асимптотические разложения поля дифракции сферической волны на полуплоскости, описывающее поле как вдали, так и в окрестности границ света-тени, при произвольной ориентации электрического диполя относительно ребра полуплоскости.

Рассмотрено влияние дифракции электромагнитных волн на площадке ограниченных размеров перед глиссадным радиомаяком на поведение траектории захода воздушных судов на посадку. Расчётные результаты сравниваются с экспериментальными результатами, полученными лётным путём на прибрежном аэродроме.

Ключевые слова: *безопасность, самолёт, дифракция сферической волны на полуплоскости, прибрежный аэродром, глиссада.*

Voytovich N.I., Iungaitis E.M., Ershov A.V.

DIFFRACTION OF ELECTROMAGNETIC WAVES ON A HALF-PLANE IN RELATION TO THE AIRCRAFT LANDING SYSTEM ON AIRFIELDS WITH A HIGH LEVEL OF SNOW COVER AND DIFFICULT TERRAIN IN THE APPROACH ZONE

The research is aimed at providing the pilot or autopilot of the aircraft with safe information on the trajectory of the landing approach to airfields with difficult terrain. Short-wave asymptotic expansions of the diffraction field of a spherical wave on a wedge, which describe the field both far away and in the vicinity of the light-shadow boundaries,

[1] Исследование выполнено при финансовой поддержке РФФИ и Челябинской области в рамках научного проекта № 20-47-740009.

with an arbitrary orientation of the electric dipole relative to the edge of the half-plane, are obtained, uniform in the angular coordinates of the source and the observation point.

The influence of the diffraction of electromagnetic waves on the site of limited dimensions in front of the glide path on the behavior of the approach trajectory of aircraft for landing is considered. The calculated results are compared with the experimental results obtained by flight at the coastal airfield.

Keywords: *safety, airplane, half-plane spherical wave diffraction, coastal airfield, glide path.*

1. Введение

Статистика аварий, поломок самолётов и катастроф в авиации говорит о том, что около 60% авиационных происшествий происходит при заходе на посадку и посадке самолета. Причиной авиационных происшествий может быть человеческий фактор, не благоприятные погодные условия или технические проблемы с самолетом либо проблемы с информацией, формируемой радиомаячной системой посадки. Пилоту чрезвычайно сложно принять правильное решение в нештатной ситуации в связи с состоянием стресса, дефицитом времени и недостатком информации, ограниченной показаниями бортового оборудования.

На тридцать третьей Ассамблее ИКАО была названа главная причина всех авиационных происшествий при заходе на посадку и посадке — «неспособность распознать экипажем воздушного судна необходимости ухода на второй круг и невыполнение этого манёвра».

Естественно стремление разработчиков и персонала, эксплуатирующего радиомаячные системы посадки воздушных судов, обеспечить пилота или автопилот безопасной информацией о траектории захода на посадку.

Радиомаячная система посадки по приборам (ILS) используется во всем мире для обеспечения захода на посадку и посадки самолета как в условиях ограниченной видимости, так и при хорошей погоде. Однако система может быть чувствительна к многолучевому распространению радиоволн, обусловленному отражением радиоволн от складок рельефа местности и местных предметов.

Исследования влияния рельефа местности на распространение радиоволн вдоль трассы: радиомаяк системы посадки — заходящий на посадку самолёт — выполняются с самого начала развития авиации, а именно с того момента, когда радиомаячные системы посадки пришли на помощь пилотам, с 1930 годов по настоящее время [1, 2]. Развитие радиомаячных систем на протяжении почти столетней их истории рассмотрено в докладе Войтовича Н.И. и Жданова Б.В. [3] "Четыре ключевых технических решений в истории развития ILS (системы посадки самолётов)". В исторически первом техническом решении влияние Земли на распространение радиоволн учитывалось введением зеркального изображения передающей антенны радиомаяка. При этом предполагалось, что подстилающая поверхность представляет собой бесконечно протяжённую во всех направлениях плоскость. Однако, даже в таких идеальных условиях местности для системы посадки из-за несовершенной аппаратуры и несовершенного способа задания навигационной информации наблюдалась низкая точность по выводу самолёта в опорную точку над началом взлётно-посадочной полосы. С развитием авиации повышались требования к точности систем посадки. Новые технические решения (второе и третье ключевые решения в упомянутом докладе) позволили существенно повысить стабильность аппаратуры радиомаяков, избавиться от влияния дальних складок местности в зоне захода самолётов на посадку на поведение глиссады. Наконец, четвёртое техническое решение, предложенное в патенте РФ на изобретение № 2429499 "Глиссадный радиомаяк" авторов Войтовича Н.И., Жданова Б.В. и Соколова А.Н. [4], позволило избавиться от влияния уровня снежного покрова на положение в пространстве траектории для захода самолёта на посадку [5]. Однако, при этом по-прежнему требуется плоская площадка перед радиомаяком протяжённостью около 600-900 метров. Выполнение требования по размерам плоской площадки (определяемым размерами первой зоны Френеля на подстилающей поверхности) перед глиссадным радиомаяком в реальных условиях аэродромов представляет проблему. На аэродромах с неблагоприятной формой рельефа местности предпринимаются попытки ввода в эксплуатацию радиомаяков методом проб и ошибок. А именно, устанавливают радиомаяк на имеющейся площадке ограниченных размеров, выполняют лётные измерения, по результатам которых вводят корректировки высот подвеса излучающих элементов глиссадной антенной решётки и корректировки в амплитудно-фазовое распределение токов вдоль решётки. По вновь полученным лётным результатам вносят новые коррективы в положение излучающих элементов и амплитудно-фазовое распределение вдоль антенной решётки. И так продолжается либо до достижения нужных результатов, либо до принятия решения о вводе в эксплуатацию некатегорированной системы посадки. Это трудоёмкий и затратный путь.

Альтернативой служит моделирование характеристик радиомаяков по заданному рельефу местности и расположению местных предметов на аэродроме.

Чтобы правильно моделировать искривления траектории захода самолётов на посадку в последнее время французская компания Airbus, Французский университет гражданской авиации (ENAC) и Европейский аэрокосмический и оборонный концерн (сокра-

щенно EADS — European Aeronautic Defence and Space Company) объединились, чтобы разработать программные и технические средства для моделирования глиссады и линии курса по заданному рельефу местности и расположению местных предметов. Предварительная и последующая обработка основаны на программном обеспечении ENAC (ATOLL для курсового радиомаяка и LAGON для глиссадного радиомаяка) [6]. В этих программах используется метод физической оптики [7].

В последние годы предложено для вычислений использовать метод моментов [8] и быстрый, так называемый, многоуровневый мультипольный метод [9].

Применение представленного метода для учёта влияния уступообразной подстилающей поверхности на характеристики системы посадки сомнительно, так метод физической оптики не учитывает многократно отражённые волны.

В работах, поддержанных грантами Японского общества содействия науки в помощь молодым ученым [10], [11], подстилающая поверхность аппроксимируется либо прямоугольными пластинами (2D модели), либо треугольными пластинами (3D модели). Представленные работы, по-существу, являются первым шагом авторов к разработке полноценных методик. Работы не содержат сравнения результатов с результатами других авторов либо с экспериментальными результатами.

В нашей работе [12], представленной на 12-ой Европейской конференции по антеннам и распространению радиоволн (12th European Conference on Antennas and Propagation, EuCAP 2018) показано, что подстилающую поверхность на прибрежных аэродромах с заходом самолётов на посадку со стороны моря целесообразно представлять поверхностью в виде уступа. Для целей моделирования траектории захода самолёта на посадку непосредственно аэродромная поверхность представляется идеально проводящей полуплоскостью. Поверхность моря считается идеально проводящей. Модель для приближённого электродинамического анализа получена путём зеркального отражения полуплоскости и антенн относительно плоской водной поверхности. Искомое приближённое решение краевой задачи в области вдали от уступа представлено суммой двух полей. Первое поле — это поле дифракции волн, излучаемых реальными источниками на полуплоскости, отображающей непосредственно аэродромную поверхность. Второе поле есть поле дифракции волн, излучаемых мнимыми источниками, на мнимой полуплоскости. При этом поле дифракции сферической волны на полуплоскости представляется в дальней зоне суммой полей обобщённой падающей и обобщённой отражённой волн. Результаты численных исследований относительных величин полей двух источников на поверхности в виде уступа хорошо согласуются с экспериментальными результатами, полученными лётным путём, на больших расстояниях от радиомаяка.

В настоящей статье мы ставим своей задачей устранить ограничение области для анализа дальней зоной. Во-первых, избавиться от ограничения, связанного с предположением, что излучающие диполи, образующие антенную решётку ГРМ параллельны ребру полуплоскости и, во-вторых, избавиться от предположения, что источник излучения и точка наблюдения находятся в одной и той же плоскости, перпендикулярной краю полуплоскости.

В настоящей работе подстилающую поверхность прибрежного аэродрома представим полуплоскостью, простирающейся от ГРМ до обрыва аэродромной поверхности к морю. Влияние водной поверхности исключим из рассмотрения.

Нашей целью является вычисление вклада в искривления траектории захода воздушного судна на посадку, обусловленного конечными размерами площадки перед ГРМ. Для достижения этой цели необходимо найти приближенное решение задачи дифракции волн диполя в присутствии полуплоскости, простое для вычислений, обладающее физической наглядностью.

2. Постановка задачи

Решения задач дифракции электромагнитных волн, излучаемых диполями, на идеально проводящей полуплоскости впервые были получены Т. Сеньором [13] и Ю. Вандакуровым [14]. Однако выражения для полей $\vec{E}$ (вектор напряжённости электрического поля) и $\vec{H}$ (вектор напряжённости магнитного поля) в общем случае произвольно ориентированных диполей не были выписаны. Вычисление полей в [13] и [14] сведено к вычислению некоторых интегралов.

В дальнейшем в близких по форме интегралах электромагнитные поля, порождённые диполями в присутствии идеально проводящей полуплоскости, представлены Тужилиным А.А. [15, 16]. По предложению Г.Д. Малюжинца этим интегралам дано название интегралов Макдональда.

Однако, использование представления электромагнитных полей, порождённых произвольно ориентированными диполями в присутствии идеально проводящей полуплоскости, через интегралы Макдональда для решения практических задач встречает затруднение. Представленные решения не обладают физической наглядностью. Интегралы Макдональда являются несобственными интегралами, что затрудняет создание программ счёта указанных полей. Кроме того, в решении присутствуют неопределённости вида $\frac{0}{0}$. Поэтому целесообразно на основе строгого решения задачи найти приближённые решения, которые обладали бы физической наглядностью и были бы удобны для численных расчётов.

3. Анализ строгого представления электромагнитных полей, порождённых диполями в присутствии идеально проводящей полуплоскости, через интегралы Макдональда

Для приближённого решения задачи найдём коротковолновое асимптотическое представление строгого решения задачи дифракции сферической волны на идеально проводящей полуплоскости.

В известном строгом решении [15] предполагается, что идеально проводящая полуплоскость расположена на плоскости y = 0 вдоль отрицательной полуоси x, т.е. её точки удовлетворяют соотношению y = 0, x<0. Все рассмотрения ведутся в цилиндрической системе координат (ρ, φ, z) с полярной осью вдоль оси z — кромки полуплоскости.

Предполагается, что диполь расположен в точке $r_0(\rho_0, \varphi_0, z_0)$; его момент $\vec{\mathrm{P}}$ представлен в виде двух составляющих — одной вдоль оси z, единичный орт которой обозначен через $\vec{e}_1$, и второй — ортогональной оси z, т.е.

$$\vec{\mathrm{P}} = P(\cos\theta_0\vec{e}_1 + \sin\theta_0\vec{e}_2),$$

где $P = |\vec{\mathrm{P}}|$ — длина вектора $\vec{\mathrm{P}}$; $\vec{e}_2$ является единичным вектором, лежащим в плоскости, перпендикулярной оси z, и направленным вдоль проекции вектора $\vec{\mathrm{P}}$ на эту плоскость. Орт $\vec{e}_2$ составляет с осью x угол ψ, т.е.

$$\vec{e}_2 = \cos\psi\vec{i} + \sin\psi\vec{j},$$

$\vec{i}$, $\vec{j}$ — единичные орты соответственно вдоль осей x и y (рис. 1).

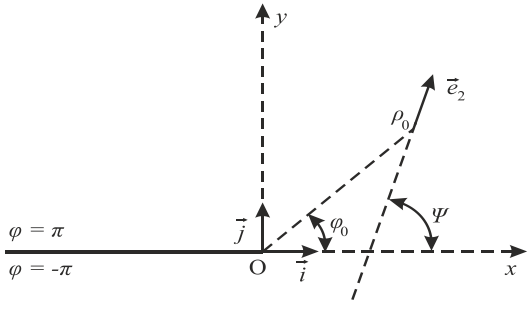


Рис. 1. Система координат.

Электромагнитные поля $\vec{E}(\rho,\varphi,z)$ и $\vec{H}(\rho,\varphi,z)$ удовлетворяют уравнениям Максвелла:

$$rot\,\vec{E} = \frac{i\omega\mu}{c}\vec{H} - \frac{4\pi}{c}\vec{j}^{*}$$

$$rot\,\vec{H} = \frac{\kappa^2 c}{i\omega\mu}\vec{E} + \frac{4\pi}{c}\vec{j}\ ,$$

где ω — частота колебаний, $\tilde{n}$ — скорость света, κ — волновое число, ε и μ — диэлектрическая и магнитная проницаемости среды. Если поле возбуждается электрическим диполем с электрическим диполем $\vec{\mathrm{P}}$, то $\vec{j}^{*} = 0$, $\vec{j} = -i\omega\mathrm{P}\delta(\vec{r} - \vec{r}_0)$, $\delta(\vec{r})$ — трёхмерная функция Дирака, $\vec{r}(\rho,\varphi,z)$. На гранях полуплоскости, т.е. при $\varphi = \pm\pi$ тангенциальная составляющая $\vec{E}$ должна обращаться в нуль; в окрестности кромки полуплоскости $\vec{E}$ и $\vec{H}$ удовлетворяют условиям Майкснера, т.е. компоненты $\vec{E}$ и $\vec{H}$, параллельные кромке, должны быть конечны на кромке, а остальные компоненты могут обращаться в бесконечность не быстрее $\rho^{-\frac{1}{2}}$. $\vec{E}$ и $\vec{H}$ должны удовлетворяют условиям излучения Зоммерфельда.

Векторы $\vec{E}$ и $\vec{H}$ в полученном в [15, 16] решении представляются через интегралы Макдональда. Электрическое поле $\vec{E}(\rho,\varphi,z)$ в присутствии идеально проводящей полуплоскости, расположенной, как указано на рис. 1, определяется через вектор функцию $\vec{\Phi}_1(\beta,\delta)$:

где:

$$\vec{a}(\beta,\delta) = \frac{(\vec{r} - \vec{r}_0(\delta))(\vec{e}_{\beta+\delta}, \vec{r} - \vec{r}_0(\delta))}{R^2(\varphi - \delta)}. \quad (2)$$

$$\vec{E}(\rho,\varphi,z) = \frac{\omega^2\mu}{c^2k^2}\left[\vec{\Phi}_1(-\varphi_0,-\varphi_0) - \vec{\Phi}_1(\varphi_0 - \right.$$
$$\left. - 2\psi, \varphi_0 - 2\pi)\right]. \quad (3)$$

В (1) приняты обозначения:

$$\vec{e}_\alpha = \cos\theta_0\vec{e}_1 + \sin\theta_0(\cos\alpha\vec{e}_2 + \sin\alpha\vec{e}_3), \quad (4)$$

$H_0^{(1)}(n)$, $H_1^{(1)}(n)$ — функции Ханкеля,

$$\kappa = \frac{2\pi}{\lambda};\ \ R(\alpha) = \sqrt{\rho^2 + \rho_0^2 + (z - z_0)^2 - 2\rho\rho_0\cos\alpha}, \quad (5)$$

$$R_0 = R(\pi) = \sqrt{(\rho + \rho_0)^2 + (z - z_0)^2}, \quad (6)$$

$M_n(x, y)$ — интеграл Макдональда:

$$M_n(x,\ y) = \int_{-\infty}^{Arsh} H_n^{(1)}(y\,ch\xi)\frac{d\xi}{(ch\xi)^{n-1}}d\xi. \quad (7)$$

Сравним между собой по величине слагаемые в векторной функции $\vec{\Phi}_1(-\varphi_0,-\varphi_0)$ (а также и в векторной функции $\vec{\Phi}_1(\varphi_0,\varphi_0 - 2\pi)$).

Как показывает анализ, векторные множители в фигурных скобках — это некоторые векторы, определяющие поляризацию той или иной волны. Векторные множители представляют собой величины по модулю равные единице.

Найдём соотношение τ_1 скалярных множителей в первых двух слагаемых, включающих в себя функции Ханкеля $H_1^{(1)}(kR_0)$ и $H_0^{(1)}(kR_0)$:

$$\tau_1 = \frac{\frac{Pik}{2\sqrt{\rho\rho_0}R_0}H_1^{(1)}(kR_0)}{\frac{Pik^2}{2\sqrt{\rho\rho_0}}H_0^{(1)}(kR_0)} = \frac{1}{\kappa R_0}\frac{H_1^{(1)}(kR_0)}{H_0^{(1)}(kR_0)}. \quad (8)$$

Асимптотика функций Ханкеля при больших значениях аргумента x имеет вид [17]:

$$H_\nu^{(1)}(x) = \sqrt{\frac{2}{\pi x}}e^{i\left(x - \nu\frac{\pi}{2} - \frac{\pi}{4}\right)} - 0\left(x^{-\frac{3}{2}}\right). \quad (9)$$

Следовательно, при $kR_0 >> 1$,

$$\left|\frac{H_1^{(1)}(kR_0)}{H_0^{(1)}(kR_0)}\right| \approx 1. \quad (10)$$

Тогда

$$|\tau_1| \approx \frac{1}{\kappa R_0}. \quad (11)$$

Следовательно, при $kR_0 >> 1$ в приближённых расчётах слагаемым с функцией $H_1^{(1)}(kR_0)$ в качестве множителя можно пренебречь.

Найдём теперь соотношение τ_2 третьего и четвёртого слагаемых, включающие в себя соответственно функции $M_0(x, y)$ и $M_1(x, y)$.

$$\tau_2 = \frac{\frac{Pik^2}{2R(\varphi+\delta)} M_0\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi+\delta)}\cos\frac{\varphi+\delta}{2}, kR(\varphi+\delta)\right)}{\frac{Pik^3}{2} M_1\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi+\delta)}\cos\frac{\varphi+\delta}{2}, kR(\varphi+\delta)\right)}. \quad (12)$$

Воспользуемся равномерным по x при $|x| \geq \varepsilon > 0$ (ε — произвольно малое число) разложением функции $M_n(x, y)$ в асимптотический ряд по асимптотической последовательности

$$\left.\frac{H^{(1)}_{m+1-n}\left(y\sqrt{1+x^2}\right)}{\left(y\sqrt{1+x^2}\right)^{m+1}}\right| m \in N: \quad (13)$$

$$M_n(x,y) \sqcap \begin{cases} \sqrt{\frac{2\pi}{y}} H^{(1)}_{n-\frac{1}{2}}(y) & при\ x>0 \\ 0 & при\ x<0 \end{cases} +$$

$$+ \frac{(-1)^n x}{\sqrt{\pi}\left(1+x^2\right)^{\frac{n}{2}}} \sum_{m=0}^{\infty} 2^m \Gamma\left(m+\frac{1}{2}\right)\left(1+\frac{1}{x^2}\right)^{m+1} \frac{H^{(1)}_{m+1-n}\left(y\sqrt{1+x^2}\right)}{\left(y\sqrt{1+x^2}\right)^{m+1}}. \quad (14)$$

Пусть x>0, $y\sqrt{1+x^2} >> 1$.

Тогда

$$M_n(x,y) \approx \sqrt{\frac{2\pi}{y}} H^{(1)}_{n-\frac{1}{2}}(y). \quad (15)$$

Функции Ханкеля с полуцелым индексом $H^{(1)}_{\frac{1}{2}}(y)$ и $H^{(1)}_{-\frac{1}{2}}(y)$ выражаются через тригонометрические функции [17]:

$$H^{(1)}_{\frac{1}{2}}(x) = -i\sqrt{\frac{2}{\pi x}} e^{ix}, H^{(1)}_{-\frac{1}{2}}(x) = i\sqrt{\frac{2}{\pi x}} e^{-ix}. \quad (16)$$

Тогда

$$\tau_2 = \frac{\frac{1}{R(\varphi+\delta)} H^{(1)}_{-\frac{1}{2}}(x)}{k H^{(1)}_{\frac{1}{2}}(x)} = -\frac{e^{-2ix}}{kR(\varphi+\delta)}. \quad (17)$$

$$|\tau_2| = \frac{1}{kR(\varphi+\delta)}. \quad (18)$$

Следовательно, при $kR(\varphi+\delta) >> 1$ третьим слагаемым в сравнении с четвёртым можно пренебречь.

Заметим, что,

$$R(\varphi+\delta)\Big|_{\delta=-\varphi_0} = R(\varphi-\varphi_0), \quad (19)$$

где $R(\varphi-\varphi_0)$ — расстояние между диполем и точкой наблюдения;

$$R(\varphi+\delta)\Big|_{\delta=\varphi_0} = R(\varphi+\varphi_0), \quad (20)$$

где $R(\varphi+\varphi_0)$ — расстояние между мнимым источником и точкой наблюдения.

Таким образом, в дальнейших исследованиях бу-

$$\vec{\Phi}_1(\beta,\delta) = \left\{\left[\vec{e}_1\left[\vec{e}_{\frac{\varphi-\delta}{2}+\beta}, \vec{e}_1\right]\right] - \frac{\vec{a}(\beta,-\delta)-\vec{a}(\beta,\ \pi+\varphi)}{2\cos\frac{\varphi+\delta}{2}}\right\}\frac{Pik^2}{2\sqrt{\rho\rho_0}} H_0^{(1)}(kR_0) -$$

$$-\left\{\frac{1}{2}\left[\vec{e}_1\left[\vec{e}_{\frac{\varphi-\delta}{2}+\beta}, \vec{e}_1\right]\right] - \frac{\vec{a}(\beta,-\delta)-\vec{a}(\beta,\ \pi+\varphi)}{2\cos\frac{\varphi+\delta}{2}} + \right.$$

$$\left. + \frac{2\rho\rho_0}{R^2(\varphi+\delta)}\cos\frac{\varphi+\delta}{2}\left(\vec{e}_{\beta-\delta} - 3\vec{a}(\beta,-\delta)\right)\right\}\frac{Pik}{2\sqrt{\rho\rho_0}R_0} H_1^{(1)}(kR_0) + \quad (1)$$

$$+ \frac{Pik^2}{2R(\varphi+\delta)}\left(\vec{e}_{\beta-\delta} - 3\vec{a}(\beta,-\delta)\right) M_0\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi+\delta)}\cos\frac{\varphi+\delta}{2}, kR(\varphi+\delta)\right) +$$

$$+ \frac{Pik^3}{2}\left(\vec{e}_{\beta-\delta} - \vec{a}(\beta,-\delta) - \frac{\vec{e}_{\beta-\delta} - 3\vec{a}(\beta,-\delta)}{k^2R^2(\varphi+\delta)}\right)\times$$

$$\times M_1\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi+\delta)}\cos\frac{\varphi+\delta}{2}, kR(\varphi+\delta)\right),$$

дем использовать следующую приближённую формулу $\vec{\Phi}_1(\beta,\delta)$:

$$\vec{\Phi}_1(\beta,\delta)\approx\left\{\left[\vec{e}_1\left[\vec{e}_{\frac{\varphi-\delta}{2}+\beta},\vec{e}_1\right]\right]-\right.$$

$$\left.-\frac{\vec{a}(\beta,-\delta)-\vec{a}(\beta,\ \pi+\varphi)}{2\cos\dfrac{\varphi+\delta}{2}}\right\}\frac{Pik^2}{2\sqrt{\rho\rho_0}}H_0^{(1)}(kR_0)+$$

$$+\frac{Pik^3}{2}\left(\vec{e}_{\beta-\delta}-\vec{a}(\beta,-\delta)-\frac{\vec{e}_{\beta-\delta}-3\vec{a}(\beta,-\delta)}{k^2R^2(\varphi+\delta)}\right)\times$$

$$\times M_1\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi+\delta)}\cos\frac{\varphi+\delta}{2},\ kR(\varphi+\delta)\right) \quad (21)$$

4. Приближённая формула напряжённости электрического поля, порождённого диполем в присутствии идеально проводящей полуплоскости

Приближённую формулу напряжённости электрического поля $\vec{E}(\rho,\varphi,z)$ в присутствии идеально проводящей полуплоскости получим, если в формулу (3) подставить приближённые значения векторной функции $\vec{\Phi}_1(\beta,\delta)$ (21).

$$\vec{E}(\rho,\varphi,z)\approx\left\{\left[\vec{e}_1\left[\vec{e}_{\frac{\varphi-\varphi_0}{2}},\vec{e}_1\right]\right]-\right.$$

$$\left.-\frac{\vec{a}(-\varphi_0,\varphi_0)-\vec{a}(-\varphi_0,\ \pi+\varphi)}{2\cos\dfrac{\varphi-\varphi_0}{2}}\right\}\times$$

$$\times\frac{Pik^2}{2\sqrt{\rho\rho_0}}H_0^{(1)}(kR_0)+\frac{Pik^3}{2}\left(\vec{e}_0-\vec{a}(-\varphi_0,\varphi_0)-\right.$$

$$\left.-\frac{\vec{e}_0-3\vec{a}(-\varphi_0,\varphi_0)}{k^2R^2(\varphi-\varphi_0)}\right)\times M_1\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi-\varphi_0)}\cos\frac{\varphi-\varphi_0}{2},\right.$$

$$\left.kR(\varphi-\varphi_0)\right)-\left\{\left[\vec{e}_1\left[\vec{e}_{\frac{\varphi-(\varphi_0-2\pi)}{2}+\varphi_0},\vec{e}_1\right]\right]-\right.$$

$$\left.-\frac{\vec{a}(\varphi_0,-\varphi_0+2\pi)-\vec{a}(\varphi_0,\ \pi+\varphi)}{2\cos\dfrac{\varphi+\varphi_0-2\pi}{2}}\right\}\times$$

$$\times\frac{Pik^2}{2\sqrt{\rho\rho_0}}H_0^{(1)}(kR_0)+\frac{Pik^3}{2}\left(\vec{e}_{2\pi}-\vec{a}(\varphi_0,-\varphi_0+\right.$$

$$\left.+2\pi)-\frac{\vec{e}_{2\pi}-3\vec{a}(\varphi_0,-\varphi_0+2\pi)}{k^2R^2(\varphi+\varphi_0-2\pi)}\right)\times$$

$$\times M_1\left(\frac{2\sqrt{\rho\rho_0}}{R(\varphi+\varphi_0-2\pi)}\cos\frac{\varphi+\varphi_0-2\pi}{2},\right.$$

$$\left.kR(\varphi+\varphi_0-2\pi)\right). \quad (22)$$

Воспользовавшись равномерным по x при $|x|\geq\varepsilon>0$ (ε — произвольно малое число) разложением функции M_n (x, y) в асимптотический ряд по асимптотической последовательности получим расчётные формулы для приближённого вычисления напряжённости электрического поля.

$$\left.\frac{H_{m+1-n}^{(1)}\left(y\sqrt{1+x^2}\right)}{\left(y\sqrt{1+x^2}\right)^{m+1}}\right|m\in N',$$

5. Теоретические и экспериментальные результаты поведения глиссады ГРМ на площадке ограниченных размеров

На рис. 2 приведён вид со спутника прибрежной части аэродрома.

Извилистая белая полоса в нижней части рисунка обусловлена набегающими на берег морскими волнами. Ниже этой полосы — море, выше земная аэродромная поверхность. Серая полоса с белыми разметками — взлётно-посадочная полоса. Перпендикулярная к ней полоска — рулёжная дорожка. Высота обрыва на границе земная поверхность-поверхность моря равна 1,5м. В точке О установлен ГРМ. Таким образом, ГРМ установлен на земной площадке ограниченных размеров.

Аппроксимируем подстилающую поверхность для ГРМ идеально проводящей полуплоскостью П, расположенной на плоскости y = 0 вдоль отрицательной полуоси x, П(y = 0, x < 0) (рис.3).

На рис. 3 точка В (точка пересечения оси ВПП с ребром полуплоскости) — начало декартовой системы координат (В, x, y, z) и начало оси z цилиндрической системы координат.

Ось z декартовой системы координат направлена вдоль ребра клина.

ГРМ установлен в точке О на расстоянии 150 м от оси O_1O_1 ВПП и 200 м от торца ВПП. Точка А – проекция источника Q на ось ВПП. Расстояние АВ от проекции А источника на ось ВПП до точки В пересечения оси ВПП с ребром полуплоскости равно 270 м.

Ось ВПП образует с ребром полуплоскости угол, равный $\Theta=69^0$. Высота подвеса h верхней антенны ГРМ, расположенной в точке Q, равна 2,55 м. Расстояние Oz_0 равно 198 м. Полуплоскость наклонена относительно горизонтальной плоскости на 25′. Угол глиссады относительно горизонтальной плоскости равен 3^0 и, следовательно, относительно полуплоскости равен $3^0\,25'$.

Рассмотрим самый простой из семейства ГРМ, так называемый ГРМ с «опорным нулём»

Рис. 2. Вид со спутника прибрежной части аэродрома

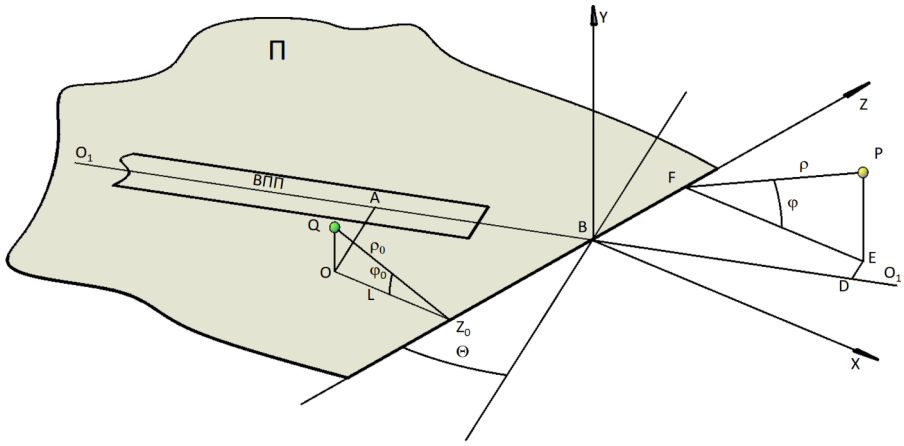


Рис. 3. Модель подстилающей поверхности в виде полуплоскости

[18]. Он включает в себя две антенны, установленные друг над другом на вертикальной мачте; высоты подвеса относительно поверхности Земли верхней h_1 и нижней h_2 антенн равны:

$$h_1 = \frac{\lambda}{2\sin\left(\theta_{gl} + \eta\right)},\ h_2 = \frac{\lambda}{4\sin\left(\theta_{gl} + \eta\right)}, \quad (24)$$

где: λ — длина волны, θ_{gl} — угол глиссады, η — угол уклона местности.

Будем для определённости рассматривать ГРМ дециметрового диапазона волн (ДЦВ) [18]. ГРМ ДЦВ формирует в окружающем пространстве навигационный параметр, называемый коэффициентом разнослышимости сигналов (*KPC*)[18].

$$KPC = \frac{\left|E_2(R,\theta) + aE_1(R,\theta)\right| - \left|E_2(R,\theta) - aE_1(R,\theta)\right|}{\left|E_2(R,\theta) + aE_1(R,\theta)\right| + \left|E_2(R,\theta) - aE_1(R,\theta)\right|} \quad (23)$$

где: (R,θ) — координаты точки наблюдения в полярной системе координат с началом в основании мачты; угол θ отсчитывается от плоскости против хода часовой стрелки;

$E_2(R,\theta)\left[E_1(R,\theta)\right]$ — комплексная амплитуда напряжённости электрического поля, формируемого нижней (верхней) антенной;

a — коэффициент, равный отношению амплитуды тока в верхней антенне к амплитуде тока в нижней антенне.

На рис. 4 представлена зависимость КРС на прямой, проходящей через точку А и составляющей угол

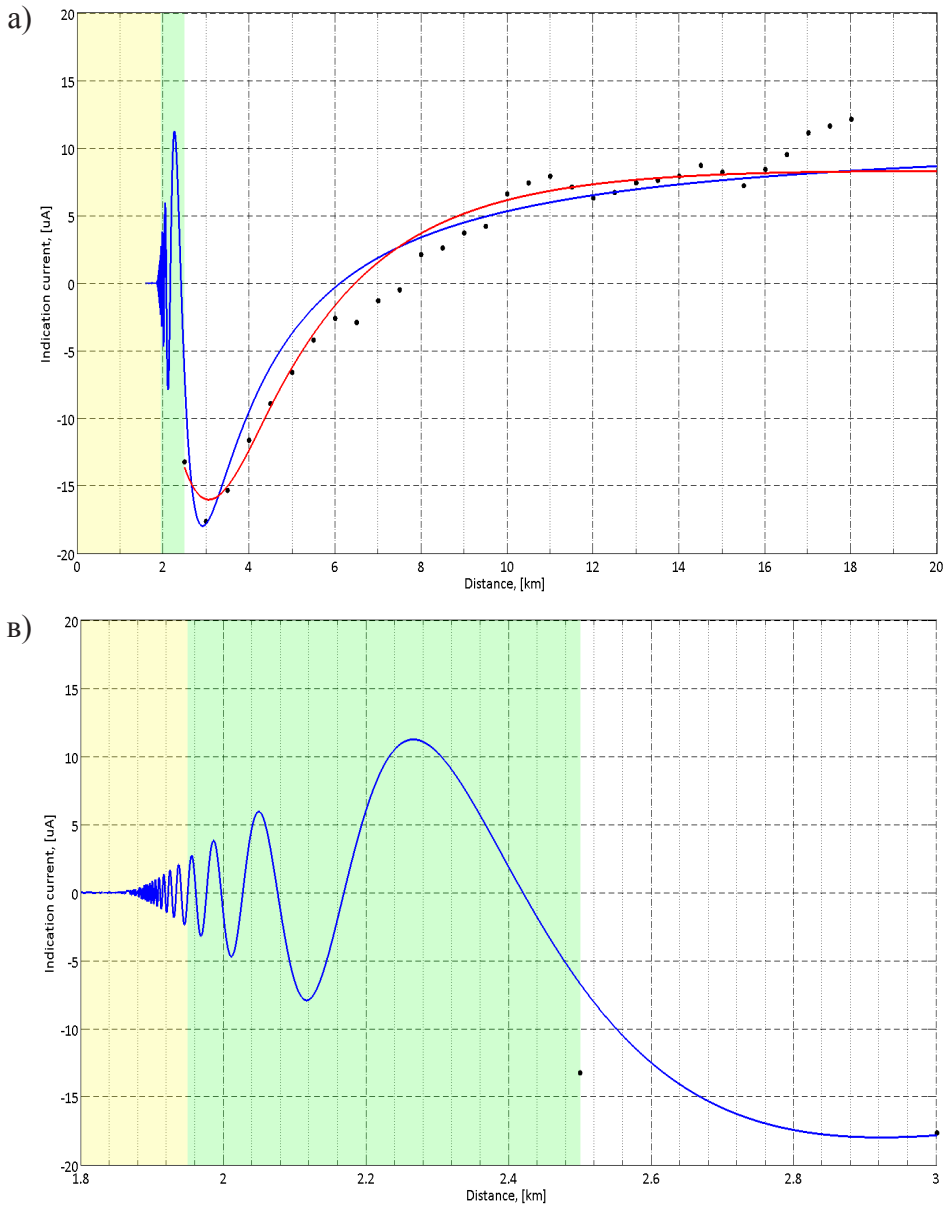


Рис.4. Зависимость Коэффициента Разнослышимости Сигналов (КРС) от дальности

3^0 25′ с осью ВПП. По горизонтальной оси отложена дальность вдоль оси ВПП относительно её центра. С приближением к ВПП, на участке от 20 км до 3 км КРС монотонно убывает, достигая минимума на удалении 3 км. Ближе 3 км зависимость КРС от расстояния имеет вид осциллирующей кривой, убывающей по амплитуде. На рис на бесцветном, зелёном и жёлтом участках приняты разные масштабы вдоль горизонтальной оси с целью демонстрации убывания периода осцилляций. Красным цветом представлен график функции КРС, вычисленной для модели подстилающей поверхности в предположении ортогональности оси ВПП с ребром полуплоскости. При этом ГРМ расположен на оси ВПП. Синим цветом представлена зависимость КРС от дальности в предположении, что ГРМ, как лётное препятствие, вынесен относительно оси ВПП. Ось ВПП составляет с ребром полуплоскости угол, равный 69^0. Точками отмечены результаты летных измерений для ГРМ, установленном на аэродроме, как показано на рис. 4.

Как следует из рассмотрения графиков на рис. 4, поведение КРС на луче, определяющее искривления глиссады, имеет одинаковый характер для представленных двух моделей подстилающей поверхности. Экспериментальные данные, представленные для больших удалений от ГРМ близки к расчетным по одной и другой модели. Колебательный характер зависимости на небольших расстояниях от ГРМ объясняется изменением фазовых соотношений между краевой волны и падающей и отражённой волнами.

6. Выводы

С целью выявления закономерностей в поведении глиссады, обусловленного конечными размерами земной площадки перед ГРМ, предложено подстилающую поверхность, на которой расположен ГРМ, аппроксимировать идеально проводящей полуплоскостью. На основе строгого решения задачи дифракции электромагнитного поля, созданного дипольным источником на идеально проводящей полуплоскости, получено приближённое решение задачи дифракции.

В области пространства, в которой расположена глиссада, приближённое решение представлено суммой полей двух сферических волн: волны, падающей непосредственно от диполя (реального источника), волны, зеркально отражённой от полуплоскости (мнимого источника) и краевой волны, формируемой в окрестности ребра полуплоскости. Поведение глиссады обусловлено интерференцией поля краевой волны с полем волн реального и мнимого источников. Расчётная зависимость информационного параметра от дальности в области далее ребра полуплоскости близка к экспериментальной зависимости, полученной лётным путём на прибрежном аэродроме, на котором ось ВПП составила с кромкой обрыва аэродромной поверхности к морю угол 690, а расстояние от проекции ГРМ на ось ВПП до точки пересечения оси ВПП с обрывом равно 435 м.

Целесообразно продолжить численные исследования влияния ограниченных размеров площадки на поведение глиссады.

Литература

1. Watts, C.B., Jr. Instrument Landing Scrapbook / C.B., Jr. Watts. – Trafford Publishing, 2005. – 392 p.

2. НИИ-33 / ВНИИРА. История становления и развития Всесоюзного НИИ радиоаппаратуры. – СПб., 2007. – 291 с.

3. Войтович Н.И., Жданов Б.В. "Четыре ключевых технических решений в истории развития ILS (системы посадки самолётов)" //Сборник 28-ой Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2018). Материалы конференции. – 9-15 Сентября 2018 г. Том 8 – С.1882-1890. Севастополь, Крым, Россия.

4. Патент РФ на изобретение № 2429499 "Глиссадный радиомаяк" авторов Войтовича Н.И. и Жданова Б.В. и Соколова А.Н.

5. Iungaitis E.M., Voytovich N.I., Ershov A.V., Zhdanov B.V., Zotov A.V. ILS Glide Slope Antenna Array for Airfields with a High Level of Snow Cover. 2019 13th European Conference on Antennas and Propagation (EuCAP), https://ieeexplore.ieee.org/document/8740267.

6. A.Thain and others. Stealh Buidings at Airbus Group Innovations. IEEE Antennas & Propagation Magazine. – February 2016.

7. S. Odunaiya, "A physical theory of diffraction model for predicting the effects of multipath on ILS and VOR performance," in Proc. 1999 Nat. Technical Meeting Institute Navigation, San Diego, CA, Jan. 1999, P. 435–446.

8. R. F. Harrington, Field Computation by Moment Methods. Piscataway, NJ: IEEE Press, ISBN 0780310144, 1993.

9. M. Song and W. C. Chew, "Multilevel fast multipole algorithm for solving combined field integral equations of electromagnetic scattering," Microwave Opt. Technol. Lett., vol. 10, no. 1, P. 14–19, 1995.

10. Unichi Honda, Hirohisa Tajima and Hisashi Yokoyama "Influences of ILS Localizer Signalover Complicated Terrain". Proceedings of the 11th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2017). - Springer.

11. Unichi Honda, Hirohisa Tajima and Hisashi Yokoyama "Numerical Simulation of Glide Slope Signal Interferences by Irregular Ground" WEB, ARTIFICIAL INTELLIGENCE AND APPLICATIONS. Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019). - Springer.

12. Yungaitis E.M., Voytovich N. I.,Golovnin A. A., Zhdanov B. V. "Radio Wave Diffraction on Ledge-like Underlying Surface", IET Conference Publications, 12th European Conference on Antennas and Propagation, EuCAP 2018, DOI: 10.1049/cp.2018.1080.

13. J.J. Bowman and T.B.A. Senior. Diffraction of a Dipole Field by a Perfectly Conducting Half Plane. Radio Science. Vol.2 (New Series). No.11. November 1967.

14. Vandakurov Y.V. Diffraction of electromagnetic waves by an arbitrarily oriented electric or magnetic dipole on a perfectly conducting half plane. Journal of Experimental and Theoretical Physics. - 1954. Vol. 26, pp. 3-18 (in Russian).

15. Тужилин, А.А Представление электромагнитных полей, порожденных диполями в присутствии идеально проводящей полуплоскости, через интегралы Макдональда, Дифференц. уравнения, 1967, том 3, номер 11, 1971–1989

16. Тужилин, А.А. Асимптотические разложения решений задач дифракции волн в угловых и клиновидных областях / А.А. Тужилин // Журнал вычислительной математики и математической физики. – 1970. – Том 10, № 1. – С. 99-113.

17. Андреева Т.Г. Математика: Специальные функции и некоторые приложения. СПб.: РГГМУ, 2013. — 102 с.

18. G.A.Paholkov, V.V.Kashinov, M.E.Solomonik, U.G.Shatrakov. [Gauge radioengineering landing systems: (Forecasting of precision characteristics)]. G.A.– M.: Transport, 1982. –p.159. (In Russian).

References

1. Watts, C.B., Jr. Instrument Landing Scrapbook / C.B., Jr. Watts. – Trafford Publishing, 2005. – 392 p.

2. NII-33 / VNIIRA. Istorija stanovlenija i razvitija Vsesojuznogo NII radioapparatury. – SPb., 2007. – 291 s.

3. Vojtovich N.I., Zhdanov B.V. "Chetyre kljuchevyh tehnicheskih reshe-nij v istorii razvitija ILS (sistemy posadki samoljotov)" //Sbornik 28-oj Mezhdunarodnoj Krymskoj konferencii «SVCh-tehnika i telekommunikaci-onnye tehnologii» (KryMiKo'2018). Materialy konferencii. – 9-15 Sen-tjabrja 2018 g. Tom 8 – S.1882-1890. Sevastopol', Krym, Rossija.

4. Patent RF na izobretenie № 2429499 "Glissadnyj radiomajak" av-torov Vojtovicha N.I. i Zhdanova B.V. i Sokolova A.N.

5. Iungaitis E.M., Voytovich N.I., Ershov A.V., Zhdanov B.V., Zotov A.V. ILS Glide Slope Antenna Array for Airfields with a High Level of Snow Cover. 2019 13th European Conference on Antennas and Propagation (EuCAP), https://ieeexplore.ieee.org/document/8740267.

6. A.Thain and others. Stealh Buidings at Airbus Group Innovations. IEEE Antennas & Propagation Magazine. – February 2016.

7. S. Odunaiya, "A physical theory of diffraction model for predicting the effects of multipath on ILS and VOR performance," in Proc. 1999 Nat. Technical Meeting Institute Navigation, San Diego, CA, Jan. 1999, P. 435–446.

8. R. F. Harrington, Field Computation by Moment Methods. Piscataway, NJ: IEEE Press, ISBN 0780310144, 1993.

9. M. Song and W. C. Chew, "Multilevel fast multipole algorithm for solving combined field integral equations of electromagnetic scattering," Microwave Opt. Technol. Lett., vol. 10, no. 1, P. 14–19, 1995.].

10. Unichi Honda, Hirohisa Tajima and Hisashi Yokoyama "Influences of ILS Localizer Signalover Complicated Terrain". Proceedings of the 11th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2017). - Springer.

11. Unichi Honda, Hirohisa Tajima and Hisashi Yokoyama "Numerical Simulation of Glide Slope Signal Interferences by Irregular Ground" WEB, ARTIFICIAL INTELLIGENCE AND APPLICATIONS. Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019). - Springer.

12. Yungaitis E.M., Voytovich N. I.,Golovnin A. A., Zhdanov B. V. "Radio Wave Diffraction on Ledge-like Underlying Surface", IET Conference Publications, 12th European Conference on Antennas and Propagation, EuCAP 2018, DOI: 10.1049/cp.2018.1080.

13. J.J. Bowman and T.B.A. Senior. Diffraction of a Dipole Field by a Perfectly Conducting Half Plane. Radio Science. Vol.2 (New Series). No.11. November 1967.

14. Vandakurov Y.V. Diffraction of electromagnetic waves by an arbitrarily oriented electric or magnetic dipole on a perfectly conducting half plane. Journal of Experimental and Theoretical Physics. - 1954. Vol. 26, pp. 3-18 (in Russian).

15. Tuzhilin, A.A Predstavlenie jelektromagnitnyh polej, porozhden-nyh dipoljami v prisutstvii ideal'no provodjashhej poluploskosti, cherez integraly Makdonal'da, Differenc. uravnenija, 1967, tom 3, nomer 11, 1971–1989.

16. Tuzhilin, A.A. Asimptoticheskie razlozhenija reshenij zadach di-frakcii voln v uglovyh i klinovidnyh oblastjah / A.A. Tuzhilin // Zhurnal vychislitel'noj matematiki i matematicheskoj fiziki. – 1970. – Tom 10, № 1. – S. 99-113.

17. Andreeva T.G. Matematika: Special'nye funkcii i nekotorye prilozhenija. SPb.: RGGMU, 2013. — 102 s.

18. G.A.Paholkov, V.V.Kashinov, M.E.Solomonik, U.G.Shatrakov. [Gauge radioengineering landing systems: (Forecasting of precision characteristics)]. G.A.– M.: Transport, 1982. –p.159. (In Russian).

ВОЙТОВИЧ Николай Иванович, доктор технических наук, профессор, заведующий кафедрой конструирования и производства радиоаппаратуры, ФГАОУ ВО «Южно-Уральский госу-

дарственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: voytovichni@mail.ru

VOYTOVICH Nikolay Ivanovich, Doctor of Technical Sciences, Professor, Head of the Department of Design and Production of Radio Equipment, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: voytovichni@mail.ru

ЮНГАЙТИС Екатерина Михайловна, младший научный сотрудник, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: jungaitis92@gmail.ru

IUNGAITIS Ekaterina Mikhailovna, junior researcher, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: jungaitis92@gmail.ru

ЕРШОВ Алексей Валентинович, кандидат технических наук, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: eav@list.ru

ERSHOV Aleksey Valentinovich, PhD in Engineering sciences, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: eav@list.ru

УДК 621.37.037 Вестник УрФО № 1(43) / 2022, с. 22–27

Степанцова А.М., Петухов А.Г., Делог А.Н., Степанцов С.В.

DOI: 10.14529/secur220103

АНАЛИЗ ВОЗДЕЙСТВИЯ ИОНОСФЕРНОГО ЛУЧА НА РАСПРОСТРАНЕНИЕ РАДИОВОЛН

На сегодняшний день можно отметить возрастание интереса обеспечения безопасности информации в области развития радиосвязи декаметрового диапазона (ДКМ), основанной на распространении радиоволн за счет отражения их от ионосферы. Внимание к ДКМ обусловлено активным развитием цифровых технологий и методов цифровой обработки информации, передачи сигналов. Любая организация приема-передачи сигналов строится на трех основных пунктах: 1 – устройство передачи, 2 – принимающее устройство, 3 – линии соединения (промежуточное звено). В радиосистеме роль промежуточного звена играет среда, в которой распространяются радиоволны. Вопрос исследования распространения электромагнитных волн в слоях верхней и нижней атмосферы является актуальным и определяется потребностью решения проблем дальней радиосвязи, радиолокации и радионавигации, при этом не следует забывать о проблемеизучения структуры средыпередачи. В статье рассматривается строение ионосферы, преломление и отражение в ней радиоволн и выбор рабочих частот для связи ионосферным лучом.

Ключевые слова: *радиоволны, ионосфера, ионизация, атмосфера, рабочая частота, напряжение поля, путь пространственной волны, безопасность информации.*

Stepancova A.M., Petukhov A.G., Delog A.N., Stepancov S.V.

ANALYSIS OF THE EFFECT OF THE IONOSPHERIC BEAM ON THE PROPAGATION OF RADIO WAVES

To date, it can be noted that there is an increasing interest in ensuring the security of information in the field of the development of decameter radio communications (DCM), based on the propagation of radio waves due to their reflection from the ionosphere. Attention to DCM is due to the active development of digital technologies and methods of digital information processing and signal transmission. Any organization of signal reception and transmission is based on three main points: 1 – transmission device, 2 – receiving device, 3 – connection lines (intermediate link). In a radio system, the medium in which radio waves propagate plays the role of an intermediate link. The issue of studying the propagation of electromagnetic waves in the layers of the upper and lower atmosphere is relevant and is determined by the need to solve the problems of long-range radio communication, radar and radio navigation, while one should not forget about the problem of studying the structure of the medium transmission. The article discusses the structure of the ionosphere, the refraction and reflection of radio waves in it and the choice of operating frequencies for ionospheric beam communication.

Keywords: *radio waves, ionosphere, ionization, atmosphere, operating frequency, field voltage, spatial wave path, information security.*

Изучая вопрос распространения радиоволн ионосферным лучом помимо учебной литературы для анализа и определения актуальности тематики статьи были приняты во внимание публикации по темам: «Эффект анизотропии ионосферных неоднородностейпри регистрации сбоев фазовых измерений ГНСС» (2019 г., И. В. Безлер, А. Б. Ишин, Е.В. Конецкая, М. В. Тинин), «Результаты исследования пространственно-корреляционных характеристик однолучевого ионосферного декаметрового канала связи» (2020 г., И.М. Орощук, И.Е. Гуреев, А.Н. Сучков, М.В. Соловьев), «Полугодовая вариация космических лучей

и ионосферы» (2020 г., В. Л. Янчуковский, А. Ю. Белинская), «Ионосферный мониторинг в интересах перспективных адаптивных систем декаметровой радиосвязи: современное состояние и перспективы развития» (2020 г., С.А. Коваль).

В своих работах авторы рассматривают ионосферу: как явление, подверженное влиянию внешних факторов, таких как освещенность атмосферы, времени суток и времени года, магнитного поля Земли; как среду, по своему строению не однородную, так как в каждом из слоев своя электрическая концентрация.

Освещена проблема намеренного создания искусственных возмущений ионосферы силами противника, с целью разрушения радиоканалов связи, находящихся в определенных диапазонах частот (создание в них замираний, помех и затуханий). Проведен анализ способов мониторинга ионосферы для сбора данных о ее состоянии, с целью определения возможностей развития измерения параметров ионосферы и радиолиний, использования собранных сведений для проектирования адаптивных систем декаметровой радиосвязи.

При рассмотрении характеристик направленного действия передающих антенн было установлено, что в вертикальной плоскости излучение энергии происходит под разными углами к горизонту. Энергия радиоволн, излучаемая под большими углами к горизонту (больше 10–15°), отрывается от поверхности земли и в создании поля земной волны не участвует. Однако эта часть энергии может быть использована для передачи сигналов, благодаря наличию в верхних слоях атмосферы ионизированных областей. Они обладают способностью отражать радиоволны.

Радиоволны, отраженные от ионосферы, называют ионосферными. Связь, осуществляемую с помощью этих волн, называют связью ионосферным (пространственным) лучом [1]. При связи ионосферным лучом, радиоволны, распространяясь от передающей станции А к приемной В, проходят путь АБВ, показанный на рис. 1 стрелками. Как видно из рисунка, ионосферные волны на всем протяжении от передатчика до приемника распространяются вдали от земли. Напряженность поля в точке приема В зависит только от электрических свойств ионизированных слоев атмосферы.

Строение ионосферы. До недавнего времени считалось, что земная атмосфера простирается на высоту до 800–1000 км. Однако согласно данным, полученным при запуске советских искусственных спутников Земли и Солнца, стало известно, что земная атмосфера простирается гораздо выше. Благодаря существованию восходящих воздушных потоков верхнии слои атмосферы имеют такой же состав газов, что и у поверхности земли. На больших высотах происходит расслоение атмосферы, причем молекулы более легких газов, составляющих атмосферу, располагаются преимущественно в вышележащих слоях. С удалением от поверхности земли изменяется и давление, а следовательно, и плотность атмосферы (число молекул, приходящихся на 1 см^3). Так, у поверхности Земли число молекул в 1 см^3 достигает 2,7 • 10^{19}, а на высоте 250 км, где давление ориентировочно равно 2 – 10^{-11} миллиметров ртутного столба, плотность составляет всего лишь 7 • 10^5 молекул в 1 см3 [2].

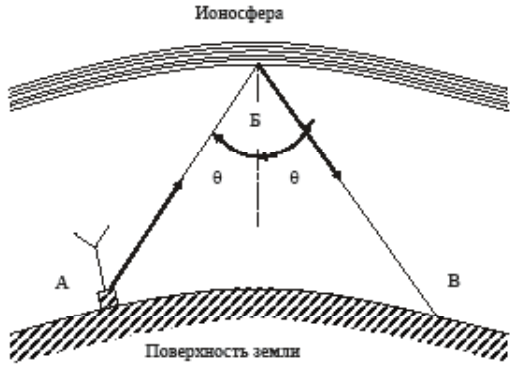


Рис. 1. Ход луча радиоволн при распространении ионосферным лучом

Земная атмосфера непрерывно находится под воздействием космических излучений различного происхождения в виде электромагнитных волн и частиц энергии (корпускул), которые достигая атмосферы земли, сталкиваются с молекулами или атомами газов, расщепляют их, отдавая им часть своей энергии. При этом из атомов и молекул выделяются свободные электроны и положительно заряженные частицы – ионы. С течением времени свободные электроны и ионы могут сталкиваться друг с другом и создавать снова нейтральные атомы и молекулы. Процесс отрывания от атомов и молекул свободных электронов называют ионизацией, а процесс воссоединения электронов с ионами – рекомбинацией. Основным источником ионизации земной атмосферы являются ультрафиолетовые лучи, испускаемые солнцем.

Из физики известно, что для ионизации молекул того или иного газа требуется определенная энергия, различная для разных газов. Учитывая это, а также указанное выше распределение газов в атмосфере по высоте, можно ожидать наличия в ней областей с максимумом и минимумом ионизации [3]. Такое предположение подтверждается многочисленными экспериментами, в том числе и результатами, добытыми при запуске искусственных спутников Земли. В настоящее время установлено существование в атмосфере четырех явно выраженных слоев (максимумов) ионизации, обозначаемых буквами D, E, F_1 и F_2. Примерное удаленность этих слоев от земли показано на рис. 2.

Основной характеристикой слоев ионизации является количество свободных электронов в одном кубическом сантиметре – так называемая электронная концентрация.

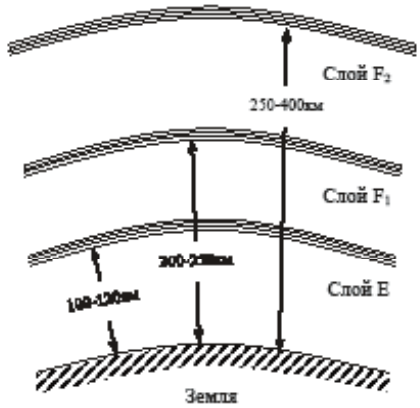


Рис. 2. Удаление ионизированных слоев атмосферы от поверхности земли; слой D располагается ниже слоя E

Электронная концентрация слоев зависит от интенсивности ионизирующих факторов, состава и плотности ионизируемого газа и скорости протекания процесса рекомбинации. Она может непрерывно изменяться как во времени, так и по месту на земном шаре, в соответствии с изменениями освещенности отдельных его областей. Наименьшая электронная концентрация наблюдается для слоя D, наибольшая – для слоя F_2. С наступлением темноты, когда источник ионизации – солнечное излучение – экранируется землей, слой D может исчезать полностью. Слой F_1 также образуется лишь в дневное время, исчезая в ночное. Слои E и F_2 устойчиво наблюдаются в любое время суток, хотя их электронная концентрация в течение суток претерпевает значительные изменения, возрастая днем и уменьшаясь в ночное время. Исчезновение в ночное время слоев D и F_1, а также уменьшение электронной концентрации слоев E и F_2 объясняется процессом рекомбинации, который протекает непрерывно, в то время как ионизация происходит главным образом при солнечном освещении, т.е. в дневное время [4].

Преломление и отражение радиоволн в ионосфере. Ионизированные слои атмосферы могут изменять направление распространения радиоволн и поглощать большую или меньшую часть их энергии. Это можно упрощенно объяснить следующим образом. При распространении электромагнитных волн в ионосфере находящиеся в ней свободные электроны под действием поля распространяющейся волны приходят в колебательное движение и создают свое электромагнитное поле излучения.

Под действием поля колеблющихся электронов, приходящая волна изменяет свое направление в сторону уменьшения электронной концентрации слоя. Как это установлено исследованиями, электронная концентрация слоя возрастает от его нижней кромки (от границы, обращенной к земле), достигая максимума в более высоких областях. Поэтому радиоволны, попадая в слой ионосферы, под тем или иным углом преломляются постепенно в сторону земли до тех пор, пока не выйдут из него. Это явление называют отражением радиоволн от ионосферы.

Перемещение электронов полем приходящей волны связано для нее с потерей части энергии, которая возрастает с увеличением длины волны (периода колебаний), так как при этом увеличивается амплитуда перемещений электронов. Амплитуда напряженности поля, создаваемого перемещающимися электронами, а следовательно, и его влияние на поле приходящей волны также возрастают с увеличением длины волны [5].

Из сказанного вытекают следующие важные заключения:

1. Чем больше в слое с заданной электронной концентрацией происходит поглощение энергии радиоволн и их преломление, тем больше длина волны.

2. Чем больше поглощение энергии радиоволн и их преломление для заданной длины волны, тем больше электронная концентрация ионизированного слоя.

Зная электронную концентрацию слоя ионизации, можно заранее определять условия поглощения и преломления в нем радиоволн той или иной длины.

Если волна очень короткая, то электронная концентрация слоя F_2 может оказаться недостаточной для их отражения. Такие волны на поверхность земли не возвращаются, они проходят через слой ионизации и уходят в мировое пространство.

Таким образом, можно наблюдать следующие особенности связи ионосферным лучом: сравнительно длинные волны в дневное время отражаются уже от слоя E. Если электронная концентрация слоя E для их отражения недостаточна, то они проходят через этот слой и отражаются от слоя F_1 или F_2. Проходя два раза через нижележащие слои (при движении от земли к отражающему слою и от этого слоя к земле), они теряют часть своей энергии, и падают на землю ослабленными. При этом более ослабленными оказываются наиболее длинные волны. Уменьшая длину волны, можно достигнуть резкого уменьшения поглощения ее энергии в нижележащих слоях. Однако уменьшать длину волны можно лишь до тех пор, пока она еще отражается от слоя F_2, имеющего наибольшую электронную концентрацию. Дальнейшее укорочение волны может привести к тому, что она не будет отражаться ни от одного слоя. Осуществить связь ионосферным лучом на такой волне невозможно.

Для связи ионосферным лучом применяются преимущественно короткие волны с расчетом отражения их от слоя F_2. Влияние на связь нижележащих слоев в этом случае сказывается лишь в том, что в них поглощается часть энергии радиоволн, причем чем больше, тем длиннее волна.

Электронная концентрация слоев ионизации колеблется в широких пределах в течение суток, време-

ни года, одиннадцатилетнего периода солнечной активности, а также географического положения наблюдаемых точек [6]. Кроме регулярных изменений состояния ионосферы, вызываемых перечисленными выше причинами, наблюдаются нерегулярные резкие изменения (ионосферные возмущения), связанные с эпизодическими вспышками солнечной активности.

Ввиду того что состояние ионосферы непрерывно меняется, естественно ожидать, что напряженность поля ионосферного луча будет меняться непрерывно. Действительно, как показывают многочисленные исследования, напряженность поля ионосферных волн с течением времени меняется в очень широких пределах.

Для получения круглосуточного устойчивого приема возникает необходимость предварительно изучать состояние ионосферы, чтобы использовать волны, которые меньше всего поглощаются в ионосфере и могут отражаться от нее.

Изучением состояния ионосферы на ответственных трассах радиосвязи занимается (в государственном или ведомственном масштабе) специальная служба, называемая ионосферной службой. В прогнозах (бюллетенях) этой службы обычно указывается: в какое время года и суток, на какие расстояния, какие волны будут наиболее эффективными, т.е. будут распространяться с наименьшим затуханием [7].

Выбор рабочих частот для связи ионосферным лучом. Самую короткую волну, которая еще может отразиться от данного слоя ионизации при излучении в зенит (рис. 3), называют критической волной, а соответствующую ей частоту $f_{кр}$ – критической частотой этого слоя. Если волны встречают тот же ионизированный слой под некоторым углом, меньшим 90°, или, согласно рисунку 3 под углом $\theta > 0^0$ (наклонное падение), то от него могут отражаться волны, имеющие частоту колебаний $f_{раб}$, соответствующую более высоким частотам, чем $f_{кр}$. Зависимость $f_{раб}$ от угла падения радиоволн на слой ионосферы и от критической частоты $f_{кр}$ выражается следующим соотношением:

$$f_{раб} = \frac{f_{кр}}{\cos\theta^2}, \qquad (1)$$

где $f_{раб}$ – рабочая частота; θ – угол падения волн на ионосферу.

Как видно, для данной $f_{кр}$ рабочая частота возрастает с увеличением θ. Волны, имеющие частоту колебаний выше найденной из соотношения (1), отражаться при падении под углом $\theta_2 < \theta_1$ не будут. Не будут отражаться и волны той же длины, но излучаемые под углом $\theta_2 < \theta_1$. Волны, имеющие частоту колебаний меньше $f_{раб}$, найденной из выражения (1), хотя и будут отражаться, но невыгодны для связи вследствие большого затухания в нижележащих слоях.

Расстояние АВ от передатчика до точки, в котором отраженный от ионосферы луч достигает земли, называют расстоянием скачка ионосферной волны. Нетрудно определить, что это расстояние зависит от угла θ и высоты h отражающего слоя ионосферы. Так, для θ = 45° и h = 300 км расстояние скачка AB = 2 • 300 tg 45° = = 600 км. При удалении меньше указанного расстояния, поле будет сильно ослаблено или полностью отсутствовать. Зона местности между передающим и приемным пунктами, в которой прием невозможен, называется «зоной отсутствия слышимости» («мертвой зоной») [8].

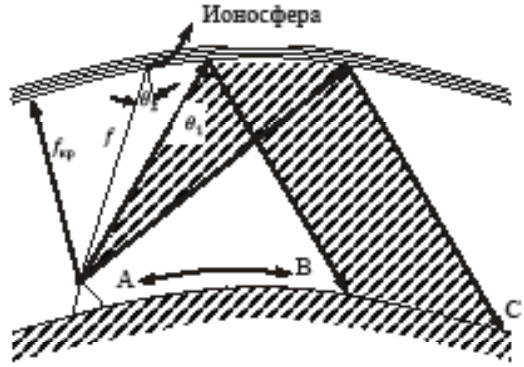


Рис. 3. Зависимость отражения радиоволн от частоты и от угла встречи радиолучей с ионизированным слоем

Критические частоты связаны с величиной электронной концентрации слоев-ионизации, поэтому их значения также меняются в широких пределах в течение суток, сезонов года и т.д. В среднем их значения колеблются в пределах: для F_2 – 4–8 Мгц; для F_1 – 4–5 Мгц; для E – 1–3,5 Мгц.

Считая наименьший угол к горизонту, под которым радиоволны распространяются еще ионосферным лучом, равным 10°, получим расстояние скачка в 3500 км. Это расстояние и будет наибольшей дальностью действия радиостанции ионосферным лучом при однократном отражении радиоволн от ионосферы. Для получения таких дальностей при одном скачке луча в дневное время применяют волны длиной 10–25 м, в ночное время 35–100 м.

Если рабочая волна выбрана равной критической, а антенна дает излучение под любыми углами к горизонту, то отражение будет при любых углах излучения. Мертвой зоны в этом случае не будет. Для иллюстрации сказанного на рис. 4 показано примерное распределение уровней напряженности поля ионосферной волны вдоль земной поверхности, создаваемое антенной зенитного излучения. Ординаты отдельных точек кривой CD показывают в некотором масштабе величины напряженности поля по мере удаления от передатчика.

Из изложенного следует, что со стороны более высоких частот выбор рабочей волны ограничивается критической частотой или условиями отражения [9]. Волны, длиннее выбранной по критической часто-

Рис. 4. Изменение напряженности поля ионосферного луча в зависимости от удаления от передатчика

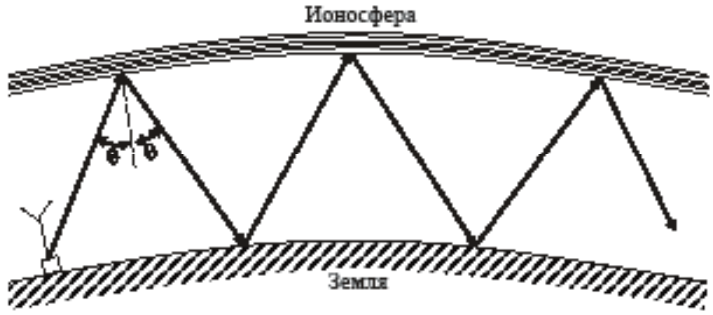


Рис. 5. Путь пространственной волны при многократном отражении от ионосферы и земли

те отражаются, но претерпевают большее поглощение в нижележащих слоях ионосферы, и поэтому их применение нецелесообразно. Следовательно, рабочие частоты со стороны низких, ограничиваются фактором поглощения.

Используя ионосферные волны, можно получать радиосвязь на весьма большие расстояния при относительно небольших мощностях передатчика и гарантированно обеспечивать безопасность каналов связи. Путь лучей радиоволн при связи на сверхдальние расстояния показан на рис. 5. После отражения от ионосферы радиоволны направляются к поверхности земли, и отражаясь от нее, снова достигают ионосферы, и после вторичного отражения направляются к поверхности земли, и так до тех пор, пока энергия волны после многократных отражений не будет полностью израсходована на потери в ионосфере и в земле.

При достаточно большой мощности передатчика с применением антенн остронаправленного действия на выбранных волнах можно получить практически регулярную радиосвязь между любыми точками земного шара.

Волны порядка 7–10 м более или менее регулярно отражаются лишь от слоя F_2 в годы максимальной солнечной активности, когда резко возрастает электронная концентрация этого слоя. От других регулярных слоев, рассмотренных выше, они не отражаются [10].

Литература

1. Баскаков С.И. Электродинамика и распространение радиоволн / С.И. Баскаков. М.: КД Либроком, 2015.416 с.

2. Ерохин Г.А. Антенно-фидерные устройства и распространение ра-диоволн / Г.А. Ерохин, О.В. Чернышев, Н.Д. Козырев. М.: ГЛТ, 2007. 491 с.

3. Кураев, А.А. Электродинамика и распространение радиоволн: Учебное пособие / А.А. Кураев, Т.Л. Попкова, А.К. Синицын. М.: НИЦ Ин-фра-М, Нов. знание, 2013. 424 с.

4. Муромцев Д.Ю. Электродинамика и распространение радиоволн: Учебное пособие, доп. / Д.Ю. Муромцев, Ю.Т. Зырянов. СПб.: Лань, 2014. 448 с.

5. Никольский В.В. Электродинамика и распространение радиоволн / В.В. Никольский, Т.И. Никольская. М.: КД Либроком, 2015. 544 с.

6. Петров Б.М. Электродинамика и распространение радиоволн: Учебник для вузов / Б.М. Петров. М.: Горячая линия - Телеком, 2014. 558 с.

7. Сомов, А.М. Распространение радиоволн и антенны спутниковых систем связи: Учебное пособие для вузов / А.М. Сомов. М.: РиС, 2015. 456 с.

8. Старостин Н. Распространение радиоволн: Учебное пособие / Н. Старостин. М.: Гелиос АРВ, 2010. 264 с.

9. Юндин, М.А. Электродинамика и распространение радиоволн: Учебное пособие / М.А. Юндин, А.М. Королев. СПб.: Лань, 2014. 448 с.

10. Яковлев О.И. Распространение радиоволн / О.И. Яковлев, В.П. Якубов, В.П. Урядов, А.Г. Павельев. М.: Ленанд, 2017. 496 с.

References

1. Baskakov S.I. Electrodynamics and propagation of radio waves / S.I. Baskakov. - M.: CD Librocom, 2015. 416 p.

2. Erokhin G.A. Antenna-feeder devices and radio wave propagation / G.A. Erokhin, O.V. Chernyshev, N.D. Kozyrev. M.: GLT, 2007. 491 p.

3. Kuraev A.A. Electrodynamics and radio wave propagation: Textbook / A.A. Kuraev, T.L. Popkova, A.K. Sinitsyn. M.:SIC In-fra-M, Nov.knowledge, 2013.424 p.

4. MuromtsevD.Yu. Electrodynamics and propagation of radio waves: Textbook, supplement / D.Yu. Muromtsev, Yu.T. Zyryanov. St. Petersburg:Lan, 2014. 448 p.

5. Nikolsky V.V. Electrodynamics and propagation of radio waves / V.V. Nikolsky, T.I. Nikolskaya. M.: CD Librocom, 2015. 544 p.

6. Petrov B. M. Electrodynamics and propagation of radio waves: the Textbook for high schools / B. M. Petrov. M.: GoryachayaLiniya - Telekom, 2014. 558 p.

7. Somov A. M. wave Propagation and antenna channels.-output commu-nication systems: textbook for universities / A. Somov. M.: Rice, 2015. 456 p.

8. Starostin N. Propagation of radio waves: A textbook / N. Starostin. M.: Helios ARV, 2010. 264 p.

9. Yundin M.A. Electrodynamics and radio wave propagation: A textbook / M.A. Yundin, A.M. Korolev. St. Petersburg: Lan, 2014. 448 p.

10. Yakovlev O.I. Propagation of radio waves / O.I. Yakovlev, V.P. Yaku-bov, V.P. Uryadov, A.G. Paveliev. M.: Lenand, 2017. 496 p.

СТЕПАНЦОВА Алёна Михайловна, студентка, «Сибирский государственный университет телекоммуникации и информатики». Россия, 630102, Сибирский федеральный округ, Новосибирская область, г. Новосибирск, ул. Кирова, д. 86. E-mail: alena169vega@yandex.ru

STEPANCOVA Aljona Mihajlovna, student, "Siberian State University of Telecommunications and Informatics". Russia, 630102, Siberian Federal District, Novosibirsk region, Novosibirsk, Kirova str., 86. E-mail: alena169vega@yandex.ru

ПЕТУХОВ Александр Георгиевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: putnik0879@mail.ru

PETUKHOV Alexander Georgievich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: putnik0879@mail.ru

ДЕЛОГ Андрей Николаевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: delog_mga@mail.ru

DELOG Andrey Nikolaevich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: delog_mga@mail.ru

СТЕПАНЦОВ Сергей Валерьевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: cjrjkjdj@mail.ru

STEPANCOV Sergej Valer'evich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: cjrjkjdj@mail.ru

УДК 342.843 Вестник УрФО № 1(43) / 2022, с. 28–34

Мирвода С.Г., Поршнев С.В., Рябко Н.Ю.

DOI: 10.14529/secur220104

АВТОМАТИЗАЦИЯ ПРОЦЕДУРЫ ДОСТУПА К ЭЛЕКТОРАЛЬНЫМ ДАННЫМ, РАЗМЕЩЕННЫХ НА САЙТЕ ЦЕНТРАЛЬНОЙ ИЗБИРАТЕЛЬНОЙ КОМИССИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье описан программный инструмент, осуществляющий автоматическую выгрузку электоральных данных о выборах в 2018 г. Президента Российской Федерации (РФ), размещенных на официальном сайте Центральной избирательной комиссии (ЦИК), включая: сводные данные по РФ; сводные данные, представленные избирательными комиссиями субъектов РФ; сводные данные, представленные территориальными избирательными комиссиями (ТИК), созданными в субъектах РФ; данные, представленные участковыми избирательными комиссиями (УИК), относящимися к соответствующим ТИК, и ее размещение в виде таблицы (размером 21 столбец на 100757 строк) в текстовом файле формата RFC 4180.

Наличие столь представительной выборки данных позволит оценить адекватность статистических методов, используемых в электоральной криминалистике для выявления фальсификации результатов выборов.

Ключевые слова: *выборы, электоральные данные, избирательная комиссия, веб-страница, веб-скрепинг, анализ данных, информационный поиск.*

Mirvoda S.G., Porshnev S.V., Ryabko N.Yu.

AUTOMATION OF THE PROCEDURE FOR ACCESSING ELECTORAL DATA POSTED ON THE WEBSITE OF THE CENTRAL ELECTION COMMISSION RUSSIAN FEDERATION

The article describes software that automatically loads electoral data on the 2018 presidential elections of the Russian Federation posted on the official website of the central committee of the elections. The data includes summary data for the Russian Federation, summary data provided by the election commissions of the subjects of the Russian Federation, summary data provided by territorial election commissions; the data provided by precinct election commissions. The data is presented in the form of a table (21 columns by 100757 rows) in a text file according to the RFC 4180 format.

Such a representative sample of the election data will allow us to assess the adequacy of statistical methods used in electoral criminology to detect falsification of election results.

Keywords: *election, election data, election commission, webpage, web-scrapping, data retrieval, data mining.*

Введение

Сегодня проблемы, связанные с оценкой достоверности результатов тех или иных выборов в органы власти и местного самоуправления в РФ и выявления возможных фальсификаций электоральных данных, являются предметом острых научных и политических дискуссий, в которых принимают участие политики, политологи, юристы, специалисты по прикладной статистике (электоральные статистики), а также политически активные избиратели) (см., например, [1,2]). При этом, в большинстве случаев, мнения участников дискуссий по обсуждаемой проблеме, в зависимости занимаемой ими политической позиции, оказываются диаметрально противоположными: от полного отрицания каких-либо фальсификаций электоральных данных (например, члены ЦИК и избирательных комиссий нижних уровней), до полного отрицания возможности проведения в РФ честных выборов (например, кандидаты, не получившие поддержки избирателей, а также члены либерально настроенного сообщества электоральных статистиков (см., например, [3]). В, как очевидно, этой ситуации требуется независимая оценка адекватности используемых ими методов и результатов.

При этом основная проблема состоит в отсутствии электоральных данных, полученных по результатам выборов, отсутствие фальсификаций в которых доказана с помощью методов, отличных от методов электоральной статистики (например, на основе данных, представленных независимыми наблюдателями, данных экзит-поллов и т.д.), анализ которых мог бы определить набор «эталонных» статистических характеристик. Однако, выводы об отсутствия фальсификаций электоральных данных, сделанные на основе использования косвенных методов, также могут быть поставлены под сомнение. В этой ситуации представляется целесообразным обратиться к электоральным данным, полученным в ходе выборов, в которых преимущество одного из кандидатов над другими кандидатами было столь велико, что его победа очевидна. Таковыми были выборы Президента РФ в 2018 г., электоральные данные которых размещены на сайте ЦИК РФ [4], на котором, однако, не предусмотрена возможность автоматической выгрузки всех или части электоральных данных в виде, пригодном для последующего анализа. В этой связи извлечение электоральных данных оказывается возможным только в ручном режиме, что весьма трудоемко, так как по данным ЦИК число избирательных участков на этих выборах превысило 97 тысяч.

В статье описана разработанная авторами технология, обеспечивающая автоматическую выгрузку электоральных данных о результатах выборов Президента РФ в 2018 г.

2. Структура электоральных данных о результатах выборов Президента РФ в 2018 г.

Напомним, что система избирательных комиссий по выборам Президента РФ в 2018 имела следующую иерархическую структуру: ЦИК, избирательные комиссии (ИК) субъектов РФ, территориальные ИК, участковые ИК. Всего в 2018 г. было сформировано: 85 ИК субъектов РФ 85 (в том числе, ИК «Территория за пределами РФ», к которой были отнесены 394 УИК, сформированные за пределами РФ, а также ИК г. Байконур (Республика Казахстан), на территории которого были сформированы 7 участковых ИК), 3177 территориальных ИК, 97314 участковых ИК.

Итоговые электоральные данные, находящиеся в свободном доступе, размещены на сайте ЦИК РФ [5]. Эти данные имеют иерархическую структуру: вершина дерева – данные ЦИК (сводные электоральные данные по всей РФ), ветви первого уровня – данные ИК субъектов РФ (сводные электоральные данные по соответствующему субъекту РФ), ветви второго уровня – данные территориальных ИК (сводные данные по территориальным ИК соответствующих субъектов РФ, ветви третьего уровня – данные участковых ИК. Информационные модели электоральных данных, размещаемых на вершине, а также первом и втором уровнях описанной выше иерархической структуры, одинаковы. Они имеют следующую структуру полей:

1. Название ИК.

2. Число избирательных комиссий на следующем уровне иерархии.

3. Число избирательных комиссий, приступивших к передаче информации.

4. Дата и время подписания протокола соответствующей ИК.

5. Число избирателей, включенных в список избирателей.

6. Число избирательных бюллетеней, полученных участковой избирательной комиссией.

7. Число избирательных бюллетеней, выданных избирателям, проголосовавшим досрочно.

8. Число избирательных бюллетеней, выданных в помещении для голосования в день голосования.

9. Число избирательных бюллетеней, выданных вне помещения для голосования в день голосования

10. Число погашенных избирательных бюллетеней.

11. Число избирательных бюллетеней в переносных ящиках для голосования.

12. Число бюллетеней в стационарных ящиках для голосования.

13. Число недействительных избирательных бюллетеней.

14. Число действительных избирательных бюллетеней

15. Число утраченных избирательных бюллетеней

16. Число избирательных бюллетеней, не учтенных при получении.

17. Число избирательных бюллетеней, поданных за Бабурина Сергея Николаевича.

18. Число избирательных бюллетеней, поданных за Грудинина Павла Николаевича.

19. Число избирательных бюллетеней, поданных за Жириновского Владимира Вольфовича.

20. Число избирательных бюллетеней, поданных за Путина Владимира Владимировича.

21. Число избирательных бюллетеней, поданных за Собчак Ксению Анатольевну.

22. Число избирательных бюллетеней, поданных за Сурайкина Максима Александровича.

23. Число избирательных бюллетеней, поданных за Титова Бориса Юрьевича.

24. Число избирательных бюллетеней, поданных за Явлинского Григория Алексеевича.

В информационной модели структуры электоральных данных на третьем уровне иерархии отсутствует поле № 2. Для отображения электоральных данных используются древовидно организованные html-страницы. Пример фрагмента отображения электоральных данных на html-странице, предоставленных ЦИК ИК Республики Адыгея, представлен на рисунке 1.

Отметим, что сайт ЦИК [4] не предоставляет заинтересованным пользователям возможностей для

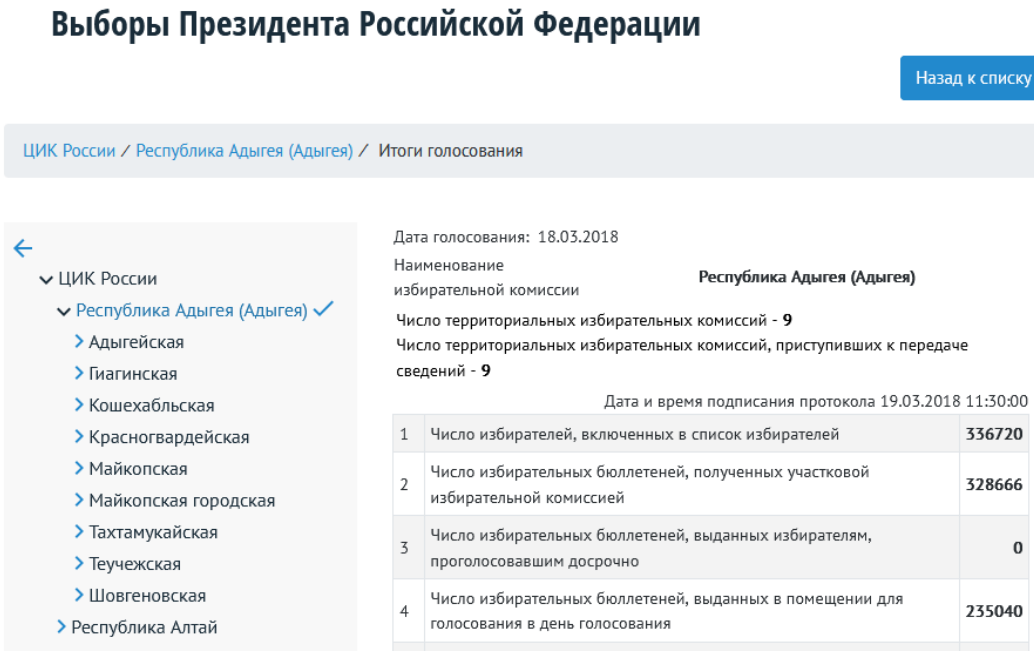


Рис. 1. Фрагмент html-страницы

выгрузки всех или части данных в пригодном для дальнейшего анализа виде. В этих условиях извлечь требующиеся электоральные данные оказывается возможным только в ручном режиме, открывая соответствующие html-страницы сайта ЦИК, выделяя электоральные данные на открытой странице и далее экспортируя их через буфер обмена в тот или иной файл. Для экспорта всех электоральных данных, размещенных на сайте ЦИК, потребуется открыть более 97 тысяч html-страниц и далее выполнить описанную выше последовательность действий, что потребует значительных временных затрат. Кроме того, в ходе экспорта электоральных данных, размещенных на сайте ЦИК, вручную, нельзя исключить внесения в них случайных ошибок, а потому потребуется последующая проверка экспортированных данных, автоматизация которой является самостоятельной нетривиальной задачей. В этой связи авторами был разработан программный инструмент, обеспечивший автоматизированную выгрузку электоральных данных о результатах выборов Президента РФ в 2018 г., представленных ИК различных уровней, с сайта ЦИК [4].

3. Технология экспорта электоральных данных о результатах выборов Президента РФ в 2018 г. с сайта ЦИК

В связи с тем, что доступ к электоральным данным, размещенным на сайте ЦИК [4], как в ручном, так и автоматическом режимах, можно получить либо в процессе обхода всего сайта по заранее заданному алгоритму, либо открывая ссылки, найденные внутри html-страниц, было принято решение использовать технологию веб-скрапинга (англ. – scraping) или сайт-скрапинг [5].

Отметим, что разрабатываемый программный инструмент, основанный на выбранной технологии, кроме собственно подключения к удалённому серверу, получения и анализа текста html-страницы должен обеспечивать:

• управление нагрузкой и пропускной способностью с целью обеспечения частоты автоматически

выполняемых запросов максимально близкой к частоте запросов, отправляемых обычным пользователем, чтобы на удалённом сервере не включились механизмы ограничения пропускной способности, известные как троттлинг или дросселирование [6], а также не произошла блокировка запросов с данного IP адреса;

• при получении ошибок сервера автоматическую повторную отправку и обработку запросов;

• возможность работы длительный срок без утечек памяти при работе со строками;

• поддержку различных механизмов выборки данных, извлекаемых из запрошенных страниц.

Для реализации разрабатываемого программного инструмента для автоматического излечения электоральных данных, размещенных на сайте ЦИК [4], был выбран один из наиболее на популярном на сегодняшний день инструментарий Scrapy (набор утилит и базовых классов), используемый для извлечения данных из веб-страниц, написанный на языке Python [7]. Инструментарий Scrapy, имеющий асинхронную конвейерную архитектуру, представленную на рисунке 2, позволяет обрабатывать необходимое количество запросов, не перегружая при этом удалённый сервер и не предъявляя существенных требований для клиентского места.

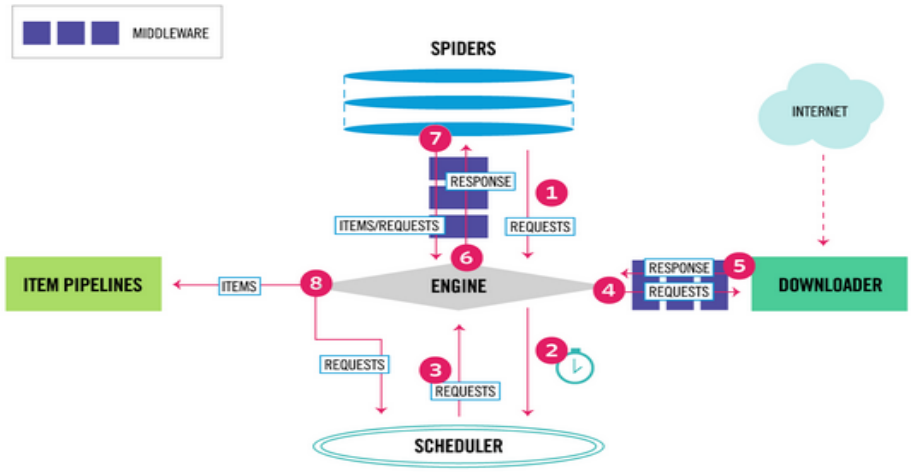


Рис. 2. Архитектура Scrapy [7]: Middleware(response/request/spiders) – пользовательский код осуществляющий обработку данных, engine/item pipelines/scheduler – механизмы распределения нагрузки, downloader – механизм загрузки данных по протоколу http

Из рисунка 2 видно, что архитектура инструментария Scrapy удовлетворяет требованиям к искомому инструменту и обеспечивает базовый набор функциональности.

Единицей функциональности в инструментарии Scrapy является объект Spider – некоторая часть кода (класс), унаследованного от базового класса, в котором пользователь должен реализовать 2 механизма:

1. механизм поиска и обхода ссылок;

2. механизм извлечения данных.

Запросы из Spider поступают в механизм обработки и с помощью планировщика управляемым способом скачивают данные из внешних источников и передают обратно на обработку.

Обработка загруженных данных, представленных в виде объекта в оперативной памяти, выполняется при помощи механизма селекторов [8]. Доступны два вида селекторов:

1. CSS-селекторы, реализуемые на языке CSS селекторов [9];

2. XPath-селекторы, реализуемые на языке XML Path [10]

Рассмотрим алгоритм работы сайта:

1. По нажатию на элемент дерева, происходит запрос на сервер по ссылке http://www.vybory.izbirkom.ru/region/izbirkom?action=show&root=1&tvd=100100084849067&vrn=100100084849062&prver=0&region=1&sub_region= 1&type=226, содержащей идентификаторы выбранного в дереве элемента.

2. После получения страницы браузером, в правой части экрана отображается таблица с данными, представленными при помощи html-атрибута <table> (рис. 1).

3. При разворачивании узла дерева на сервер уходит Ajax-запрос для получения дочерних элементов. Адреса всех запросов для получения дочерних элементов задаются в соответствии со следующим шаблоном: {root}/region/izbirkom?action=tvdTree&tvd children=true&vrn={vrn}&tvd={tvd}, где

1. root - http://www.vybory.izbirkom.ru

2. vrn и tvd идентификаторы из ссылки на текущую страницу

Таким образом, алгоритм получения данных, записанный на псевдоязыке, реализуется выполнением следующей последовательности действий:

1. Начинаем со первой страницы.

2. Извлекаем из страницы коды vrn и tvd.

3. На основе этих кодов формируем URL для получения данных дерева.

4. Из полученных JSON данных (см. рисунок 3) извлекаем ссылки на страницы нижних уровней.

5. Создаём объект scrapy.Request для загрузки данных по полученному URL.

6. При получении данных ищем в них при помощи XPath-запроса //table[@class='table-bordered table-striped table-sm']/tr таблицу с данными и извлекаем их в словарь проиндексированный идентификаторами строк таблицы.

Далее на языке Python была разработана программная реализация вышеуказанного псевдоалго-


```
{
    "id": 100100084849066,
    "text": "ЦИК России",
    "href": "region/izbirkom?action=show&root=0&tvd=100100084849066&vrn=100100084849062&prver=0
    "prver": "0",
    "isUik": false,
    "selected": true,
    "load_on_demand": false,
    "children": [{
            "id": 100100084849067,
            "text": "Республика Адыгея (Адыгея)",
            "href": "region/izbirkom?action=show&root=1&tvd=100100084849067&vrn=100100084849062
            "prver": "0",
            "isUik": false,
            "selected": false,
            "load_on_demand": true,
            "children": []
        }, {
            "id": 100100084849068,
            "text": "Республика Алтай",
            "href": "region/izbirkom?action=show&root=1&tvd=100100084849068&vrn=100100084849062
            "prver": "0",
            "isUik": false,
            "selected": false,
            "load_on_demand": true,
            "children": []
        }, {
            "id": 100100084849069,
            "text": "Республика Башкортостан",
            "href": "region/izbirkom?action=show&root=1&tvd=100100084849069&vrn=100100084849062
```


Рис. 3. Фрагмент представление дочерних элементов в виде JSON

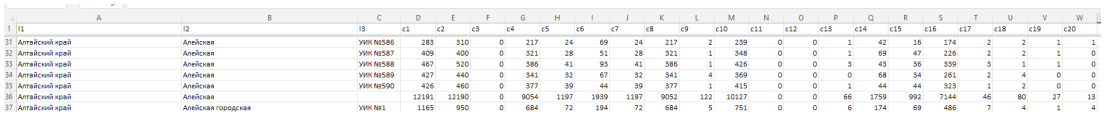
Таблица 1

Описание данных

Наименование колонки	Тип данных	Описание
I1	Строка	наименование ИК субъекта РФ
I2	Строка	Наименование территориальной ИК субъекта РФ
I3	Строка	Наименование участковой ИК 3 уровня, сформированной территориальной ИК субъекта РФ
c1	Целое число	Число избирателей, включенных в список избирателей
c2	Целое число	Число избирательных бюллетеней, полученных участковой избирательной комиссией
c3	Целое число	Число избирательных бюллетеней, выданных избирателям, проголосовавшим досрочно
c4	Целое число	Число избирательных бюллетеней, выданных в помещении для голосования в день голосования
c5	Целое число	Число избирательных бюллетеней, выданных вне помещения для голосования в день голосования
c6	Целое число	Число погашенных избирательных бюллетеней
c7	Целое число	Число избирательных бюллетеней в переносных ящиках для голосования
c8	Целое число	Число бюллетеней в стационарных ящиках для голосования
c9	Целое число	Число недействительных избирательных бюллетеней

Продолжение таблицы 1

Наименование колонки	Тип данных	Описание
c10	Целое число	Число действительных избирательных бюллетеней
c11	Целое число	Число утраченных избирательных бюллетеней
c12	Целое число	Число избирательных бюллетеней, не учтенных при получении
c13	Целое число	Бабурин Сергей Николаевич
c14	Целое число	Грудинин Павел Николаевич
c15	Целое число	Жириновский Владимир Вольфович
c16	Целое число	Путин Владимир Владимирович
c17	Целое число	Собчак Ксения Анатольевна
c18	Целое число	Сурайкин Максим Александрович
c19	Целое число	Титов Борис Юрьевич
c20	Целое число	Явлинский Григорий Алексеевич



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	l1	l2	l3	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	c12	c13	c14	c15	c16	c17	c18	c19	c20
31	Алтайский край	Алейская	УИК №586	283	310	0	217	24	69	24	217	2	239	0	0	1	42	16	174	2	2	1	1
32	Алтайский край	Алейская	УИК №587	409	400	0	321	28	51	28	321	1	348	0	0	1	69	47	226	2	2	1	0
33	Алтайский край	Алейская	УИК №588	467	520	0	386	41	93	41	386	1	426	0	0	3	43	36	339	3	1	1	0
34	Алтайский край	Алейская	УИК №589	427	440	0	341	32	67	32	341	4	369	0	0	0	68	34	261	2	4	0	0
35	Алтайский край	Алейская	УИК №590	426	460	0	377	39	44	39	377	1	415	0	0	1	44	44	323	1	2	0	0
36	Алтайский край	Алейская		12191	12190	0	9054	1197	1899	1197	9052	122	10127	0	0	66	1759	992	7144	46	80	27	13
37	Алтайский край	Алейская городская	УИК №1	1165	950	0	684	72	194	72	684	5	751	0	0	6	174	69	486	7	4	1	4

Рис. 4. Фрагмент скриншота Excel с открытым CSV-файлом

ритма, запускаемая с помощью утилиты runspider. Например, так: runspider cik/spiders/data_spider.py.

4. Результатов автоматической выгрузки с сайте ЦИК результатов выборов Президента РФ в 2018 г.

Для автоматической выгрузки электоральных данных, представленных ИК после выборов Президента РФ в 2018 г., с сайта ЦИК [4] был использован обычный офисный компьютер (AMD Ryzen 5 4 ГГц, 32 Гб ОЗУ, Интернет со скоростью 50Мб/с. На выгрузку данных потребовалось 8 часов, в течение которых было выполнено 201156 http-запросов и скачано около 10 ГБ сырых данных. Далее из первичных («сырых») данных извлечено 11Мб полезных данных, которые были сохранены в CSV-файл (в формате RFC 4180) со следующей структурой (таблица 1).

Фрагмент скриншот программы Excel с открытым файлом, содержащим результаты выгрузки электоральных данных, представленных ИК после выборов Президента РФ в 2018 г., подтверждающий работоспособность разработанного программного инструмента приведен на рисунке 4. Данный файл содержит 100577 строк.

Для верификации результатов выгрузки электоральных данных, представленных ИК после выборов Президента РФ в 2018 г., выгружаемые данные также в текстовом файле, объемом 392 МБ. Результаты выборочного сравнения соответствующих данных в CSV и текстовом файлах показали их идентичность.

Заключение

Разработан программный инструмент и реализована автоматическая выгрузка электоральных данных о выборах в 2018 г. Президента Российской Федерации (РФ), размещенных на официальном сайте ЦИК, включая: сводные данные по РФ; сводные данные, представленные избирательными комиссиями субъектов РФ; сводные данные, представленные территориальными избирательными комиссиями (ТИК), созданными в субъектах РФ; данные, представленные участковыми избирательными комиссиями (УИК), относящимися к соответствующим ТИК, и ее размещение в виде таблицы (размером 21 столбец на 100757 строк) в файле формата CSV.

Далее электоральные данные о выборах Президента РФ в 2018 г. Будут использованы для оценки адекватности статистических методов, используемых в электоральной криминалистике для выявления фальсификации результатов выборов.

Литература

1. Доклад Российского общественного института избирательного права (РОИИП) «Математические инструменты делигитимации выборов»//И.Б. Борисов, И.В Задорин, А.В. Игнатов, В.Н. Марачевский, В.И. Федоров/ –М.: РОИИП, 2020. 76 с. URL: http://www.roiip.ru/images/data/gallery/0_299_Matematicheskie_instrumenti_delegitimatsii_viborov.pdf (дата обращения 19.02.2022).

2. Шень А. Как доклад РОИИП делегитимирует выборы. URL: https://trv-science.ru/2020/09/kak-doklad-roiip-delegitimiruet-vybory/ (дата обращения 19.02.2022).

3. URL:http://electoralpolitics.org/ru/articles/vozmozhnosti-matematicheskikh-metodov-po-vyiavleniiu-elektoralnykh-falsifikatsii/

4. (дата обращения 19.02.2022).

5. URL: http://www.vybory.izbirkom.ru (дата обращения 19.02.2022).

6. Райн М. Скрапинг веб-сайтов с помощью Python. –М.: ДМК Пресс, 2016. 280 с.

7. URL: https://www.nginx.com/blog/rate-limiting-nginx/

8. URL: https://scrapy.org/ (дата обращения 19.02.2022).

9. URL: https://docs.scrapy.org/en/latest/topics/selectors.html (дата обращения 19.02.2022).

10. URL: https://developer.mozilla.org/ru/docs/Web/CSS/CSS_Selectors (дата обращения 19.02.2022).

11. URL: https://www.w3.org/TR/xpath/all/ (дата обращения 19.02.2022).

References

1. Doklad Rossiyskogo obshchestvennogo instituta izbiratel'nogo prava (ROIIP) «Matematicheskiye instrumenty deligitimatsii vyborov»//I.B. Borisov, I.V Zadorin, A.V. Ignatov, V.N. Marachevskiy, V.I. Fedorov/ –M.: ROIIP, 2020. 76 s. URL: http://www.roiip.ru/images/data/gallery/0_299_Matematicheskie_instrumenti_delegitimatsii_viborov.pdf (data obrashcheniya 19.02.2022).

2. Shen' A. Kak doklad ROIIP delegitimiruyet vybory. URL: https://trv-science.ru/2020/09/kak-doklad-roiip-delegitimiruet-vybory/ (data obrashcheniya 19.02.2022).

3. URL: http://electoralpolitics.org/ru/articles/vozmozhnosti-matematicheskikh-metodov-po-vyiavleniiu-elektoralnykh-falsifikatsii/ (data obrashcheniya 19.02.2022).

4. URL: http://www.vybory.izbirkom.ru (data obrashcheniya 19.02.2022).

5. Rayn M. Skraping veb-saytov s pomoshch'yu Python. –M.: DMK Press, 2016. 280 s.

6. URL: https://www.nginx.com/blog/rate-limiting-nginx/

7. URL: https://scrapy.org/ (data obrashcheniya 19.02.2022).

8. URL: https://docs.scrapy.org/en/latest/topics/selectors.html (data obrashcheniya 19.02.2022).

9. URL: https://developer.mozilla.org/ru/docs/Web/CSS/CSS_Selectors (data obrashcheniya 19.02.2022).

10. URL: https://www.w3.org/TR/xpath/all/ (data obrashcheniya 19.02.2022)

МИРВОДА Сергей Геннадьевич, заместитель генерального директора по технологиям ООО «Октоника». 620014, г. Екатеринбург ул. 8 марта 2. E-mail: sergey@mirvoda.com

MIRVODA Sergey Gennadievch, CTO, Octonica LLL, 8th March St., 2. 620014, Yekaterinburg, Russia. E-mail: sergey@mirvoda.com

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: s.v.porshnev@urfu.ru

РЯБКО Николай Юрьевич, аспирант федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: N. Yu.Ryabko@urfu.ru

RYABKO Nikolay Yurievich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "Ural Federal University named after the first President of Russia B.N. Yeltsin". 620002, Yekaterinburg, st. Mira, 32. E-mail: N.Yu.Ryabko@urfu.ru

УДК 004.414.23 + 519.711.2 Вестник УрФО № 1(43) / 2022, с. 35–42

Шамонин Е. Д.

DOI: 10.14529/secur220105

МОДЕЛИРОВАНИЕ ДИСКОВОЙ ПОДСИСТЕМЫ ЭВМ НА ОСНОВЕ НАКОПИТЕЛЯ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ В РЕЖИМЕ ЧТЕНИЯ

Одним из основных направлений использования современных вычислительных систем является хранение данных.

Основными устройствами хранения цифровой информации являются накопители на жестких магнитных дисках — НЖМД (Hard Disk Drive, HDD).

В криминалистической практике применительно к машинным носителям информации (МНИ) решаются две основные задачи. Это либо копирование содержимого носителя (полное посекторное или выборочное) с последующим исследованием копии на предмет наличия криминалистически значимой информации, либо поиск какой-либо конкретной информации (контекстный поиск) непосредственно на целевом машинном носителе информации (МНИ) с возможным последующим ее копированием.

Таким образом, как в первом, так и во втором случае основным режимом работы целевого МНИ будет чтение.

Моделирование функционирования жесткого магнитного диска в режиме чтения на основе информации о модели накопителя (а, следовательно, и спецификации устройства) позволит оценить время, необходимое для получения полной копии содержимого НЖМД.

В ходе исследования на основании уточненной математической модели были получены результаты весьма близкие к тем, которые были получены при копировании содержимого накопителей на практике. Однако реальное время копирования содержимого целевого накопителя в значительной мере зависит от его технического состояния. Наличие областей на магнитном диске, не позволяющих при первом проходе блока магнитных головок получить ожидаемый результат, требует дополнительных обращений к этим участкам магнитного диска и, как следствие, дополнительным временным затратам.

Ключевые слова: *моделирование, дисковая подсистема, время поиска, время перехода, файловая система.*

Shamonin E. D.

SIMULATION OF A COMPUTER DISK SUBSYSTEM BASED ON A HARD DISK DRIVE IN READ MODE

One of the main options for using modern computing systems is data storage.

The main devices for storing digital information are hard disk drives.

In forensic practice in relation to media type, two main tasks are solved. This is either media content copying (full sector-by-sector or selective) with subsequent examination of the copy for forensic information presence, or searching for any specific information (context search) directly on the target media with possible subsequent copying.

Thus, both in the first and in the second case, the main mode of target media operation is reading.

In the course of the study, based on a refined mathematical model, results were obtained very close to those obtained when copying the contents of storage devices in practice. However, the actual time of copying the contents of the target drive largely depends on its technical condition. The presence of areas on the magnetic disk that do not allow the expected result to be obtained during the first pass of the magnetic head unit requires additional access to these areas of the magnetic disk and, as a result, additional time costs.

Keywords: *modeling, disk subsystem, average seek time, seek time track-to-track, file system.*

При считывании данных с НЖМД цепь прохождения считанных данных (рис. 1) будет включать как элементы механической подсистемы (гермоблока), так и платы электроники (контроллера).

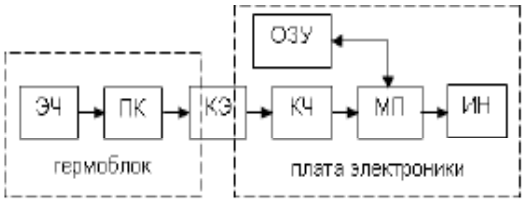


Рис. 1. Цепь прохождения считанных данных в НЖМД

На рис. 1: ЭЧ — элемент чтения; ПК — предусилитель-коммутатор; КЭ — контактные элементы; КЧ — канал чтения; МП — микропроцессор; ОЗУ — оперативное запоминающее устройство; ИН — интерфейс накопителя.

Основные временные затраты приходятся на механическую часть НЖМД, т. к. если необходимо записать или прочитать какие-либо данные, блок магнитных головок (БМГ) перемещается на требуемый цилиндр (дорожку) и ожидает поворота диска до требуемого участка дорожки. В каждый конкретный момент времени с помощью предусилителя-коммутатора в HDD выбирается один из элементов (чтения или записи) одной магнитной головки. Параллельное выполнение операций чтения/записи либо чтения по двум и более головкам невозможно.

Данные на долговременных носителях обрабатываются блоками (порциями). То есть если на носитель требуется записать лишь один байт или даже один бит, под новый файл будет сразу выделена некоторая фиксированная порция дискового пространства. Соответственно, продолжительность операции с целым блоком или с одним из байтов этого блока будет одинаковой.

На минимальные порции данные делятся на двух уровнях: на уровне физического носителя минимальная порция данных — сектор в 512 байтов. На уровне файловой системы минимальной порцией данных является кластер, который объединяет в себе несколько соседних секторов. Стандартным в настоящее время является кластер объемом 4 096 байт. Он включает восемь последовательно идущих друг за другом секторов по 512 байт. При перефор-матировании, если это необходимо, объем кластера можно изменять как в большую, так и меньшую сторону.

Сектора требуются для оптимизации работы аппаратной части носителя данных. Кластеры нужны для оптимизации работы файловой системы.

Операционная система и приложения работают не с абстрактными блоками данных, а с прикладными файлами. Для того, чтобы получить тот или иной файл, сначала нужно узнать, в каких блоках он размещен. Сведения об этом хранятся среди данных файловой системы (ФС), которые сами хранятся на диске. Таким образом, для получения данных из файла сначала нужно выполнить ряд вспомогательных дисковых операций, в том числе и для работы со служебной информацией ФС, т. е. на скорость дисковых операций влияют и особенности файловой системы (FAT, NTFS, …).

Кроме того, большие файлы обрабатываются быстрее, чем множество небольших файлов такого же суммарного объема. Ведь во втором случае потребуется большее число обращений к файловой системе [1].

Один из подходов моделирования дисковой подсистемы основан на построении математической модели конкретной файловой системы NTFS [2].

Поскольку NTFS оперирует двумя типами данных, кэшированными (присутствующими в файловом кэше) и не кэшированными (для доступа к которым необходимо обращение к диску), можно говорить о так называемой модели двух хранилищ информации: быстрого (cache) и медленного (disk).

Пусть *C* — множество запросов, при которых данные берутся только из кэша, а *D* — множество запросов, требующих обращения к диску. Нагрузка представляет собой последовательность запросов из множества $C \cup D$, причем для чтения $C \cap D = \varnothing$.

Предположив, что скорость чтения данных из каждого хранилища постоянна и равна v^r_c и v^r_d ($v^r_c > v^r_d$), можно записать время выполнения одного запроса:

$$t^r_c = s^r_c / v^r_c,\ t^r_d = s^r_d / v^r_d,$$

где s^r_c и s^r_d — количество запрашиваемых байт соответственно из кэша и жесткого диска.

Тогда общее время выполнения последовательности запросов чтения равно:

$$T^r = T^r_d + T^r_c = \sum_{req_i \in D} t^r_{di} + \sum_{req_j \in C} t^r_{cj} = 1/v^r_d *$$

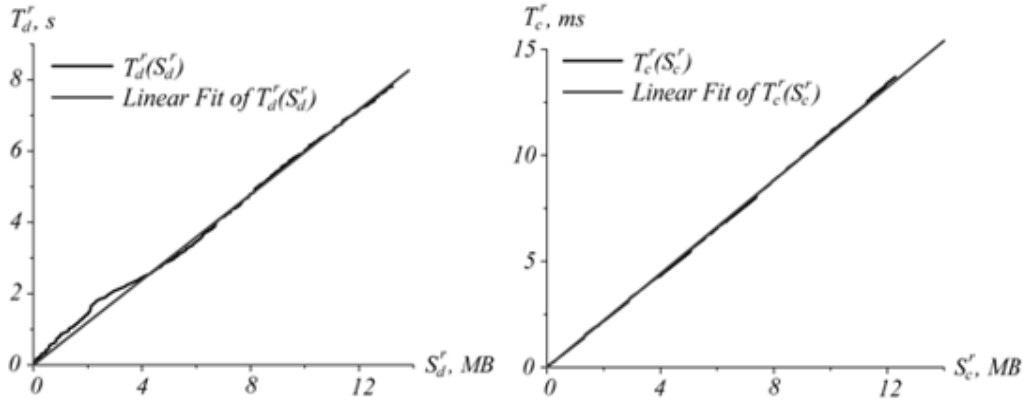
$$* \sum_{req_i \in D} s^r_{di} + 1/v^r_c * \sum_{req_j \in C} s^r_{cj},$$

$$T^r = T^r\left(S^r_d, S^r_c\right) = S^r_d / v^r_d + S^r_c / v^r_c,$$

где S^r_d и S^r_c — общее число байтов, прочитанных за время T^r с пластин жесткого диска и из кэша соответственно.

Гипотеза о линейности функции подтвердилась экспериментально при контекстном поиске данных в выбранной директории (рис. 2) [2], что позво-лило автору вычислить коэффициенты и с помощью линейной аппрокси-мации по методу наименьших квадратов (МНК).

Однако при смене директории поиска значение



а) б)

Рис. 2. Зависимость времени чтения от количества прочитанных данных: а — с диска; б — из кэша

коэффициента v^r_d изменялось, в отличие от величины v^r_c, которая оставалась постоянной во всех опытах. Это позволило заключить, что скорость чтения данных с диска не постоянна, а, возможно, зависит от некоторого дополнительного параметра.

Предположим, что обработка запроса к диску происходит с некоторой задержкой t^r_0, которая вызвана работой механических компонентов устройства:

$$t^r_d = t^r_0 + s^r_c / v^r_c,$$

где t^r_0, v^r_0 = const.

Обозначим через N^r_d общее количество дисковых запросов на чтение. Тогда время выполнения запросов чтения с диска:

$$T^r_d = \sum_{i=1}^{N^r_d} t^r_{di} = N^r_d * t^r_0 + S^r_d / v^r_0,$$

а скорость $v^r_d = S^r_d / T^r_d$, которая вопреки первоначальному предположению оказалась не постоянной, равна:

$$v^r_d\left(\bar{s}^r_d\right) = \frac{\bar{s}^r_d}{t^r_0 + \bar{s}^r_d / v^r_0}, \quad (1)$$

где $\bar{s}^r_d = S^r_d / N^r_d$ — средний размер запросов чтения с диска.

Гипотеза (1) получила экспериментальное подтверждение (коэффициент детерминации для выбранного приближения $R^2 = 0{,}9$). Поэтому время выполнения последовательности запросов чтения есть линейная функция трех переменных:

$$T^r = T^r\left(N^r_d, S^r_d, S^r_c\right) = N^r_d * t^r_0 + S^r_d / v^r_0 + S^r_c / v^r_c. \quad (2)$$

Тестирование NTFS на различных аппаратных конфигурациях позволило сделать ряд важнейших выводов касательно коэффициентов модели (2) [2]:

– величина t^r_0 характеризует степень фрагментации запрашиваемых данных: математическое ожидание t^r_0 совпадает со средним временем поиска по диску (Average Seek Time, AST), обозначаемым производителем в спецификации устройства;

– величина v^r_0 представляет собой скорость передачи данных с пластин диска в его внутренний буфер (Internal Data Transfer Rate, IDTR), которая прямо пропорциональна скорости вращения пластин диска (Revolutions Per Minute, RPM), также указываемой производителем в специ-фикации устройства;

– величину v^r_c можно назвать эффективной скоростью чтения данных из кэша: значение не изменяется при тестировании на машинах с различными характеристиками RAM, хотя оно гораздо меньше предельной скорости чтения данных из памяти, заявляемой производителем.

В системе (3) приведены точные значения коэффициентов, полученные при моделировании с использованием диска SAMSUNG SV4002H [2].

$$\begin{cases} t^r_0 = 9 * 10^{-3}\ \text{с}, \\ 1/v^r_0 = 3 * 10^{-4}\ \text{с/КБ}, \\ 1/v^r_c = 1 * 10^{-6}\ \text{с/КБ}. \end{cases} \quad (3)$$

Коэффициенты t^r_0 и v^r_0 соответствуют физическим характеристикам устройства, указанным в спецификации: среднее время поиска — 8,9 мс, скорость вращения — 5400 RPM (1 / IDTR ≈ $3*10^{-4}$ с/КБ).

На практике время выполнения последовательности запросов меняется от эксперимента к эксперименту при одинаковых условиях тестирования. Значит, характеристику производительности T^r необходимо рас-сматривать как случайную величину, зависящую от неслучайных переменных x^r_i, $i = \overline{1,k}$.

В задаче оценки производительности файловой системы значения x^r_i играют роль переменных параметров нагрузки, входящих в распределение величины T^r, т. е. k=3, $x^r_i = N^r_d$, $x^r_2 = S^r_d$, $x^r_3 = S^r_c$.

Таким образом, достоверность модели (2) можно проверить статистическим методом множественной регрессии:

$$E(T^r) = \beta^r_0 + \sum_{i=1}^{k} \beta^r_i * x^r_i.$$

При помощи критерия согласия Пирсона с уровнем значимости 5% в работе [2] было показано, что при фиксированных параметрах нагрузки T^r есть нормально распределенная случайная величина. Для определения коэффициентов регрессии использовалась выборка из n=14 независимо наблюденных точек (T^r_v, x^r_{1v}, x^r_{2v}, x^r_{3v}), $v = \overline{1,n}$. Каждый элемент выборки был получен в результате последовательного или произвольного чтения файлов из случайной директории. Причем степень фрагментации диска, а также доля кэшированных данных были различными для всех экспериментов.

Выяснилось, что при уровне значимости 5% значимыми являются только коэффициенты β^r_1, β^r_2, причем их значения в точности совпадают с величинами t^r_0, v^r_0, полученными ранее и имеющими конкретный физический смысл. Свободный член β^r_0 оказался не значимым, что подтвердило предыдущие результаты. Отсутствие влияния коэффициента $\beta^r_3 = 1/v^r_c$ можно объяснить небольшой размерностью выборки, а также тем, что чтение данных из кэша вносит сравнительно малый вклад в общее время выполнения последовательности запросов. Тем не менее, из практических соображений не стоит пренебрегать параметром нагрузки x^r_3. В случае, когда большая часть данных кэширована (например, на web-сервере), время чтения будет мало, однако отлично от нуля.

Резюмируя вышесказанное, математическую модель прогнозирования производительности файловой системы NTFS при нагрузке чтения можно записать в виде следующего линейного соотношения [2]:

$$T^r = \beta^r_1 * x^r_1 + \beta^r_2 * x^r_2 + \beta^r_3 * x^r_3, \quad (4)$$

где x^r_i — параметры нагрузки, β^r_i — коэффициенты модели.

Недостатками рассмотренного варианта модели являются следующие позиции:

1. Несмотря на то, что как следует из названия работы [2], построена модель нагрузки файловой системы NTFS при активном поиске данных, первые два коэффициента модели напрямую имеют отношение к физическим характеристикам НЖМД и только третий коэффициент, обратно пропорцио-нальный скорости чтения из кэша, косвенно указывает на использование файловой системы NTFS.

2. Если обратиться к рис. 1, то видно, что представленная модель учитывает временные задержки только механической подсистемы НЖМД, в то время как тракт прохождения считанных данных включает и электронные компоненты, размещенных как в гермоблоке, так и на плате электроники. Часть этих временных затрат учитывается вторым коэффициентом модели, а именно скоростью передачи данных с пластин диска в его внутренний буфер.

Поскольку гипотеза о линейности функции была доказана теоретически и подтвердилась экспериментально, то модель производительности НЖМД можно уточнить вводом дополнительного слагаемого:

$$T^r = \beta^r_1 * x^r_1 + \beta^r_2 * x^r_2 + \beta^r_3 * x^r_3 + \sum_{i=1}^{n} t_i, \quad (5)$$

где t_i — временная задержка, вносимая i-м электронным компонентом, $i = \overline{1,n}$, n — количество электронных компонентов, через которые проходят считанные данные.

Если на старых моделях жестких дисков каждому элементу на плате электроники соответствовала своя интегральная микросхема (ИМС), то более современные версии плат электроники строятся на двух-трех микросхемах: ИМС SOC (System On Chip, SOC), в состав которой входит микропроцессор, канал записи/чтения, опционально постоянное запоминающее устройство (ПЗУ). Отдельно могут быть представлены ИМС оперативного запоминающего устройства (ОЗУ), ИМС ПЗУ и ИМС управления шпиндельным двигателем и звуковой катушкой.

К сожалению, производители ИМС достаточно часто их характеристики не разглашают. Так компания Marvell, основной поставщик ИМС SOC для HDD компании Western Digital и некоторых других компаний, вообще не поставляет ни какой информации по этим микросхемам, поскольку значительная их часть задействована в процедурах аппаратного шифрования.

Данные пользователя перед записью на магнитные диски (МД), подвергаются ряду преобразований (рис. 3) [3].

При считывании кодированных таким образом данных происходит процесс декодирования, который также занимает какое-то время. Поскольку в большинстве случаев задержки, вносимые электронными компонентами, напрямую оценить нельзя в виду отсутствия на ИМС внятной документации, попробуем оценить их косвенно.

Рис. 3. Процесс кодирования данных перед записью на МД

В состав комплекса PC-3000, кроме технологических утилит, входит универсальная утилита, позволяющая осуществлять ряд текстов в различных режимах работы НЖМД.

НЖМД, который использовался в качестве тестируемого (SAMSUNG SV4002H) в работе [2], найти не удалось.

Наиболее близкий по характеристикам диск SAMSUNG HM121HC имеет другой форм-фактор (2,5 дюйма против 3,5), втрое больший объем (120 ГБ против 40), но ту же скорость вращения пластин — 5400 об/мин. Причем форм-фактор напрямую повлиял на скоростные характеристики системы позиционирования БМГ. Предположительно вследствие значительно меньших размеров постоянных магнитов и, значит, меньшей «мощности» магнитной системы, среднее время поиска возросло до 12,0 мс против 8,9 мс (в данном случае еще возможно и влияние объема МНИ). Другая характеристика — время перехода с дорожки на соседнюю дорожку — также увеличилась с 0,8 до 2,0 мс. Внутренняя скорость передачи данных диска SAM-SUNG HM121HC — 826 Мбит/с.

Комплексный тест универсальной утилиты, входящей в состав PC-3000, позволяет тестировать накопитель в режиме верификации, при котором осуществляется проверка только возможности считывания содержимого поверхности магнитных дисков без дальнейшей обработки содержимого секторов.

Перед тестированием накопителя было осуществлено зануление содержимого секторов, форматирование в файловой системе NTFS и заполнение всего объема жесткого диска файлами различного формата и длины.

Тестирование НЖМД в режиме верификации было осуществлено за 40 мин 17 с. Полное посекторное копирование диска SAMSUNG HM121HC с использованием комплекса PC-3000 и программы Data Extractor осуществлялось в течение 40 мин 46 с. Таким образом, разница между обработкой считанных данных только механической подсистемой и той же подсистемой вместе с электронными компонентами составляет 29 с.

Несмотря на то, что комплекс PC-3000 разворачивается «поверх» ОС Windows, работа комплекса с НЖМД осуществляется на аппаратном уровне. Считывание данных по умолчанию (независимо от режима) осуществляется блоками по 256 секторов. Следовательно, количество запросов на чтение всех блоков составляет x^r_1 = 234 441 648 / 256 = 915 788.

Поскольку при посекторном копировании чтение секторов осуществляется последовательно, начиная с нулевого цилиндра с постепенным продвижением к максимальному, первый коэффициент, а именно среднее время поиска, заменяем на время перехода с дорожки на соседнюю дорожку (с цилиндра на цилиндр), т. е. β^r_1 = 2 мс = 0,002 с. Внутренняя скорость передачи данных НЖМД составляет 826 Мбит/с или 826/8 = 103,25 МБ/с, т. е. значение второго коэффициента в формуле (5) равно β^r_2 = 1/103,25 = 0,0097 с/МБ. Поскольку снимается полная посекторная копия, то количество считанных данных составит x^r_2 = (234 441 648*512)/1024/1024 = 114 473,46 МБ.

Так как файловый хэш при чтении с НЖМД практически не задейство-ван [1], то третье слагаемое в (5) опускаем.

Таким образом, расчетное время получения полной копии:

$$T^r = \beta^r_1 * x^r_1 + \beta^r_2 * x^r_2 + \sum_{i=1}^{n} t_i = 0{,}002 * 915\,788 +$$

+ 0,0097 * 114 473,46 + 29 = 1831,576 + 1110,388 + 29 = = 2 970,964 с = 49,51 мин = 49 мин 30 с.

Полученное расчетное значение значительно превышает то, которое было получено в процессе снятия копии с использованием PC-3000. При этом в качестве времени перехода с дорожки на дорожку было взято время Seek Time Minimum (рис. 4) [4]. К сожалению, в спецификации на устройство, такая характеристика, как время перехода с дорожки на дорожку (Seek Time Track-to-Track, STTT), отсутствует. Так как время поиска включает в себя время успокоения головок и время ожидания момента, когда требуемый сектор окажется под магнитной головкой, можно предположить, что время перехода с дорожки на соседнюю дорожку меньше 2 мс.

Анализ различных источников указывает, что время перехода с дорожки на дорожку для НЖМД разных производителей лежит в пределах от 0,5 до 1,5 мс [5]. Если взять максимальное значение 1,5 мс и подставить его в выражение (5), то получим:

$$T^r = \beta^r_1 x^r_1 + \beta^r_2 x^r_2 + \sum_{i=1}^{n} t_i = 0{,}0015 * 915\,788 +$$

+ 0,0097 * 114 473,46 + 29 = 1 373,682 + 1110,388 + 29 = = 2 513,07 с = 41,88 мин = 41 мин 53 с.

Полное посекторное копирование диска SAMSUNG HM121HC с использованием комплекса PC-3000 и программы Data Extractor осуществлялось в течение 40 мин 46 с, т. е. разница составляет чуть более минуты, а именно 1 мин 07 с.

Для того, чтобы проверить, насколько адекватной является полученная модель производительно-

1-1. Functional Specification

		HM061GC	HM080GC	HM121HC	HM160HC
Storage Capacity	Formatted *1	60GB	80GB	120GB	160GB
Sector Length		512 Bytes			
Rotational Speed		5400 RPM ± 0.5%			
Seek Time	Minimum	2 ms			
	Average	12 ms			
	Maximum	22 ms			
Dimensions		69.85mm×100mm×9.5mm			
Weight		below 96g			
Data Transfer Rate		100MB / s (Max.)			
Buffer Size		8MB			
Mean Time Between Failure		MTBF(POH) 600,000 hours			

Рис. 4. Основные характеристики дисков SpinPoint M5P Series

сти дисковой подсистемы, были протестированы еще два накопителя такой же емкости, а именно HITACHI HTS543212L9A300 и FUJITSU MHW2120BH.

Оба накопителя имеют интерфейс SATA, скорость вращения пластин 5400 об/мин, но различные характеристики по внутреннему обмену данными и времени перехода с дорожки на дорожку. Перед тестированием оба накопителя были подготовлены аналогично НЖМД SAMSUNG, т. е. содержимое секторов было заполнено нулями, произведено форматирование в файловой системе NTFS, и на накопителях были размещены те же данные, что и ранее на диске SAMSUNG.

Для накопителя HITACHI HTS543212L9A300 время перехода с дорожки на дорожку 1,0 мс (β^r_1 = 0,001 с), внутренняя скорость передачи данных 674 Мбит/с = 84,25 МБ/с (β^r_2 = 1/84, 25 = 0,012 с/МБ), верификация осуществлена за 41 мин 49 с, а посекторное копирование за 42 мин 31 с.

$$T^r = \beta_1^r x_1^r + \beta_2^r x_2^r + \sum_{i=1}^{n} t_i = 0{,}001 * 915\ 788 +$$

+ 0,012 * 114 473,46 + 42 = 915,788 + 1 373,68 + + 42 = 2 331,468 с = 38,86 мин = 38 мин 52 с.

Для накопителя FUJTSU MHW2120BH время перехода с дорожки на дорожку 1,5 мс (β^r_1 = 0,001 с), внутренняя скорость передачи данных 490,4 Мбит/с = 61,3 МБ/с (β^r_2 = 1/61, 3 = 0,016 с/МБ), верификация осуществлена за 1 ч 01 мин 20 с, а посекторное копирование за 1 ч 02 мин 06 с.

$$T^r = \beta_1^r x_1^r + \beta_2^r x_2^r + \sum_{i=1}^{n} t_i = 0{,}0015 * 915\ 788 +$$

+ 0,016 * 114 473,46 + 46 = 1 373,682 + 1 867,43 + + 46 = 3 287,112 с = 54,78 мин = 54 мин 47 с.

Для наглядности исходные данные и полученные результаты сведены в таблицу (табл. 1).

Необходимо отметить, что данные, полученные на основании практических тестов, являются усредненными в виду того, что даже при проведении тестов на одном и том же компьютере в одной и той же конфигурации вследствие наличия нестабильных секторов могут достаточно значительно отличаться (до единиц и даже десятков секунд). При наличии подобного рода секторов микропроцессор предпринимает несколько попыток вычитать их содержимое, изменяя величину тока головки, смещая положение головки относительно центра дорожки в ту и другую сторону. Естественно, что каждая последующая попытка вычитать содержимое сектора требует полного оборота магнитных пластин для того, чтобы целевой сектор вновь начал взаимодействовать с элементом чтения.

Выводы

1. Имея информацию о модели целевого накопителя можно предварительно оценить потребное время на получение его полной посекторной копии с использованием скорректированной модели производительности дисковой подсистемы (5).

2. Учет временных затрат на обработку секторов электронными компонентами не привносит сколько-нибудь значительных корректив в конечный результат расчетов, в то время как незначительное изменение технических параметров механической подсистемы может оказать весьма серьезное влияние на конечный результат. Так, изменение времени перехода с дорожки на дорожку с 2,0 мс на 1,5 мс диска

Таблица 1.

Характеристики НЖМД

Характеристика\ НЖМД	SAMSUNG	HITACHI	FUJITSU
Модель	HM121HC	HTS543212L9A300	MHW2120BH
Емкость, Гбайт	120	120	120
Скорость вращения, об/мин	5400	5400	5400
Интерфейс	PATA	SATA	SATA
Internal Data Transfer Rate, МБ/с	103,25	84,25	61,3
Seek Time Track-to-Track, мс	1,5	1,0	1,5
Расчетное время копирования, мин	41,88	38,86	54,78
Практическое время копирования, мин	40,77	42,52	62,1
Разница между расчет-ным и практическим временами, мин	+1,11	-	-

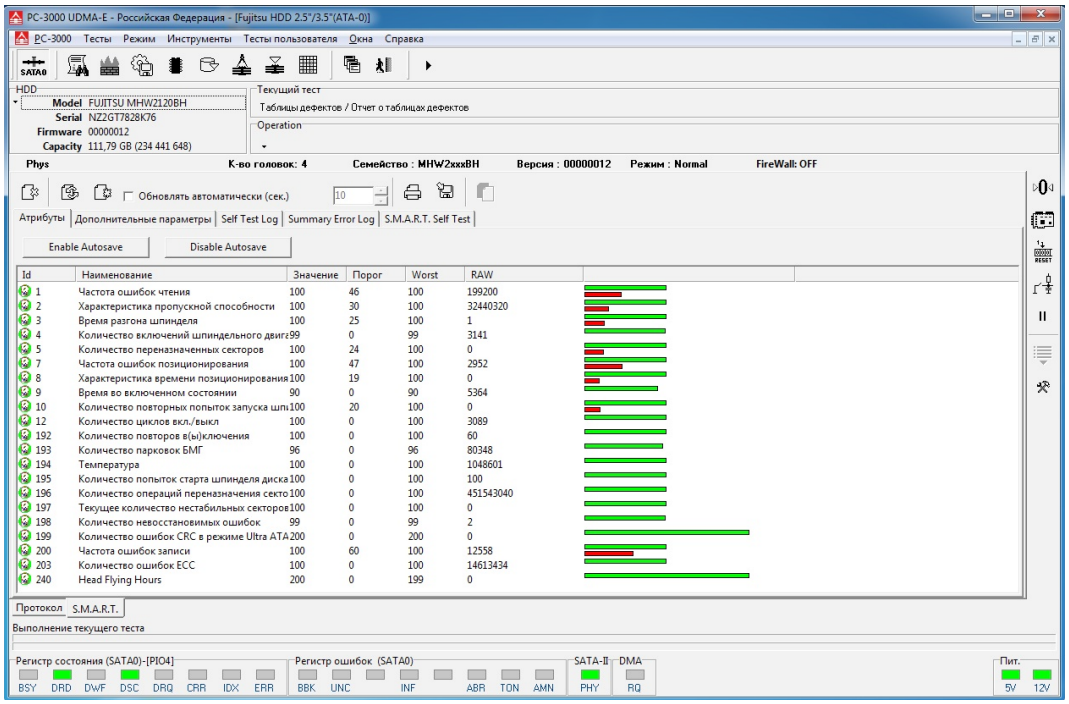


Рис. 5. Параметры S.M.A.R.T. FUJITSU MHW2120BH

SAMSUNG HM121HC позволило получить расчетное время копирования весьма близкое к практическому результату.

3. В виду наличия нестабильных секторов расчетное время копирования может значительно отличаться от того времени, которое затрачивается на реальное копирование. Такая ситуация характерна, например, для модели компании FUJITSU. Параметр номер 1 S.M.A.R.T. данного накопителя (рис. 5) указывает на наличие значительного количества ошибок чтения. Значение поля этого параметра RAW 199 200. Ошибки чтения требуют повторных обращений к сектору (и, следовательно, дополнительных затрат времени). Кроме того, в тех же параметрах S.M.A.R.T. отражено большое количество попыток переназначения секторов — параметр номер 196 имеет значение поля RAW 451 543 040, но попытки эти не были реализованы, т. к. другой параметр S.M.A.R.T. — номер 5, имеет значение поля RAW 0, но даже попытка переназначения требует временных затрат.

4. Из предыдущего пункта следует, что для того, чтобы расчетное время было близко к реальному, необходимо располагать не только информацией о модели НЖМД, но и о его техническом состоянии. Изу-

чение параметров S.M.A.R.T. может в какой-то степени помочь скорректировать расчетное значение времени копирования.

5. Для того, чтобы оценить время, необходимое для копирования данных произвольного объема, необходимо иметь информацию о том, какой объем подлежит копированию, и использовать формулу без корректировки, т. е. в качестве первого коэффициента модели β^r_1 использовать среднее время поиска.

Литература

1. Производительность HDD- и SSD-дисков. [Электронный ресурс] – URL: https://1cloud.ru/blog/proizvoditelnost-diskov/ (дата обращения: 07.03.2021).

2. Нижник Е. И. Математическая модель нагрузки файловой системы NTFS при активном поиске дисковых данных. [Электронный ресурс] – URL: http://tekhnosfera.com/ matematicheskoe-modelirovanie-proizvoditelnosti-faylovyh-sistem (дата обращения: 07.03.2021).

3. Коженевский С. Взгляд на жесткий диск «изнутри»: Перезапись информации. – Киев: ООО «ЕПОС», 2006. – 120 с.

4. SAMSUNG HM061GC HM080GC HM121HC HM160HC SPINPOIN M5P SERIES HDD. [Электронный ресурс] — URL: https://elektrotanya.com/samsung_hm061gc_hm080gc_hm121hc_hm160hc_spinpoin_m5p_series_hdd.pdf/download.html (дата обращения: 16.09.2021).

5. Устройство и принцип работы жесткого диска. [Электронный ресурс] – URL: https://leally.ru/download-soft/ustroistvo-i-princip-raboty-zhestkogo-diska/ (дата обращения: 16.09.2021).

References

1. Proizvoditel'nost' HDD- i SSD-diskov [HDD and SSD Performance]. Available at: https://1cloud.ru/blog/proizvoditelnost-diskov/ (accessed 7 March 2021).

2. Nizhnik E. Matematicheskaya model nagruzki faylovoy sistemy NTFS pri aktivnom poiske diskovykh dannykh [Mathematical model of NTFS file system load in active disk data search]. Available at: http://tekhnosfera.com/matematiches-koe-modelirovanie-proizvoditelnosti-faylovyh-sistem (accessed 7 March 2021).

3. Kozhenevskiy S. Vzglyad na zhestkiy disk "iznutri": Perezapis' informatsii. – Kiev: OOO "EPOS", 2006. – p. 120.

4. SAMSUNG HM061GC HM080GC HM121HC HM160HC SPINPOIN M5P SERIES HDD. Available at: https://elektrotanya.com/samsung_hm061gc_hm080gc_hm121hc_hm160hc_spinpoin_m5p_series_hdd.pdf/download.html (accessed 16 September 2021).

5. Ustroystvo i printsip raboty zhestkogo diska [Hard Drive Device and Operating Principle]. Available at: https://leally.ru/download-soft/ustroistvo-i-princip-raboty-zhestkogo-diska/ (accessed 16 September 2021).

ШАМОНИН Евгений Дмитриевич, кандидат технических наук, доцент кафедры алгебры и фундаментальной информатики, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, Уральский федеральный округ, Свердловская область, Екатеринбург, ул. Мира, 19. E-mail: shamonined@mail.ru

SHAMONIN Evgeniy Dmitrievich, Candidate of Technical Sciences, Associate Professor of Algebra and Fundamental Informatics, Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Ural Federal District, Sverdlovsk Region, Yekaterinburg, 19 Mira St. E-mail: shamonined@mail.ru

УДК 004.932.2 Вестник УрФО № 1(43) / 2022, с. 43–49

Вильховский Д.Э., Гуц, А.К.

DOI: 10.14529/secur220106

МЕТОД ОБНАРУЖЕНИЯ LSB-ВСТАВОК В ИСКУССТВЕННЫХ ЦВЕТНЫХ ИЗОБРАЖЕНИЯХ С ГРАДИЕНТНОЙ ЗАЛИВКОЙ С НИЗКИМ ЗАПОЛНЕНИЕМ СТЕГОКОНТЕЙНЕРА

В статье представлен метод обнаружения LSB-вставок и области их расположения в искусственных цветных изображениях с градиентной заливкой, эффективный при работе с низким заполнением стегоконтейнера. Метод обнаружения встраивания основывается на анализе комбинаций пикселей нулевого слоя исследуемого изображения и определении уникальных и повторяющихся последовательностей и локализации области встраивания посредством решения задачи о наибольшем пустом прямоугольнике с применением фильтра предварительной обработки полученного массива. Использование предлагаемого метода позволит организациям повысить уровень информационной безопасности за счет своевременного выявления наличия в таких изображениях скрытой злоумышленниками информации и принятия мер по блокировки пересылаемого сообщения.

Ключевые слова: *стегоанализ, стеганографический анализ, анализ стегоконтейнера, обнаружение LSB-вставки, метод замены наименее значащего бита.*

Vilkhovsky D.E., Guts A.K.

METHOD OF DETECTING LSB INSERTION IN LOW STEGO-PAYLOAD ARTIFICIAL COLOR IMAGES OF A GRADIENT FILL

The paper presents a method of detecting LSB insertion and its exact location in artificial color images of a gradient fill that is efficient when dealing with low stego-payload. The embedding detection method is based on a binary pixel combination matrix analysis for the zero layer of the image under study in order to determine the presence of unique and repeating sequences, the embedding area locating method that uses an algorithm for largest empty rectangles along with using a preprocessing filter that processes the resulting data array in order to eliminate noise distortions that narrow the area potential embedding area. Using the proposed method enables organizations to enhance their information security by timely detecting the information hidden by intruders in the images and taking measures to block the message from forwarding.

Keywords: *steganalysis, steganographic analysis, stegocontainer analysis, LSB-insertion detection, least significant bit replacement method.*

Популярность и эффективность LSB-вставок, то есть вставок, выполненных методом замены наименее значащего бита, как метода стеганографии объясняется тем, что встраивание в наименее значащий бит не приводит к визуально-заметным артефактам на изображении. При этом, чем меньший уровень заполнения стегоконтейнера, тем сложнее обнаружение стеговставки, что позволяет злоумышленникам незаметно передавать информацию в пересылаемом медиа-контейнере и ставит под угрозу информационную безопасность организаций.

Работы по стеганографическому анализу, выполненные в течение последних лет, предлагают преимущественно использование сверточных нейронных

сетей [1 –5] или алгоритмов на основе машинного обучения [6 – 8]. При этом применение сверточных нейронных сетей для целей стегоанализа имеет высокую стоимостную нагрузку, обусловленную сложностью вычислений. Использование алгоритмов на основе машинного обучения имеет меньшую стоимостную нагрузку, однако зачастую связано с проблемой выбора ядра и практически не решает задачу определения области встраивания.

Для искусственного изображения с градиентной заливкой применение нейронных сетей или алгоритмов, построенных на машинном обучении экономически нецелесообразно. Следовательно, для таких изображений необходимо разработать такой алгоритм, который бы имел высокую эффективность обнаружения наличия встраивания и высокую точность определения области встраивания при невысокой стоимости расчетов.

Таким образом, целью данного исследования является разработка алгоритма стеганографической атаки на метод LSB замены в искусственных цветных изображениях, позволяющего в автоматическом режиме детектировать скрытое в изображении сообщение. Подобный алгоритм целесообразно интегрировать во внутреннюю систему документооборота организации с целью предотвращения несанкционированной передачи третьим лицам чувствительной информации, т.е. противодействия промышленному шпионажу и повышения информационной, а следовательно, и экономической безопасности организации.

1. Общая постановка задачи

Карта битов нулевого слоя пикселей искусственного изображения с градиентной заливкой, в правый нижний угол которого было произведено встраивание наглядно демонстрирует измененную структуру в области встраивания (рис. 1).

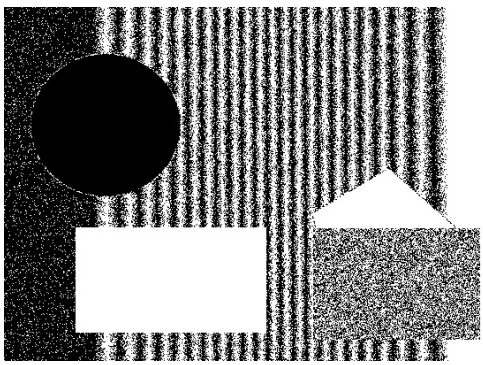


Рис. 1. Карта битов нулевого слоя пикселей искусственного изображения с градиентной заливкой

Анализ множества карт битов нулевого слоя пикселей искусственных изображений с градиентной заливкой, в которые было произведено встраивание методом LSB-замены, позволил установить, что область встраивания содержит преимущественно уникальные комбинации пикселей, тогда как в областях без встраивания в большом количестве присутствуют неуникальные последовательности, формирующие достаточно четко определяемые черно-белые полосы. Пример различий комбинаций пикселей приведен на рисунке 2.

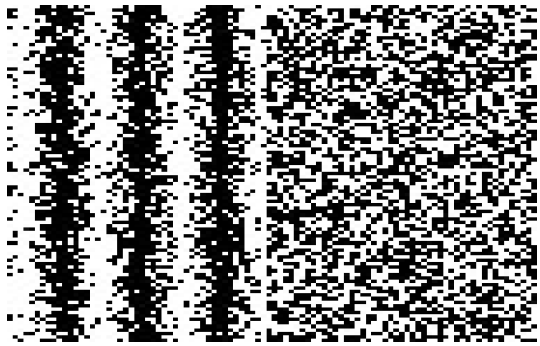


Рис. 2. Различие в комбинациях пикселей на карте битов нулевого слоя в области без встраивания (слева) и со встраиванием (справа)

Автоматическое обнаружение области сосредоточения уникальных комбинаций пикселей позволит выявлять наличие LSB-вставок, а также область их расположения на изображении-стегоконтейнере.

2. Характеристика алгоритма обнаружения наличия и месторасположения LSB-вставки на основе анализа комбинаций битов нулевого слоя пикселей

Алгоритм обнаружения встроенного сообщения, выполненного методом LSB-вставки, основывается на последовательном анализе каждого из пикселей нулевого слоя с окном 5 и записи последовательностей каждого окна в бинарном виде.

Окно 5 означает, что анализируется комбинация пикселей с размерностью 5x5, где центральным является анализируемый пиксель. Таким образом, справа, слева, сверху и снизу от исследуемого пикселя располагаются еще по 2 пикселя. Пример двух уникальных комбинаций пикселей с окном 5 приведен на рисунке 3.

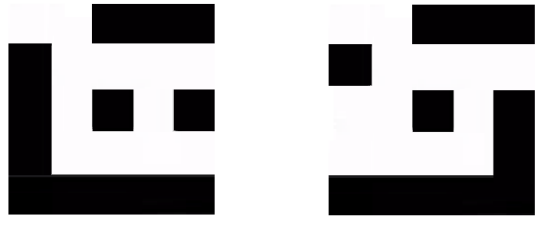


Рис. 3. Пример двух уникальных комбинаций пикселей с окном 5

Так, для окон, представленных на рисунке 3, комбинации имеют следующий вид (табл. 1):

Данные о комбинациях заносятся в хеш-таблицу линейным списком, где ключом является закодированная последовательность окна с исследуемым пик-

Таблица 1

Комбинации комбинаций пикселей в бинарном виде

Последовательность для окна а)	Последовательность для окна б)
0 1 1 1 1	1 0 0 0 0
1 0 0 0 1	0 0 0 0 1
0 0 1 0 1	1 0 1 0 1
1 0 0 0 1	0 0 0 0 1
1 1 1 1 1	0 1 1 1 0

селем, а значением – координаты исследуемого (центрального) пикселя.

Кроме того, заполняется еще одна структура, куда заносятся данные о комбинациях, включая саму последовательность и количество ее повторов. В результате, мы получаем бинарную матрицу размером N x M, содержащую единичные и нулевые значение, где нулевое значение присваивается пикселю, входящему в уникальную комбинацию, а единичное значение присваивается пикселю, входящему в неуникальную комбинацию. В результате, формируется матрица M_0, содержащая данные об уникальных и неуникальных комбинациях в бинарном виде.

В графическом виде данные указанной выше структуры представлены в виде массива из черных и белых точек. Пример графического изображения области, содержащей встраивание и области, не содержащей встраивание, в идеальной ситуации представлен на рисунке 4.

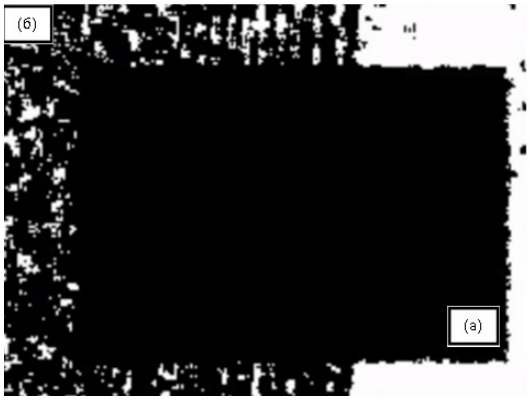


Рис. 4. Участки со встраиванием (а) и без встраивания (б)

Далее переходим к задаче о наибольшем пустом прямоугольнике, решение которой позволит определить наибольший прямоугольник, содержащий только нулевые значения, т.е. только уникальные комбинации.

3. Задача о набольшем пустом прямоугольнике

3.1. Общая характеристика о наибольшем пустом прямоугольнике

Задача о наибольшем пустом прямоугольнике впервые была представлена в работах А. Наамад, Д. Ли и В. Шу [9] с последующей корректировкой и уточнениями в работах этих и других авторов [10 – 14].

Решение задачи осуществляется в 2 этапа.

Этап 1. Анализируются отдельные значения элементов исходной бинарной матрицы M_0. Анализ проводится по рядам с последовательным преобразованием значений каждого из элементов и формированием новой матрицы M_1 по установленной схеме:

1. В строгом порядке все обнаруженные единичные значения элементов матрицы инвертируются в нулевые значения. Инвертирование осуществляется в неизменном виде вне зависимости от того, какое значение (нулевое или единичное) наблюдается у вышестоящих элементов исходной матрицы.

2. Каждому из обнаруженных нулевых значений присваивается порядковый номер его обнаружения по столбцам. Таким образом, всем элементам в первом ряду с нулевыми значениями присваивается значение 1, а элементу во втором ряду с нулевым значением, присваивается значение 2 только при условии, что значение вышестоящего элемента по его столбцу уже равно единице в формируемой матрице, что означает наличие нулевого значения по этому столбцу в исходной матрице. И т.д.

3. Любое инвертирование единичного значения элемента исходной матрицу в нулевое считается разрывом (обнулением) при анализе элементов исходной матрицы с нулевыми значениями. Например, если элемент (3;3) в исходной матрице был инвертирован в 0, то элементу (4;3), имеющему исходное нулевое значение, присваивается значение 1 независимо от того, какие значения присвоены элементам (1;3) и (2;3).

Пример анализа значений элементов бинарной матрицы приведен в таблице 2.

Таблица 2

Пример анализа значений элементов бинарной матрицы

Исходная матрица M_0						Получаемая матрица M_1					
0	0	0	1	0	0	1	1	1	0	1	1
0	0	1	0	0	1	2	2	0	1	2	0
0	1	0	0	0	0	3	0	1	2	3	1
0	0	0	0	0	0	4	1	2	3	4	2
0	0	0	0	0	1	5	2	3	4	5	0
1	0	0	1	0	0	0	3	4	0	6	1

Этап 2. Анализируется матрица M_1 с целью обнаружения прямоугольника с наибольшей площадью:

1) Определяются всех прямоугольники, расположенные между нулевыми значениями матрицы M_1;

2)Анализ осуществляется последовательно, начиная с самого нижнего ряда;

3) Основание прямоугольника должно лежать на исследуемом ряду;

Ниже приведен пример обнаружения прямоугольника с наибольшей площадью на основе данных, представленных в таблице 1:

$$H[6] = 0\,3\,4\,0\,6\,1 \rightarrow 6\,(3 \times 2)$$
$$H[5] = 5\,2\,3\,4\,5\,0 \rightarrow 10\,(2 \times 5)$$
$$H[4] = 4\,1\,2\,3\,4\,2 \rightarrow 8\,(2 \times 4)$$
$$H[3] = 3\,0\,1\,2\,3\,1 \rightarrow 4\,(2 \times 2)$$
$$H[2] = 0\,3\,4\,0\,6\,1 \rightarrow 4\,(2 \times 2)$$
$$H[1] = 1\,1\,1\,0\,1\,1 \rightarrow 3\,(1 \times 3)$$

Следовательно, искомая область – прямоугольник размером (2×5), основанием которого является 5 ряд (рис. 5)

Получаемая матрица M_1					
1	1	1	0	1	1
2	2	0	1	2	0
3	0	1	2	3	1
4	1	2	3	4	2
5	2	3	4	5	0
0	3	4	0	6	1

Рис. 5. Определение размеров и расположения наибольшего прямоугольника

3.2. Анализ уязвимости алгоритма решения задачи о наибольшем пустом прямоугольнике в рамках стегоанализа

Задача о наибольшем пустом прямоугольнике в качестве ограничителей рассматривает любые препятствия, включая случайные, то есть шумы. В рамках предлагаемого метода стегоанализа, основанного на нахождении уникальных комбинаций пикселей, шумом считается такой пиксель, который был определен как входящий в неуникальную комбинацию, но при этом находится в зоне предполагаемого встраивания, то есть среди множества уникальных комбинаций с высокой степенью плотности.

Выше было указано, что в идеальной ситуации, область со встраиванием должна содержать только уникальные комбинации пикселей, т.е. графически выражаться в виде прямоугольника, состоящего только из черных пикселей – как представлено на рис. 4. Однако, проведенные нами эмпирические исследования показали, что шумы присутствуют более чем в 99% случаях.

Так, для искусственного изображения с стеговставкой, карта битов которого приведена на рисунке 1, область встраивания содержит шумы, приведенные на рисунке 6.

Рис. 6. Карта пикселей с шумом в области со встраиванием

Таким образом, уязвимостью алгоритма решения задачи о наибольшем пустом прямоугольнике в рамках стегоанализа является риск значительного сокращения области предполагаемого встраивания из-за шумовых препятствий. Так, для примера, приведенного на рисунке 6, область обнаружения стеговставки в несколько раз меньше действительной – рисунок 7.

Рис. 7. Область обнаружения стеговставки при наличии шумов

3.3. Фильтр предварительной обработки изображения

С целью нивелирования шума и повышением точности обнаружения встраиваемых сообщений, структуру, полученную на 1 этапе решения задачи о наибольшем пустом прямоугольнике, необходимо предварительно обработать при помощи специального фильтра.

Для фильтрации шума последовательно произ-

водится сравнение исследуемого пикселя с двумя соседними пикселями с каждой стороны, а также двумя диагонально прилегающими пикселями. Таким образом, фильтр последовательно анализирует каждый из пикселей структуры с окном 5, в центре которого располагается исследуемый пиксель.

Для максимального учета всех возможных вариаций шумов, предлагается применять коэффициент 0,7. Т.е. если более 70% пикселей исследуемого окна являются пикселями, входящими в уникальную комбинацию (на рисунке – черного цвета), то исследуемый пиксель следует считать случайным шумом, не нарушающим общую картину уникальности имеющихся в этом окне комбинаций. Следовательно, для целей обнаружения стегоконтейнера данный пиксель следует считать пикселем, входящим в уникальную комбинацию, и присвоить ему нулевое значение.

Пример карты пикселей областей со встраиванием и без встраивания до и после обработки фильтром представлены, соответственно, на рисунках 8 и 9.

Рис. 8. Карта пикселей областей со встраиванием (а) и области без встраивания (б) до обработки фильтром

Рис. 9. Карта пикселей областей со встраиванием (а) и области без встраивания (б) после обработки фильтром

Таким образом, после обработки фильтром, в области со встраиванием мы получаем однородную карту пикселей, без каких-либо шумов, что позволяет в дальнейшем с максимальной точностью определить область встраивания.

Заключение

Алгоритм определяет координаты левого верхнего угла и правого нижнего угла и, основываясь на найденных координатах, выстраивает обнаруженный прямоугольник. Данный прямоугольник является областью стего-вставки. Решение задачи обнаружения области встраивания с применением данного алгоритма для искусственного изображения, карта пикселей которого представлена на рисунке 1, представлено на рисунке 10, где серый прямоугольник является областью встраивания, обнаруженной при помощи предлагаемого алгоритма.

Рис. 10. Карта битов нулевого слоя пикселей искусственного изображения с градиентной заливкой с обнаруженной областью встраивания (серый прямоугольник)

Тестирование предложенного алгоритма обнаружения встраивания, выполненного методом замены наименее значащих бит, было произведено с использованием 1000 цветных искусственных изображений с градиентной заливкой. Встраивание производилось поочередно в красную компоненту (33% всех встраиваний), зеленую компоненту (33% всех встраиваний) и синюю компоненту (34% всех встраиваний). Уровень заполнения стегоконтейнера варьировался от 25 до 10%.

Тестирование показало, что предлагаемый алгоритм способен обнаруживать факт наличия встраивания в 99,2% анализируемых случаях. В среднем, точность обнаружения области встраивания составляет 94,6%, что означает, что границы обнаруженной области встраивания в среднем на 5,4% меньше фактической области встраивания.

Таким образом, можно сделать вывод, что предлагаемый в данной работе метод обнаружения LSB-вставки с низким уровнем заполнения стегоконтейнера обладает высокой эффективностью в искусственных изображениях с градиентной заливкой.

Литература

1. Chaumont M. Deep learning in steganography and steganalysis // In Digital Media Steganography, Academic Press, 2020. P. 321–349.

2. Chen M, Boroumand M, Fridrich J. Deep learning regressors for quantitative steganalysis // Electron Imaging 2018. No 7. P 160–161.

3. Cogranne R., Giboulot Q., Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis // In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019. P. 125–137.

4. Xu G., Wu H-Z., and Shi YQ. Ensemble of CNNs for steganalysis: An empirical study // Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016. P. 103–107.

5. Ye J, Ni J, Yi Y. Deep learning hierarchical representations for image steganalysis // IEEE Trans Inf Forensics Secur. 2017, No 12(11). P. 2545–255.

6. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun, 2019. No. 70. P 233–245.

7. Chaeikar. S.S., Ahmadi A. SW: A blind LSBR image steganalysis technique // In Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018. P. 14–18.

8. Kumar U.P., Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers // International Journal of Innovative Technology and Exploring Engineering (IJITEE). Vol 8. 2019. P 1239 – 1246.

9. Naamad A., Lee D. T., Hsu W.-L. On the Maximum Empty Rectangle Problem // Discrete Applied Mathematics, 1984. P. 267–277.

10. Acharyya A, De M., Subhas C., Pandit S. Variations of largest rectangle recognition amidst a bichromatic point set // Discrete Applied Mathematics. Vol 286. 2020, P. 35-50.

11. Alok A., Subhash S. Fast algorithms for computing the largest empty rectangle // Proc. 3rd Annu. Symposium on Computational Geometry, 1987. P. 278–290.

12. Chazelle B., Drysdale R. L., Lee D. T. Computing the largest empty rectangle // STACS. Vol. 166. 1984. P. 43–54.

13. Sarkar, A., Biswas, A., Dutt, M., Bhattacharya, A. Finding a largest rectangle inside a digital object and rectangularization // Journal of Computer and System Sciences. Vol 95. 2018. P. 204-217.

14. Subhas C. Nardy, Bhargab B. Bhattacharya. Location of Largest Empty Rectangle among Arbitrary Obstacles // Foundations of Software Technology and Theoretical Computer Science. Vol.880. 1994. P.10-28.

References

1. Chaumont M. Deep learning in steganography and steganalysis // In Digital Media Steganography, Academic Press, 2020. P. 321–349.

2. Chen M, Boroumand M, Fridrich J. Deep learning regressors for quantitative steganalysis // Electron Imaging 2018. No 7. P. 160–161.

3. Cogranne R., Giboulot Q., Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis // In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019. P. 125–137.

4. Xu G., Wu H-Z., and Shi YQ. Ensemble of CNNs for steganalysis: An empirical study // Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016. P. 103–107.

5. Ye J, Ni J, Yi Y. Deep learning hierarchical representations for image steganalysis // IEEE Trans Inf Forensics Secur. 2017, No 12(11). P. 2545–255.

6. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun, 2019. No. 70. P. 233–245.

7. Chaeikar. S.S., Ahmadi A. SW: A blind LSBR image steganalysis technique // In Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018. P. 14–18.

8. Kumar U.P., Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers // International Journal of Innovative Technology and Exploring Engineering (IJITEE). Vol 8. 2019. P. 1239 – 1246.

9. Naamad A., Lee D. T., Hsu W.-L. On the Maximum Empty Rectangle Problem // Discrete Applied Mathematics, 1984. P. 267–277.

10. Acharyya A, De M., Subhas C., Pandit S. Variations of largest rectangle recognition amidst a bichromatic point set // Discrete Applied Mathematics. Vol 286. 2020, P. 35-50.

11. Alok A., Subhash S. Fast algorithms for computing the largest empty rectangle // Proc. 3rd Annu. Symposium on Computational Geometry, 1987. P. 278–290.

12. Chazelle B., Drysdale R. L., Lee D. T. Computing the largest empty rectangle // STACS. Vol. 166. 1984. P. 43–54.

13. Sarkar, A., Biswas, A., Dutt, M., Bhattacharya, A. Finding a largest rectangle inside a digital object and rectangularization // Journal of Computer and System Sciences. Vol 95. 2018. P. 204-217.

14. Subhas C. Nardy, Bhargab B. Bhattacharya. Location of Largest Empty Rectangle among Arbitrary Obstacles // Foundations of Software Technology and Theoretical Computer Science. Vol.880. 1994. P.10-28.

ВИЛЬХОВСКИЙ Данил Эдуардович, аспирант, ассистент кафедры информационной безопасности, Омский государственный университет им. Ф.М. Достоевского. 644077, г. Омск, пр. Мира, 55. E-mail: vilkhovskiy@gmail.com

ГУЦ Александр Константинович, доктор физико-математических наук, профессор кафедры кибернетики, Омский государственный университет им. Ф.М. Достоевского. 644077, г. Омск, пр. Мира, 55. E-mail: aguts@mail.ru

VILKHOVSKY Danil, postgraduate student, assistant professor of the Department of Information Security, Dostoevsky Omsk State University. 644077, Omsk, Mira Ave., 55. E-mail: vilkhovskiy@gmail.com

GUTS Alexander, Doctor of Physical and Mathematical Sciences, professor, of the Department of Cybernetics, Dostoevsky Omsk State University. 644077, Omsk, Mira Ave., 55. E-mail: aguts@mail.ru

УДК 004.056 Вестник УрФО № 1(43) / 2022, с. 50–63

Максимова Е. А., Буйневич М. В.

DOI: 10.14529/secur220107

МЕТОД ОЦЕНКИ ИНФРАСТРУКТУРНОЙ УСТОЙЧИВОСТИ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье отмечается, что существующие в настоящее время подходы к обеспечению безопасности критической информационной инфраструктуры (КИИ) не рассматривают субъекты КИИ с точки зрения системного подхода и (или) не учитывают инфраструктурную составляющую КИИ при построении системы защиты информации. В это же время, сама система при определенных условиях может генерировать деструктивизм инфраструктурного характера. Предлагаемая авторами исследования модель оценки инфраструктурной устойчивости (ИУ) КИИ представлена на инфраструктурно-контекстном (оценка инфраструктурной надежности) и структурном (оценка инфраструктурной целостности) уровнях и является ключевым компонентом в комплексной оценке информационной безопасности КИИ. Представлено решение проблемы учета факторов, связанных с инфраструктурной устойчивостью КИИ в процессе анализа ИБ и обеспечения возможности прогнозирования деструктивных воздействий при различных изменениях информационной инфраструктуры.

Ключевые слова: *критическая информационная инфраструктура, деструктивное воздействие, инфраструктурная устойчивости, инфраструктурный деструктивизм, надежность, целостность, субъект, объект, когнитивная модель, информационная безопасность.*

Maksimova E. A., Buynivich M. V.

THE METHOD OF ASSESSING THE INFRASTRUCTURAL STABILITY OF THE SUBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

The article notes that currently existing approaches to ensuring the security of critical information infrastructure (CII) do not consider CII subjects from the point of view of a systematic approach and (or) do not take into account the infrastructure component of CII when building an information security system. At the same time, the system itself, under certain conditions, can generate infrastructural destructiveness. The model for assessing the infrastructure sustainability (IS) of CII proposed by the authors of the study is presented at the infrastructure-contextual (assessment of infrastructure reliability) and structural (assessment of infrastructure integrity) levels and is a key component in a comprehensive assessment of information security of CII. A solution to the problem of taking into account factors related to the infrastructural stability of CII in the process of IS analysis and providing the possibility of predicting destructive impacts with various changes in the information infrastructure is presented.

Keywords: *critical information infrastructure, de-structive impact, infrastructural sustainability, infrastructural destructivism, reliability, integrity, subject, an object, cognitive model, Information Security.*

1. Введение

Вопросы безопасности критических инфраструктур являются приоритетными в международной практике. Однако, каждой страной данный вопрос исследуется и прорабатывается индивидуально, исходя из категориальной сущности понятия «критиче-

ская инфраструктура» [1 – 3]. Тем не менее, функционально, общим для всех стран в данном вопросе являются значимость КИ на всех уровнях государств, ослабляющий социально-экономический эффект развития общества в случае нарушения работы КИ, сложность КИ по своей структуре. Кроме того, практически во всех странах используется секторальный подход к определению КИ и актуализируется проблема обеспечения безопасности КИ, в том числе, с учетом инфраструктурных зависимостей и связей. Анализ международного опыта построения и развития КИ показал эффективность рассмотрения КИ с точки зрения системного подхода, что выражается в представлении КИ на структурном, функциональном, макроскопическом и микроскопическом уровнях.

Уникальность РФ в решении данного вопроса определяется объектным построением и развитием КИИ на базе регулятивного подхода, в том числе, определяющегося в [4, 5]. Регулятивный подход, с одой стороны, создает «тепличные условия» для развития КИИ РФ, с другой стороны обладает существенным недостатком, определяемым на методологическом уровне, что предлагается устранить за счет введение «системного» взгляда на «обустройство» КИИ. Выявленные в ходе анализа функции инфраструктуры КИИ: структурная, дифференцирующая, коммуникационная, процессуальная, управленческая, регулятивные (концептуальные, проектные, плановые), являются основой становления и развития КИИ как системы.

Инфраструктурно, КИИ представляют собой взаимосвязанные системы, включающие субъекты и объекты КИИ. Так, в РФ субъекты КИИ (СКИИ) – собственники объектов КИИ (ОКИИ), функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. ОКИИ – информационные системы (ИС), автоматизированные системы управления (АСУ), информационно-телекоммуникационные системы (ИТС), подразделяются на значимые и не значимые [5]. Однако, вопрос обоснования учета информационного взаимодействия при разработке мер по обеспечению безопасности значимого ОКИИ пока не проработан. В решении данного вопроса, на наш взгляд, необходимо учесть:

– динамичность СКИИ на инфраструктурном уровне;

– обеспечение безопасного функционирования ОКИИ как целевой задачи в системе поддержки принятия решений по управлению эксплуатацией ОКИИ;

– увеличение значимости межобъектного взаимодействия при обеспечении безопасности КИИ на фоне отсутствия регулятивных методов и методик для их идентификации и оценки.

Таким образом, в качестве ключевой проблемы в процессе обеспечения безопасности КИИ, можно определить проблему, связанную с необходимостью учета факторов, связанных с инфраструктурной устойчивостью (ИУ) КИИ в процессе анализа ИБ и обеспечением возможности прогнозирования деструктивных воздействий (ДВ) при различных изменениях информационной инфраструктуры.

Оценка ИУ в настоящее время рассматривается как самостоятельная задача. Так, например, в работе [6] представлена схема обеспечения устойчивости функционирования КИИ в условиях угроз комплексных информационно-технических воздействий и информационно-психологических воздействий, приводящих к компьютерным инцидентам в КИИ. Вопросы зависимости устойчивости инфраструктуры от топологии рассмотрены в [7, 8]. Достаточно близким к понятию «устойчивость» является понятие «надежность», но она характеризуется обычно как мера вероятности устойчивой работы, вероятности безотказной работы [9].

В контексте данного исследования, так как решается задача, связанная с определением меры инфраструктурной устойчивости, то на инфраструктурном уровне данная задача может быть решена путем оценки надежности и целостности рассматриваемой системы.

2. Используемые методы

КИИ является сложноструктурированной системой, для описания которой требуется учет большого количества факторов, что является определяющим для выбора метода нечеткого когнитивного анализа и сценарного моделирования [10-13] для ее исследования.

Применение когнитивного подхода в качестве основного инструмента моделирования задач управления и принятия решений в социальных и экономических системах обосновывается в работах А. Н. Целых, Л. А. Целых, Н. А. Абрамова, З. К. Авдеева, В. В. Борисов, В. Е. Гвоздев, Г.В. Горелова, Д.А. Новиков, Б. Г. Ильясов, В. А. Камаев, С. В. Ковриги, А. А. Кулинич, Д. Г. Лагерев, В. И. Максимов, Л. В. Массель, А. Г. Подвесовский, А. Н. Райков, В. Б. Силов, А. С. Федулов,R. Axelrod, P. P. Groumpos, B. Kosko, E .I. Papageorgiou, F.S. Roberts, J.L. Salmeron, C. D. Stylios, Y Y Haimes, P. Jiang. Однако в данных работах не рассматриваются вопросы управления ИБ инфраструктуры как сложной системы с учетом внутрисистемных деструктивно-образующих связей. При рассмотрении данного вопроса интересны работы Р. А. Демидова, П. Д. Зегжды, П. Ивановой, А. Е. Колоденковой, N. A. Jones, H. Ross, T. Lynam, P. Perez, A. Leitch, описывающие сложные информационные структуры, однако не исследующие вопросы комплексной обработки информации о состоянии инфор-

мационной инфраструктуры для поддержки принятия управленческих решений. Для инфраструктуры инфокоммуникационных систем с учетом факторов технического и экономического характера данные вопросы частично рассматривались в работах О. С. Лаута, Young-HyunChoi, S.Kukliński, Zhao, M. J. Creaner. Принципы функционирования и структура системы управления IT-инфраструктурой предложены Теленик С. Ф., Ролік О. І., Букасовым М. М., Соколовським Р. Л. Однако, ими не рассматривались аспекты ИБ.

Таким образом, вопрос оценки инфраструктурной устойчивости КИИ будем рассматривать с точки зрения комплексного учета различных факторов инфраструктурного, технического, экономического и регулятивного характера для поддержки принятия решений во время управления ИБ КИИ.

3. Дискуссия

Оценка ИУ КИИ выполнялась в рамках комплексной оценки ИБ КИИ для реализации которой разработана соответствующая когнитивная модель, где кроме регулятивных составляющих, регламентированных в документе [5], предусматривается влияние на целевой концепт факторов, связанных с деструктивными воздействиями инфраструктурного характера (рисунок 1).

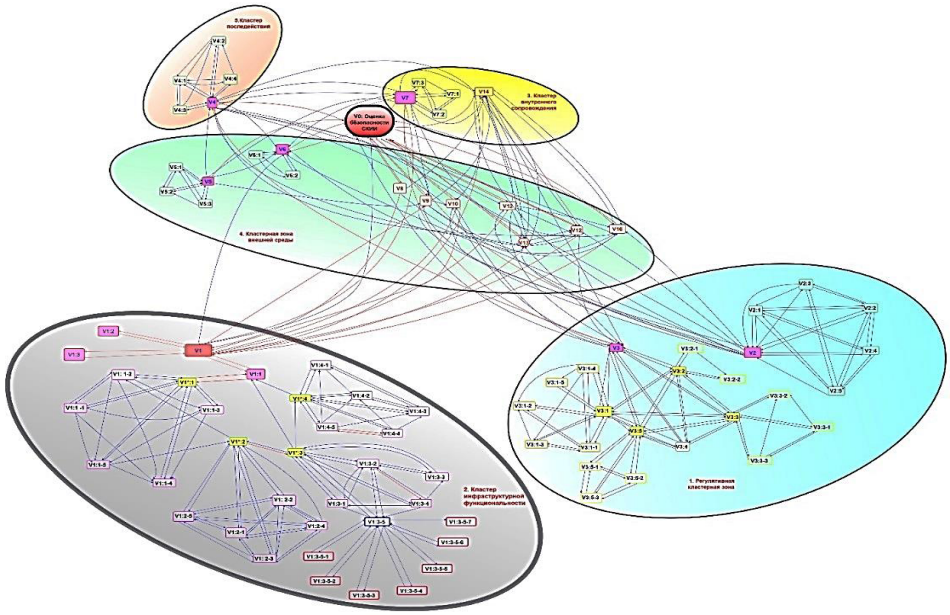


Рис. 1. Когнитивная модель «Оценка информационной безопасности КИИ при деструктивных воздействиях»

Представленная на рисунке 1 когнитивная модель имеет многоуровневую структуру. К примеру, для оценки инфраструктурного деструктивизма, в том числе определены концепты: V1*:1 «Ошибки, связанные с развитием СЗИ СКИИ на разных этапах жизненного цикла», V1*:2 «Оценка факторов риска безопасности СКИИ инфраструктурного характер», V1*:4 «Оценка факторов риска безопасности СКИИ, связанных с межсубъектными связями», представленные на втором уровне модели. К концептам третьего уровня модели отнесены, к примеру, V1:1-3 «Ошибки при реализации системы защиты субъекта КИИ», V1:1-5 «Отсутствие (не корректное построение) системы разграничения доступа в среде субъекта КИИ», V1:3-2 «Не учет межобъектных связей в среде субъекта КИИ», V1:3-5 «Наличие деструктивно-образующих межобъектных связей», V1:4-1 «Не учет межсубъектных отношений в среде функционирования КИИ», V1:4-2 «Снижение уровня безопасности хотя бы одного из взаимодействующих субъектов КИИ» и др. [16].

Инфраструктурная устойчивость СКИИ проявляется в инертной форме и в контексте когнитивного моделирования ИБ СКИИ может рассматриваться как мера силы концепта V1: «Оценка функциональности СКИИ» [14, 15]. При этом, в рамках когнитивного моделирования, традиционно, значения концептов задаются экспертно. В это же время, на наш взгляд, возможна ее оценка с использованием аппарата логико-вероятностного моделирования, путем четкой структуризации системы – СКИИ. Таким образом, повышается уровень достоверности получаемых результатов.

В ходе исследования инфраструктурной устойчивости СКИИ предлагается выполнить процедуру структуризации СКИИ как системы через процедуру деструктуризации инфраструктуры соответствующего субъекта и определения топологических особенностей полученных подсистем. Согласно [16] при декомпозиции структуры СКИИ можно выделить односвязную, многосвязную, логическую декомпозиции структуры, а также декомпозицию, связанную с разложени-

ем по полной группе событий относительно выделенных элементов, блоков и др. Применительно к КИИ возможны также декомпозиции системы на уровне КИИ (для межсубъектного взаимодействия) и на уровне СКИИ (для межобъектного взаимодействия).

Таким образом, на уровне субъекта КИИ рассматриваем три варианта декомпозиции: регулятивная декомпозиция (однослойная) – пообъектная декомпозиция СКИИ, двухслойная декомпозиция СКИИ – декомпозиция на уровне одного субъекта КИИ выполненная путем объединения взаимодействующих объектов в подсистемы. При данном варианте декомпозиции внешнее воздействие на элементы СКИИ не учитываются, двухслойная декомпозиция СКИИ - декомпозиция на уровне взаимодействующих субъектов КИИ с одновременным выполнением двухслойной декомпозиции взаимодействующих субъектов.

В теории надежности технических систем перечисленные схемы декомпозиции являются базовыми. С помощью них и при использовании аппарата структурно-логического анализа можно выйти на оценку основных характеристик надежности исследуемого объекта, где не маловажную роль играет определение его структуры.

Таким образом, оценка ИУ СКИИ характеризуется возможностью оценивания вероятности безотказной работы объектов КИИ и предотвращения сбоев в функционировании сфер КИИ, что гарантирует стабильность и требуемый уровень ИБ. Проблема оценки ИУ в данном случае приобретает ключевой характер при комплексной оценке ИБ СКИИ.

С этой точки зрения необходимо в структуре СКИИ выделить группы элементов:

1) отказ которых практически не влияет на работоспособность системы;

2) работоспособность которых практически не изменяется и вероятность их безотказной работы близка к единице;

3) ремонт или регулировка которых возможны в процессе работы;

4) отказ которых приводит к отказу системы.

При анализе инфраструктурной устойчивости системы (ИУС) имеет смысл включать в рассмотрение элементы только последней группы. При расчете вероятности безотказной работы подъобъектов КИИ и других характеристик инфраструктурной устойчивости целесообразно воспользоваться структурно-логическими схемами надежности, в которых учитываются взаимосвязь элементов друг с другом и их влияние на работоспособность СКИИ как системы.

Оценка инфраструктурной устойчивости СКИИ P_{subj} рассчитывается аналогично схемам оценки инфраструктурной устойчивости ОКИИ для параллельного и последовательного соединения ОКИИ. Далее, для оценки инфраструктурной устойчивости СКИИ осуществляется формирование структурной схемы взаимосвязи ОКИИ и, исходя из вероятностей безотказной работы ОКИИ и вероятности реализации угроз, рассчитывается оценка инфраструктурной устойчивости СКИИ.

Полученная оценка инфраструктурной устойчивости СКИИ позволяет оценивать вероятность безотказной работы ОКИИ и предотвращать сбои в работе КИИ, что гарантирует стабильность и требуемый уровень ИБ.

Оценка инфраструктурной устойчивости СКИИ на уровне инфраструктуры субъекта в когнитивной модели «Оценка ИБ СКИИ» реализована на уровне подсистем. Результаты работы данной модели представлены:

1) оценкой коэффициента инфраструктурной целостности СКИИ (как исходного данного для оценки силы концепта V1 «Оценка функциональности СКИИ») – K(inf_int);

2) оценкой коэффициента структурной функциональности СКИИ (как исходного данного для оценки силы концепта V1 «Оценка функциональности субъекта КИИ») – K(str_func);

3) набором сценариев достижения требуемого уровня функциональности СКИИ в зависимости от вида инфраструктуры СКИИ.

Оценку коэффициента инфраструктурной целостности СКИИ K(inf_int) предложено выполнить с учетом топологии подсистемы взаимодействующих ОКИИ. Данный показатель напрямую определяется целостностью подсистем взаимодействующих объектов (ПВО) СКИИ.

Оценка целостности ПВО СКИИ выполняется исходя из реализации комплекса мероприятий, связанных с оценкой прогнозируемых состояний информационной инфраструктуры на соответствие предъявляемым требованиям и регламентам. Структурные характеристики системы в данном случае являются показателями качества инфраструктуры с точки зрения системного подхода.

Кроме того, вводим новый показатель – коэффициент структурной функциональности СКИИ – K(str_func). Данный показатель не является стандартной топологической характеристикой с точки зрения системного подхода и теории надежности систем. В данном исследовании он введен для определения значения соответствующего концепта.

Для оценки K(str_func) разработана модель оценки коэффициента инфраструктурной функциональности СКИИ. Алгоритмически, она представлена следующим набором шагов:

Шаг 1: анализ инфраструктуры СКИИ.

Шаг 2: декомпозиция инфраструктуры СКИИ путем выделения подсистемы взаимодействующих объектов.

Шаг 3: построение модели «Оценка структурной

функциональности СКИИ» в виде инфраструктурной схемы взаимодействующих объектов. Для данной модели:

1) веса связей O_{ij} определяются экспертным путем, исходя из вида взаимосвязи,

2) значения концептов F(Oi) устанавливаются, исходя из категорий значимости соответствующих объектов в шкале [0,1] по заданному правилу,

3) значения весов связей «Oi_F(Sj)» равны +1 для всех i, j,

4) значения весов связей «F(Sj)_V1» равны +1 для всех j.

Шаг 4: На основе треугольной функции принадлежности оцениваем значение коэффициента структурной функциональности K(str_func).

4. Экспериментальное исследование

Предложенная модель оценки ИУ КИИ в рамках комплексной оценки ИБ КИИ имеет программную реализацию (рисунок 2) [17 – 25], для разработки которых в том числе использовалась [26, 27] и апробирована в ходе экспериментального исследования на базе СКИИ Поликлиника.

В соответствии с договором на НИР было произведено обследование технических средств Поликли-

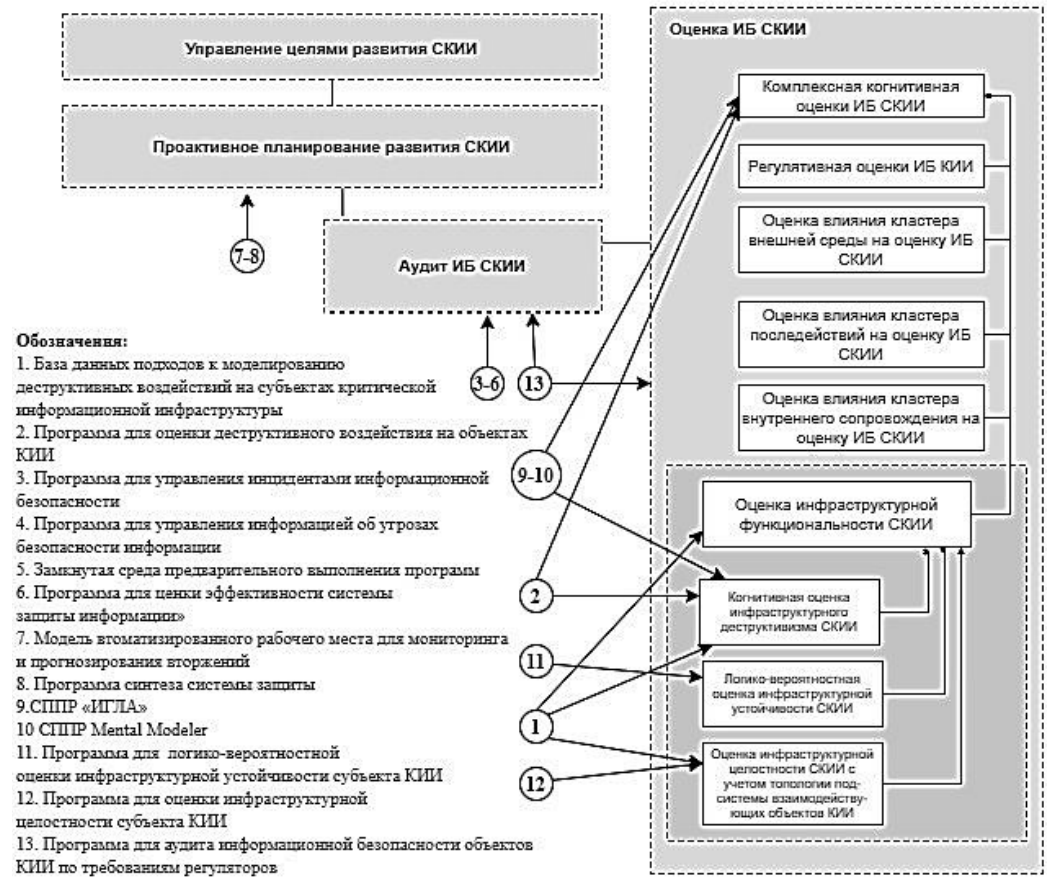


Рис. 2. Систематизация использования программных средств при решении задачи обеспечения безопасности СКИИ при ДВ

ники по требованиям регуляторов. В результате обследования было выявлено, что на данных технических средствах ведется обработка персональных данных работников и пациентов Поликлиники. Технические средства объединены в локальную сеть. Локальная сеть в Поликлинике является одноранговой, имеющей подключение к сетям связи общего пользования.

На момент обследования была представлена информация о следующих ИС, в которых обрабатываются персональные данные в Поликлинике – O_1: ИСПДн «1С зарплата и кадры»; O_2: ИСПДн «1С Бухгалтерия»; O_3: ИСПДн «Система видеонаблюдения»; O_4: ИС «Система пожарной охраны»; O_5: ИСПДн МИС «Инфоклиника»; O_6: ИСПДн МИС «1С ОМС»; O_7: ИСПДн «База данных «Chip»»; O_8: ИСПДн «МИС ПАКС».

Согласно [5] определены категории значимости ОКИИ: $Cat\_Zn(O_1) \equiv 3$, $Cat\_Zn(O_2) \equiv 3$, $Cat\_Zn(O_3) \equiv O3$; $Cat\_Zn(O_4) \equiv 3$, $Cat\_Zn(O_5) \equiv 2$, $Cat\_Zn(O_6) \equiv 3$, $Cat\_Zn(O_7) \equiv 3$, $Cat\_Zn(O_8) \equiv 3$.

Исходя из анализа исходных данных, полученных при анкетировании работников Поликлиники, все ИСПДн были объединены в две группы:

– подсистема S1: «не медицинская» – ИСПДн «Бухгалтерия, кадры и системы сопровождения». Работники подсистемы S2 осуществляют передачу данных в сторонние организации;

– подсистема S2: «медицинская» – ИСПДн «Пациенты». Работники ИСПДн «Пациенты» осуществляют передачу данных в Территориальный фонд медицинского страхования региона, региональный областной медицинский информационно-аналитический центр и комитет здравоохранения области, используя ПО ViPNet Client 4.x (сеть Интернет) и АПКШ «континент-К» (защищенная сеть передачи данных «РИСЗ»).

В результате обследования ИС Поликлиники выявлены реализуемые меры по защите информации на объектах КИИ.

В ходе исследования выполнялись следующие виды работ: 1) сбор сведений о программном обеспечении, установленном на ПК; 2) сбор сведений об аппаратном обеспечении и его характеристик; 3) опрос пользователей, с целью выявления уязвимых мест защиты информации, обрабатываемой на данном ПК; 4) сбор и анализ данных о физической защите информации.

В ходе аудита ИБ Поликлиники стандартными методами, оценка ИБ определена на среднем уровне, с выдачей соответствующих рекомендаций по ее повышению.

На следующем этапе исследование выполнялось с использованием представленных методов и моделей. Для этого:

Шаг 1. Выполнена декомпозиция инфраструктуры Поликлиники на подсистемы взаимодействующих объектов (рисунок 3).

По результатам данного этапа определено следующее:

1) в составе СКИИ Поликлиника – 2 подсистемы

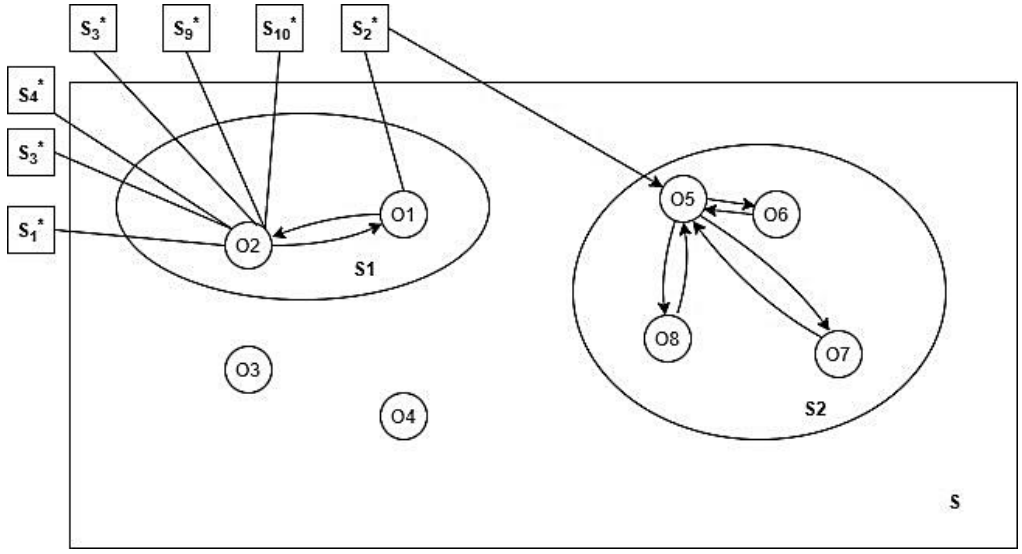


Рис. 3. Декомпозиция инфраструктуры СКИИ Поликлиника на подсистемы взаимодействующих объектов

взаимодействующих объектов и два локальных ОКИИ, не участвующих во взаимодействии ни на внутреннем, ни на внешнем уровнях;

2) объект О1 имеет двустороннюю связь с внешним СКИИ S_2*;

3) объект О2 имеет двустороннюю связь с внешними СКИИ S_1*, S_3*– S_7*;

4) существует односторонняя связь между S_2* и O_5;

5) двусторонние связи присутствуют между объектами: О1 и О2, О5 и О6, О5 и О7, О5 и О8.

Шаг 2. Определено наличие возможных деструктивных межсубъектных взаимодействий.

В ходе анализа определено наличие межсубъектных взаимодействий по сферам: здравоохранение (Z), банковская и иная финансовая сфера (B): «Z – Z», «Z – B», «B – Z». Где:

1) межсубъектное взаимодействие вида «Z – B» является нейтральным;

2) межсубъектное взаимодействие вида «B – Z» является косвенным, т. е. изменение состояния СКИИ из банковской сферы может повлечь за собой изменения в состоянии СКИИ сферы здравоохранения при выполнении определенного рода условий;

3) межсубъектное взаимодействие вида «Z – Z» может рассматриваться как деструктивно-образующее, так как изменение состояния одного субъекта приводит к изменениям в состоянии другого субъекта.

Таким образом приходим к следующему выводу.

Вывод: для предотвращения ИД на уровне межсубъектного взаимодействия рекомендуется использовать дополнительные средства защиты в системах взаимодействия: во-первых, в ИС ТФОМС с ИСПДн «1С Бухгалтерия» Поликлиники; во-вторых, в ИС ОМИ-

АЦ с ИСПДн «1С Бухгалтерия», ИСПДн «1С зарплата и кадры», ИСПДн МИС «Инфоклиника» Поликлиники.

Шаг 3. Откорректированы категории значимости ОКИИ СКИИ Поликлиники.

Для выполнения данного шага определены подсистемы взаимодействующих объектов, в которых категории значимости имеют различные значения. Так, в подсистеме S_2 объекту O_5 присвоена вторая категория значимости, категория значимости взаимодействующих с данным объектов O_6, O_7 и O_8 – третья.

Важно отметить, что в данной подсистеме присутствуют двусторонние связи между объектами O_5 и O_6, O_5 и O_7, O_5 и O_8. Таким образом, возникает вопрос о необходимости корректировки категорий значимости объектов O_6, O_7 и O_8, так как они имеют категорию значимости ниже, чем у взаимодействующего с ними объекта O_5. Данные ОКИИ представляют из себя ИС. По результатам экспертного опроса определены виды межобъектных взаимодействий, согласно чего можно говорить об отсутствии необходимости корректировки категорий значимости ОКИИ Поликлиники.

Шаг 4. Выполнена оценка ИЦ СКИИ Поликлиника.

Шаг 4.1. Выполнена оценка топологических показателей.

Для оценки ИЦ СКИИ Поликлиника использована программа для оценки ИЦ СКИИ [26]. По результатам работы получены оценочные данные (таблица 1).

По результатам анализа матрицы связности констатируем наличие в структуре СКИИ обрывов и висячих вершин. Кроме того, параметр R, отвечающий за структурную избыточность меньше нуля, что говорит об отсутствии связанности инфраструктуры на данном СКИИ. По параметрам структурной компактности данный субъект не является относительно целостным, так как соответствующий параметр Qотн <0. По оценке степени централизации: так как $\sigma \neq 1$ и $\sigma \neq 0$, то можно говорить о том, что исследуемый СКИИ не относится к типам: звезда, полный граф и кольцо.

Таблица 1

Количественные значения показателей ИЦ СКИИ Поликлиника

Показатель ИЦ	Количественное значение
Структурная избыточность, R	– 0.765
Неравномерность распределения связей, ε^2 (для систем с большой избыточностью)	– 8.22
Абсолютная компактность, Q	36
Относительная компактность, Qотн	– 0.88
Диаметр, d	2
Индекс центральности, σ	None

Шаг 4.2. Выполнена оценка коэффициента структурной функциональности СКИИ Поликлиника.

Для оценки коэффициента структурной функциональности СКИИ Поликлиника построен вероятностный граф межобъектного влияния (рисунок 4).

Для определения K(str_func) использована шкала соответствия значений концептов и категорий значимости ОКИИ, согласно которой: $Cat\_Zn(Oi) \equiv 3$, $i = \{1, 2, 3, 4, 6, 7, 8\} \Longrightarrow F\_zn(Oi) \equiv 0{,}35$, $Cat\_Zn(O5) \equiv 2 \Longrightarrow F\_zn(O5) \equiv 0{,}7$.

По результатам экспертной оценки определены значения МОС (таблица 2).

В итоге, получено рассчитанное значение K(str_func) = 2,52; (Max_K(str_func) = 4.85) (таблица 3). Данное значение определяет значение концепта «Оценка ИЦ СКИИ» в общей когнитивной модели «Прогнозирование развития ситуаций и оценка ИБ СКИИ при деструктивных воздействиях».

Шаг 5. Выполнена оценка ИУ СКИИ Поликлиника.

Оценка ИУ СКИИ Поликлиника выполнено с помощью обозначенного выше алгоритма. В результате, значение ИУ получено на уровне 0.14.

По имеющимся исходным данным с помощью разработанного программного средства выполнено построение схемы взаимодействия подобъектов ОКИИ Поликлиники (рисунок 5).

Для оценки ИУ СКИИ использовались значения вероятностей реализации угроз, спрогнозированные на основе существующей статистики компании InfoWatch по инцидентам ИБ на предприятиях и в организациях, функционирующих в сферах КИИ [29]. Оценка ИУ СКИИ Поликлиника показала недостаточный уровень ИУ.

В данной ситуации возможно два варианта дальнейших действий: 1) полученный результат использовать для оценки ИБ СКИИ. В данном случае полученное значение будет принято, как значение соответствующего концепта; 2) воспользоваться предлагаемыми рекомендациями.

Шаг 6. Выполнена оценка и исследован ИД СКИИ Поликлиника.

Шаг 6.1. Статичный анализ.

В ходе работы с разработанной когнитивной моделью (рисунок 6), тип вершин V1*:1 и V1*:4 определен как «управляемый», с целью сокращения затрачиваемых вычислительных мощностей.

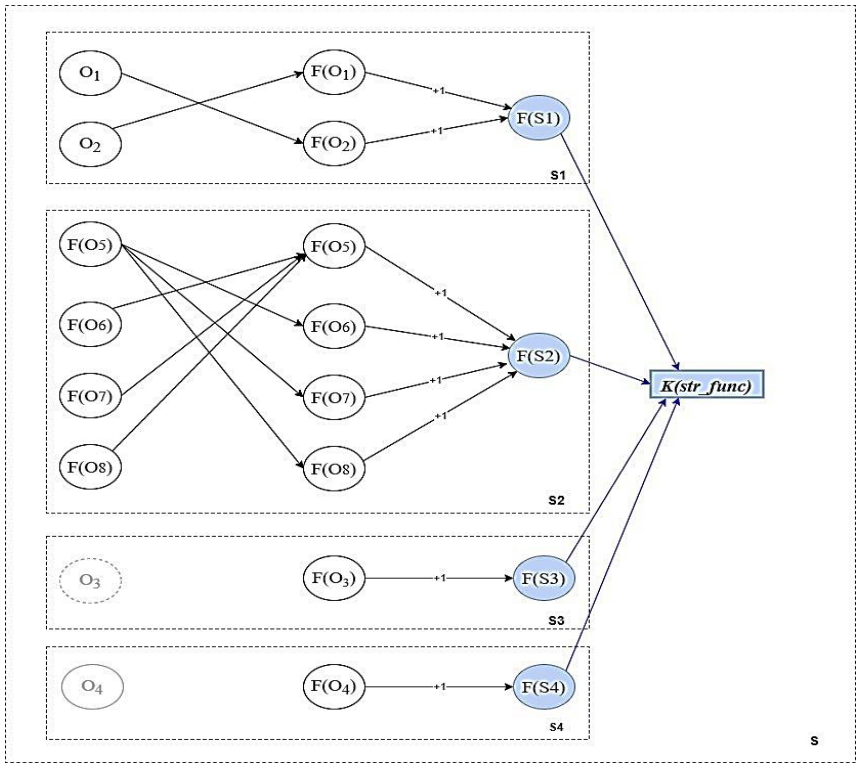


Рис. 4. Модель «Оценка коэффициента структурной функциональности СКИИ Поликлиника»

Таблица 2

Матрица значений МОС на СКИИ Поликлиника

	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8
O_1	0	0.5	0	0	0	0	0	0
O_2	0.5	0	0	0	0	0	0	0
O_3	0	0	0	0	0	0	0	0
O_4	0	0	0	0	0	0	0	0
O_5	0	0	0	0	0	0.7	0.8	0.2
O_6	0	0	0	0	0.3	0	0	0
O_7	0	0	0	0	0.6	0	0	0
O_8	0	0	0	0	0.1	0	0	0

Таблица 3

Расчётные значения для оценки коэффициента структурной функциональности СКИИ Поликлиника

Sj	Oi	Cat_Zn(Oi)	F_zn(Oi)	F(Oi)	max F(Oi)	Cat_Zn(Sj)	F_ zn(Sj)	F(Sj)	max F_zn(Sj)
S_1	O_1	3	0.35	0.175	0.5	3	0.35	0.35	1
	O_2	3	0.35	0.175	0.5				
S_2	O_5	2	0.7	0.35	1.05	2	0.7	1.47	3.15
	O_6	3	0.35	0.49	0.7				
	O_7	3	0.35	0.56	0.7				
	O_8	3	0.35	0.07	0.7				
S_3	O_3	3	0.35	0	0	3	0.1	0.35	0.35
S_4	O_4	3	0.35	0	0	3	0.35	0.35	0.35

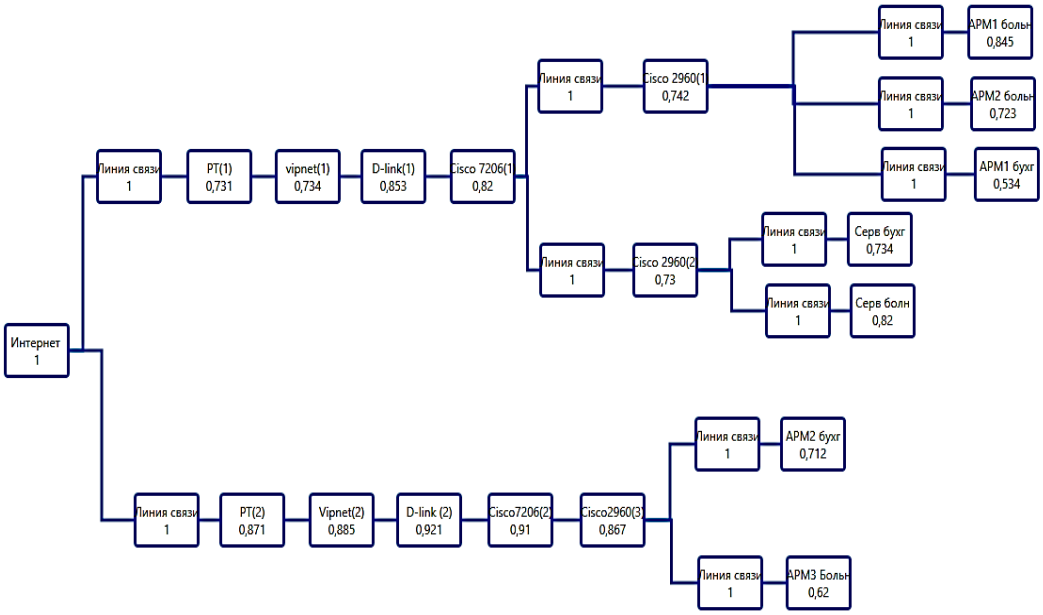


Рис. 5. Схема взаимодействия подобъектов ОКИИ Поликлиника на примере ИСПДн МИС «Инфоклиника»

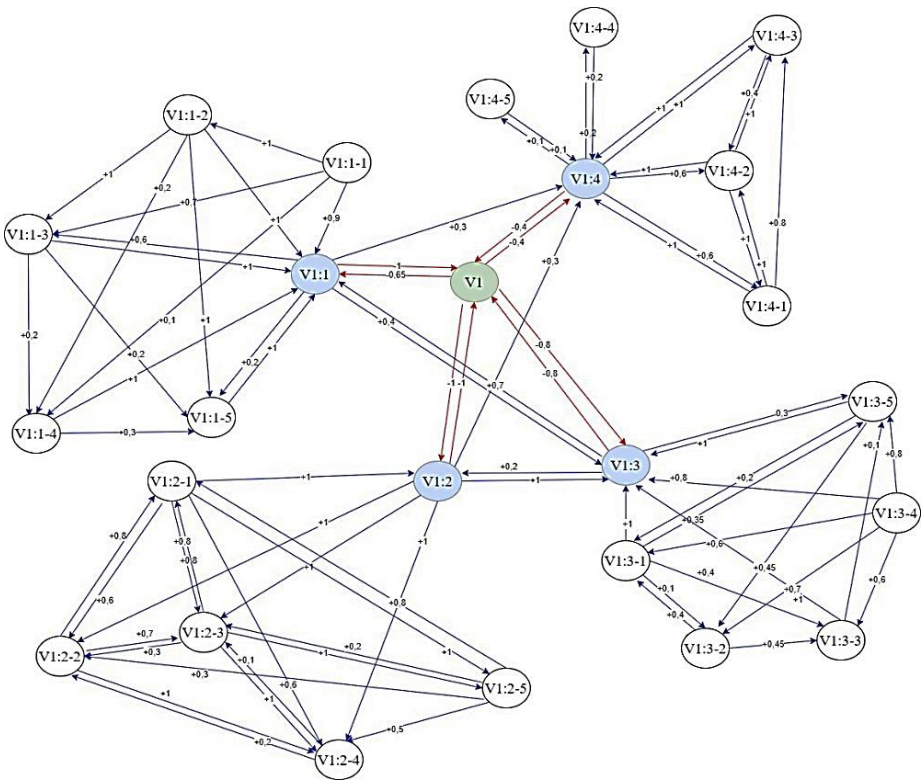


Рис. 6. Когнитивная модель «Оценка ИД СКИИ Поликлиника»

Таким образом, исходная когнитивная модель отождествляется с вариантом когнитивной модели, в которой, в отличии от рассматриваемой, поведение концептов третьего уровня, влияющих на концепты V1*:1 и V1*:4 в явном виде не рассматривается. В качестве целевых определены вершины V1 и V1*:2.

В ходе исследования по результатам экспертной оценки построена матрица взаимного влияния факторов когнитивной модели «Оценка ИД СКИИ Поликлиника» и рассчитаны значения системных показателей когнитивной модели «Оценка функциональности СКИИ».

Расчет системных показателей построенной когнитивной карты выявил высокий уровень консонан-

са. Оцененные консонансные значения концептов принимают максимальные значения, что говорит о высокой степени доверия к разработанной модели.

Анализ полученных значений позволяет определить концепты, оказывающие наиболее сильное влияние на систему. Так, наиболее сильное положительное влияние на систему среди всех концептов оказывают концепты: «Ошибки, связанные с первичной разработкой информационной инфраструктуры организации (предприятия)» (V1:1-1); «Инфраструктурное возмущение системы» (V1:3-4); «Ошибки инфраструктурного анализа» (V1:3-1); «Инфраструктурные ошибки при развитии СКИИ» (V1:2); «Ошибки при сопровождении СКИИ» (V1:2-1); «Реализация атаки на ОКИИ» (V1:2-2); «Ошибки при анализе требований для СКИИ» (V1:2-3); «Ошибки, связанные с определением перечня объектов, подлежащих категорированию» (V1:2-4). Соответствующие значения: 0.2584, 0.2525, 0.2493, 0.2460, 0.2460, 0.2460, 0.2460, 0.2460 соответственно (рисунок 7).

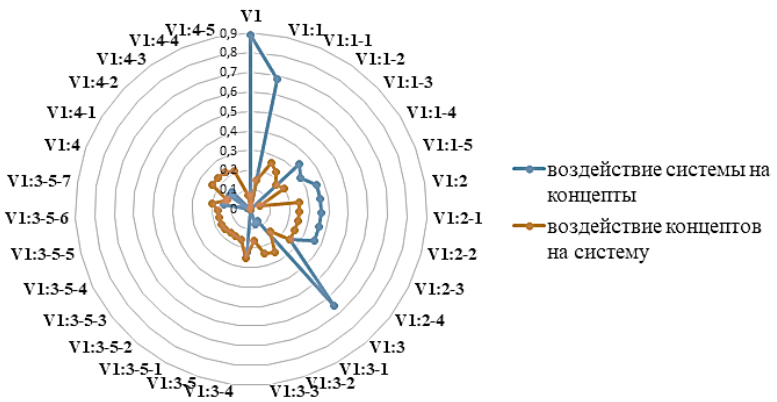


Рис. 7. Диаграмма результатов элементов статического анализа когнитивной модели «Оценка ИД СКИИ Поликлиника»

Отрицательно влияя на вышеперечисленные факторы, можно «сдвинуть» всю систему в положительную сторону. «Отрицательно» – в связи с формулировкой концептов.

Таким образом, с помощью когнитивного анализа выполнена формулировка концептов, которые наиболее сильно влияют на оценку функциональности СКИИ: ошибки, связанные с первичной разработкой информационной инфраструктуры Поликлиники, инфраструктурное возмущение системы, ошибки инфраструктурного анализа, инфраструктурные ошибки при развитии СКИИ, ошибки при сопровождении СКИИ, реализация атаки на ОКИИ, ошибки при анализе требований для СКИИ. Воздействуя на вышеперечисленные факторы, можно значительно повысить уровень безопасности СКИИ.

Результаты

Отличительной особенностью предложенного метода оценки ИУ СКИИ является системный подход к новому объекту защиты – СКИИ, а также комплексный подход к оценке ИБ. Для оценки ИБ, помимо регулятивных составляющих, предложено учитывать инфраструктурные особенности субъекта, порождающие угрозу саморазрушения системы. Основой алгоритма прогнозирования развития ситуаций и оценки ИБ СКИИ при деструктивных воздействиях являются сформулированные принципы выполнения декомпозиции СКИИ на подсистемы взаимодействующих объектов. Экспериментально подтверждено, что выделенные виды деструктивных воздействий инфраструктурного характера оказывают влияние на оценку ИБ СКИИ, что дает дополнительную информацию для принятия управленческих решений по вопросам обеспечения безопасности КИИ.

Литература

1. Infrastructure for the 21st Century Framework for a Research Age. [Электронный ресурс] / Vining Aidan R., Richards John (eds.). – Режим доступа: http://www.noravank.am/upload/pdf/21_VEK_01_2018.pdf.

2. Infrastructure Capital: What Is It? Where Is It? How Much of It Is There? [Электронный ресурс] / J. R. Baldwin, J. Dixon. – Режим доступа: https://www.researchgate.net/publication/23649155_Infrastructure_Capital_What_Is_It_Where_Is_It_How_Much_of_It_Is_There.

3. О критических инфраструктурах Евразийской интеграции [Электронный ресурс] / Г. Арутюнян. – Режим доступа: www.noravank.am/ rus/issues/detail.php?ELEMENT_ID=16344.

4. О безопасности критической информационной инфраструктуры Российской Федерации: Фе-

деральный закон от 26 июля 2017г. N 187-ФЗ (с изм. и доп.) [Электронный источник]. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

5. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также Перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постанов Постановление Правительства РФ от 8 февраля 2018 г. № 127 (не вступил в силу) [Электронный источник]. – URL: https://www.garant.ru/products/ipo/prime/doc/71776120/.

6. Климов С. М., Поликарпов С. В., Рыжов Б. С., Тихонов Р. И., Шпырня И. В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кибербезопасности. 2019. № 6(34), С.37–48.

7. Гаджиев Б.Р., Гибина Е.Ю., Прогулова Т.Б., Щетинина Д.П. Топология и устойчивость локально-мировых сетей // Программные продукты и системы № 4, 2009. С.51-54 - URL: https:// topologiya-i-ustoychivost-lokalno-mirovyh-setey.pdf.

8. Балашова Т.И. обеспечение отказоустойчивости сети повышением надежности её топологии // Современные проблемы науки и образования. – 2014. – № 6. – URL: http://science-education.ru/ru/article/view?id=16846.

9. Косолапов О.В. Устойчивость как одна из основных характеристик системы [Электронный ресурс] / О.В. Косолапов, М.Н. Игнатьева. // Известия Уральского государственного горного университета. — Электрон. дан. — 2013. — № 4. — С. 77-81. — URL: https://e.lanbook.com/journal/issue/290438. — Загл. с экрана.

10. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам: пер. с англ. М.: Наука, 1986. 496 с

11. Kosko V. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. 1986. Vol. 24. P. 65–75.

12. Ажмухамедов И.М. Информационная безопасность. Системный анализ и нечеткое когнитивное моделирование. – М.: Изд-во LAP, 2012. –385с.

13. Садовникова Н. П. Выбор стратегий территориального развития на основе когнитивного анализа и сценарного моделирования [Электронный ресурс] / Н. П. Садовникова, Н. П. Жидкова // Интернет-вестник ВолгГАСУ : серия Строительная информатика. - 2012. - № 7 (21). – URL: http://vestnik.vgasu.ru/attachments/SadovnikovaZhidkova-2012_7(21).pdf.

15. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103

16. Максимова Е.А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях//Монография: Федер. гос. авт. образоват. учреждение высш. образования «Волгогр. гос. ун-т»». - Волгоград: Изд-во ВолГУ, 2020. - 95 с.

17. Викторова В. С., Степанянц А. С. Многоуровневое моделирование надежности систем // Датчики и системы. – 2014. – № 6(181). – С. 33–37.

18. Патент на полезную модель № 139517 U1 Российская Федерация, МПК G06F 17/10. Автоматизированное рабочее место для мониторинга и прогнозирования вторжений / В. А. Корнева, Е. А. Максимова; заявитель Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Волгоградский государственный университет». – № 2013133255/08: заявл. 16. 07. 2013: опубл. 20.04.2014. – 2 с.

19. Патент на полезную модель №139517. Российская Федерация, Автоматизированное рабочее место для мониторинга и прогнозирования вторжений / В. А. Корнева, Е. А. Максимова; патентообладатель ФГАОУ ВО ВолГУ. – №2013133255; приоритет от 16.07.2013., зарегистр.19.03.2014, Бюл. № 11. – 2 с.

20. Свидетельство о государственной регистрации программы для ЭВМ №2020667300. Российская Федерация. Оценка деструктивного воздействия на объектах критической информационной инфраструктуры / Е. А. Максимова, М. Е. Каменнов; правообладатель ФГАОУ ВО ВолГУ. – №2020662052; заявл. 12.10.2020; опублик. 22. 12. 2020 – 1 с.

21. Свидетельство о регистрации программы для ЭВМ № 2021610425. Российская Федерация. Средство управления инцидентами информационной безопасности “ВЕКТОР” / М. Е. Каменнов, Е. А. Максимова, Ю. Н. Голубев; правообладатель ООО «Региональный аттестационный центр». – № 2020667689, заявл. 28.12.2020; опублик. 14.01.2021 – 1 с.

22. Свидетельство о регистрации программы для ЭВМ № 2021610482. Российская Федерация. Средство управления информацией об угрозах безопасности информации “БЕРЕСТЬЕ”/ М. Е. Каменнов, Е. А. Максимова, Ю. Н .Голубев; правообладатель ООО «Региональный аттестационный центр», № 2020667772, заявл. 28.12.2020; опублик. 14.01.2021 – 1 с.

23. Свидетельство о государственной регистрации программы для ЭВМ № 2019660368 Россий-

ская Федерация. Замкнутая среда предварительного выполнения программ «ТОР»/ В. А. Петров, Е. А. Максимова, Ю. Н. Голубев, М. В. Пономарев; заявитель Общество с ограниченной ответственностью «Региональный аттестационный центр». – № 2019619100: заявл. 24. 07. 2019: опубл. 05. 08. 2019 – 1 с.

24. Свидетельство о государственной регистрации программы для ЭВМ №2015662413. Российская Федерация. Оценка эффективности системы защиты информации / А. В. Петькиев, Е. А. Максимова; правообладатель ФГАОУ ВО ВолГУ. – №2015619218, заявл. 05. 10. 2015 г.; опублик. 24. 11. 2015. – 1 с.

25. Свидетельство о государственной регистрации программы для ЭВМ №2012618761. Российская Федерация. Синтез системы защиты / Максимова, В. А. Корнева; правообладатель ФГАОУ ВО ВолГУ. – № 2012616588; заявл. 01. 08. 2012; опублик. 26. 09. 2021. – 1 с.

26. Свидетельство о государственной регистрации программы для ЭВМ № 20216666613 Российская Федерация. Оценка инфраструктурной целостности субъекта критической информационной инфраструктуры / Е. А. Максимова; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Волгоградский государственный университет». – № 2021665746: заявл. 12. 10. 2021: опубл. 18. 10. 2021 – 1 с.

27. MentalModeler [Электронный ресурс]: сайт. – Режим доступа: http://www.mentalmodeler.org/

28. СППР «ИГЛА» [Электронный ресурс]: сайт. – Режим доступа: http://iipo.tu-bryansk.ru/quill/download.html.

29. Аналитика отрасли информационной безопасности [Электронный ресурс]: сайт. – Режим доступа: https://www.infowatch.ru/analytics/analitika.

References

1. Infrastructure for the 21st Century Framework for a Research Age. [Электронный ресурс] / Vining Aidan R., Richards John (eds.). – Режим доступа: http://www.noravank.am/upload/pdf/21_VEK_01_2018.pdf.

2. Infrastructure Capital: What Is It? Where Is It? How Much of It Is There? [Электронный ресурс] / J. R. Baldwin, J. Dixon. – Режим доступа: https://www.researchgate.net/publication/23649155_Infrastructure_Capital_What_Is_It_Where_Is_It_How_Much_of_It_Is_There.

3. O kriticheskikh infrastrukturakh Yevraziyskoy integratsii [Elektronnyy resurs] / G. Arutyunyan. – Rezhim dostupa: www.noravank.am/ rus/issues/detail.php?ELEMENT_ID=16344.

4. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Federal'nyy zakon ot 26 iyulya 2017g. N 187-FZ (s izm. i dop.) [Elektronnyy istochnik]. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

5. Ob utverzhdenii Pravil kategorirovaniya ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe Perechnya pokazateley kriteriyev znachimosti ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy: Postanov Postanovleniye Pravitel'stva RF ot 8 fevralya 2018 g. № 127 (ne vstupil v silu) [Elektronnyy istochnik]. – URL: https://www.garant.ru/products/ipo/prime/doc/71776120/.

6. Klimov S. M., Polikarpov S. V., Ryzhov B. S., Tikhonov R. I., Shpyrnya I. V. Metodika obespecheniya ustoychivosti funktsionirovaniya kriticheskoy informatsionnoy infrastruktury v usloviyakh informatsionnykh vozdeystviy // Voprosy kiberbezopasnosti. 2019. № 6(34), s .37–48.

7. Gadzhiyev B.R., Gibina Ye.YU., Progulova T.B., Shchetinina D.P. Topologiya i ustoychivost' lokal'no-mirovykh setey // Programmnyye produkty i sistemy № 4, 2009. C.51-54 - URL: https:// topologiya-i-ustoychivost-lokalno-mirovyh-setey.pdf.

8. Balashova T.I. obespecheniye otkazoustoychivosti seti povysheniyem nadezhnosti yeyo topologii // Sovremennyye problemy nauki i obrazovaniya. – 2014. – № 6. - URL: http://science-education.ru/ru/article/view?id=16846.

9. Kosolapov O.V. Ustoychivost' kak odna iz osnovnykh kharakteristik sistemy [Elektronnyy resurs] / O.V. Kosolapov, M.N. Ignat'yeva. // Izvestiya Ural'skogo gosudarstvennogo gornogo universiteta. — Elektron. dan. — 2013. — № 4. — C. 77-81. — URL: https://e.lanbook.com/journal/issue/290438. — Загл. с экрана.

10. Robertc F.S. Diskretnyye matematicheskiye modeli s prilozheniyami k sotsial'nym, biologicheskim i ekologicheskim zadacham: per. s angl. M.: Nauka, 1986. 496 c

11. Kosko V. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. 1986. Vol. 24. P. 65–75.

12. Azhmukhamedov I.M. Informatsionnaya bezopasnost'. Sistemnyy analiz i nechetkoye kognitivnoye modelirovaniye. – M.: Izd-vo LAP, 2012. -385c.

13. Sadovnikova N. P. Vybor strategiy territorial'nogo razvitiya na osnove kognitivnogo analiza i stsenarnogo modelirovaniya [Elektronnyy resurs] / N. P. Sadovnikova, N. P. Zhidkova // Internet-vestnik VolgGASU: seriya Stroitel'naya informatika. - 2012. - № 7 (21). – URL: http://vestnik.vgasu.ru/attachments/SadovnikovaZhidkova-2012_7(21).pdf.

15. Maksimova Ye.A. Kognitivnoye modelirovaniye destruktivnykh zloumyshlennykh vozdeystviy na ob"yektakh kriticheskoy informatsionnoy infrastruktury // Trudy uchebnykh zavedeniy svyazi. 2020. T. 6. № 4. C. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103

16. Maksimova Ye.A. Otsenka informatsionnoy bezopasnosti sub"yekta kriticheskoy informatsionnoy infrastruktury pri destruktivnykh vozdeystviyakh//Monografiya: Feder. gos. avt. obrazovat. uchrezhdeniye vyssh. obrazovaniya «Volgogr. gos. un-t»». - Volgograd: Izd-vo VolGU, 2020.- 95 c.

17. Viktorova V. S., Stepanyants A. S. Mnogourovnevoye modelirovaniye nadezhnosti sistem // Datchiki i sistemy. – 2014. – № 6(181). – C. 33-37.

18. Patent na poleznuyu model' № 139517 U1 Rossiyskaya Federatsiya, MPK G06F 17/10. Avtomatizirovannoye rabocheye mesto dlya monitoringa i prognozirovaniya vtorzheniy / V. A. Korneva, Ye. A. Maksimova; zayavitel' Federal'noye gosudarstvennoye avtonomnoye obrazovatel'noye uchrezhdeniye vysshego professional'nogo obrazovaniya "Volgogradskiy gosudarstvennyy universitet". – № 2013133255/08: zayavl. 16. 07. 2013: opubl. 20.04.2014. – 2 c.

19. Patent na poleznuyu model' №139517. Rossiyskaya Federatsiya, Avtomatizirovannoye rabocheye mesto dlya monitoringa i prognozirovaniya vtorzheniy / V. A. Korneva, Ye. A. Maksimova; patentoobladatel' FGAOU VO VolGU. – №2013133255; prioritet ot 16.07.2013., zaregistr.19.03.2014, Byul. № 11. – 2 c.

20. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2020667300. Rossiyskaya Federatsiya. Otsenka destruktivnogo vozdeystviya na ob"yektakh kriticheskoy informatsionnoy infrastruktury / Ye. A. Maksimova, M. Ye. Kamennov; pravoobladatel' FGAOU VO VolGU. – №2020662052; zayavl. 12.10.2020; opublik. 22. 12. 2020 – 1 c.

21. Svidetel'stvo o registratsii programmy dlya EVM № 2021610425. Rossiyskaya Federatsiya. Sredstvo upravleniya intsidentami informatsionnoy bezopasnosti "VEKTOR" / M. Ye. Kamennov, Ye. A. Maksimova, YU. N. Golubev; pravoobladatel' OOO «Regional'nyy attestatsionnyy tsentr». – № 2020667689, zayavl. 28.12.2020; opublik. 14.01.2021 – 1 c.

22. Svidetel'stvo o registratsii programmy dlya EVM № 2021610482. Rossiyskaya Federatsiya. Sredstvo upravleniya informatsiyey ob ugrozakh bezopasnosti informatsii "BEREST'Ye"/ M. Ye. Kamennov, Ye. A. Maksimova, YU. N. Golubev; pravoobladatel' OOO «Regional'nyy attestatsionnyy tsentr», № 2020667772, zayavl. 28.12.2020; opublik. 14.01.2021 – 1 c.

23. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2019660368 Rossiyskaya Federatsiya. Zamknutaya sreda predvaritel'nogo vypolneniya programm "TOR"/ V. A. Petrov, Ye. A. Maksimova, YU. N. Golubev, M. V. Ponomarev; zayavitel' Obshchestvo s ogranichennoy otvetstvennost'yu «Regional'nyy attestatsionnyy tsentr». – № 2019619100: zayavl. 24. 07. 2019: opubl. 05. 08. 2019 – 1 c.

24. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2015662413. Rossiyskaya Federatsiya. Otsenka effektivnosti sistemy zashchity informatsii / A. V. Pet'kiyev, Ye. A. Maksimova; pravoobladatel' FGAOU VO VolGU. – №2015619218, zayavl. 05. 10. 2015 g.; opublik. 24. 11. 2015. – 1 c.

25. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2012618761. Rossiyskaya Federatsiya. Sintez sistemy zashchity / Maksimova, V. A. Korneva; pravoobladatel' FGAOU VO VolGU. – № 2012616588; zayavl. 01. 08. 2012; opublik. 26. 09. 2021. – 1 c.

26. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 20216666613 Rossiyskaya Federatsiya. Otsenka infrastrukturnoy tselostnosti sub"yekta kriticheskoy informatsionnoy infrastruktury / Ye. A. Maksimova; zayavitel' Federal'noye gosudarstvennoye avtonomnoye obrazovatel'noye uchrezhdeniye vysshego obrazovaniya «Volgogradskiy gosudarstvennyy universitet». – № 2021665746: zayavl. 12. 10. 2021: opubl. 18. 10. 2021 – 1 c.

27. MentalModeler [Электронный ресурс]: sayt. – Rezhim dostupa: http://www.mentalmodeler.org/

28. SPPR «IGLA» [Elektronnyy resurs]: sayt. – Rezhim dostupa: http://iipo.tu-bryansk.ru/quill/download.html.

29. Analitika otrasli informatsionnoy bezopasnosti [Elektronnyy resurs]: sayt. – Rezhim dostupa: https://www.infowatch.ru/analytics/analitika.

МАКСИМОВА Елена Александровна, кандидат технических наук, доцент, доцент кафедры КБ-2 «Прикладные информационные технологии» института кибернетики и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет». Российская Федерация, 119454, ЦФО, г. Москва, Проспект Вернадского, д. 78. E-mail: maksimova@mirea.ru

MAKSIMOVA Elena Alexandrovna, Candidate of Technical Sciences, Associate Professor, Department of KB-2 "Applied Information Technologies" of the Institute of Cybernetics and Digital Technologies 1FGBOU VO "MIREA - Russian Technological University". Russian Federation, 119454, CFD, Moscow Moscow, Prospect Vernadsky, 78. E-mail: maksimova@mirea.ru.

БУЙНЕВИЧ Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России. Российская Федерация, 196105, СЗФО, г. Санкт-Петербург, Московский проспект, д. 149. E-mail: bmv1958@yandex.ru

BUINEVICH Mikhail Viktorovich, Doctor of Technical Sciences, Professor, Professor, Department of Applied Mathematics and Information Technology, St. Petersburg State Fire Service University EMERCOM of Russia. Russian Federation, 196105, NFD, St. Petersburg, Moskovsky Prospect, 149. E-mail: bmv1958@yandex.ru

УДК 347.775.03 Вестник УрФО № 1(43) / 2022, с. 64–73

Макарова О.С., Поршнев С.В.

DOI: 10.14529/secur220108

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ДИНАМИКИ ВЕРОЯТНОСТИ ПРОВЕДЕНИЯ КОМПЬЮТЕРНОЙ АТАКИ С ТОЧКИ ЗРЕНИЯ НАРУШИТЕЛЯ[1]

В статье отмечается, что методика оценки рисков информационной безопасности (ИБ) имеет ряд существенных ограничений, в частности, используется метод экспертных оценок. Как показывает практика ИБ, метод экспертных оценок имеет ряд ограничений, что в результате не позволяет сформировать необходимый и достаточный перечень мер по защите информации.

В статье детально описаны математические подходы, лежащие в основе методики прогнозирования динамики вероятности проведения компьютерной атаки (КА) с точки зрения нарушителя на основе статистических данных, в частности Теория положений криминологии, и Теория диффузии инноваций.

Отдельно отмечается важность формирования модели нарушителя для определения источников общедоступной информации для расчета вероятности КА. Приведено детальное описание методики прогнозирования динамики вероятности проведения КА с точки зрения нарушителя на основе статистических данных. А также оценка ее адекватности на основе данных о более чем 700 тысячах КА на кредитно-финансовый сектор (КФС) за 2017-2018 гг.

Ключевые слова: *компьютерная атака, прогнозирование вероятности угрозы, модель нарушителя, ожидаемая полезность, нарушитель.*

Makarova O.S., Porshnev S.V.

PREDICTING METHODOLOGY OF THE PROBABILITY DYNAMICS OF A COMPUTER ATTACK FROM THE POINT OF VIEW OF THE INTRUDER

The article notes that the methodology for assessing information security (IS) risks has a number of significant limitations, in particular, the method of expert assessments is used. As the practice of IS shows, the method of expert assessments has a number of limitations, which as a result makes it impossible to form a necessary and sufficient list of measures to protect information.

The article describes in detail the mathematical approaches underlying the methodology for predicting the dynamics of the probability of a computer attack from the intruder point of view based on statistical data, in particular, the Theory of the provisions of criminology, and the Theory of diffusion of innovations.

Separately, the importance of forming a model of the intruder for determining the sources of publicly available information for calculating the probability of an accident is noted. A detailed description of the methodology for predicting the dynamics of the probability of conducting a spacecraft from the point of view of the violator based on statistical data is given. As well as an assessment of its adequacy based on data on more than 700 thousand loans to the credit and financial sector for 2017-2018.

Keywords: *computer attack, threat probability prediction, intruder model, expected utility, intruder.*

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ).

Введение

В действующем законодательстве предусмотрена возможность дополнения перечня актуальных угроз ИБ новыми моделями угроз (МУ) [1-2]. В соответствие с «Методикой оценки угроз БИ», разработанной ФСТЭК России [1], оценка угроз ИБ осуществляется с помощью метода экспертных оценок.

Как показывает практика ИБ, метод экспертных оценок имеет ряд ограничений (в том числе: субъективность; отсутствие полноты или избыточность; сложная повторяемость процесса), что в результате непозволяет сформировать необходимый и достаточный перечень мер по защите информации.

Анализ результатов научных исследований, проведенный в работах [3-10], показал, что в большинстве исследований оценка эффективности и практической применимости предлагаемых подходов и методов оценки угроз БИ и рисков ИБ не проводится. Практические примеры реализации, приводимые в работах [11-15], зачастую используют либо несвязанные с реальными данными значения переменных показателей, либо их экспертные оценки. В этой связи в данной статье описываются математические подходы к определению методики прогнозирования вероятности угроз ИБ с точки зрения нарушителя, алгоритм реализации методики, а также оценка адекватности данной методики.

Математические подходы к описанию методики прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя

Данная методика основана на установленной в работах [4, 5, 8, 9] особенности реализации КА, проявляющейся в том, что вероятность проведения КА нарушителем является условной вероятностью достаточности ожидаемой полезности КА при наличии возможности реализации КА, которая вычисляется по следующей формуле:

$$P(EUA) = P(EU|A)\,P(A), \qquad (1.1)$$

где

P(EUA) – вероятность достаточности ожидаемой полезности КА вида «А» с точки зрения нарушителя;

P(A) – вероятность наличия возможности реализации нарушителем КА вида «А»;

P (EU|A) – условная вероятность ожидаемой полезности КА вида «А» с точки зрения нарушителя, при оценивании которой учитывается возможность незаметного проведения КА.

При этом.

1. Оценки векторов возможных КА, для которых вычисляется оценка вероятности КА на организацию, могут быть получены на основе анализа данных DarkNet, так как нарушители предпочитают использовать известные методы КА, либо адаптировать и дорабатывать их под новую инфраструктуру, чем разрабатывать новые векторы КА.

2. Возможность реализации метода КА и вектора КА, установлена в работе [4, 5, 8, 9], можно оценить в соответствие по следующим формулам

$$Y(t) = \frac{1}{1 + \alpha e^{-\beta t}}, \qquad (1.2)$$

где α, β – параметры модели, называемых s-образными кривыми Перла-Рида.

Согласно исследованиям, проведенным [16] инновация может также развиваться по каскадной модели, описываемой следующей формулой:

$$Y(t) = \begin{cases} \frac{1}{1+\alpha_1 e^{-\beta_1 (t-t_0)}}, \text{ если } t_0 \le t \le t_1, \\ \frac{1}{1+\alpha_1 e^{-\beta_1 (t_1-t_0)}} + \frac{1}{1+\alpha_2 e^{-\beta_2 (t-t_1)}}, \text{ если } t_1 < t \le t_2, \\ \cdots \\ \frac{1}{1+\alpha_1 e^{-\beta_1 (t_1-t_0)}} + \frac{1}{1+\alpha_2 e^{-\beta_2 (t_2-t_1)}} + \cdots + \frac{1}{1+\alpha_n e^{-\beta_n (t-t_{n-1})}}, \text{ если } t_{n-1} < t \le t_n, \end{cases} \qquad (1.3)$$

где

$[t_0, t_1]$ – длительность первого этапа развития инновации;

$]t_1, t_2]$ – длительность второго этапа развития инновации;

…

$]t_{n-1}, t_n]$ – длительность n-го этапа развития инновации.

3. Оценку достаточности ожидаемой полезности КА можно вычислить по следующей формуле, детальное обоснование такой возможности приведено в [4, 5, 8, 9]:

$$EU = (1 - \rho_n) U(W_m + W_j) + \rho_n U(W_m + W_j - F), \qquad (1.4)$$

где $U(\xi)$ – функция полезности, определенная ниже;

P_n – вероятность разоблачения нарушителя (соответственно, вероятность проведения незаметной КА $p_m = 1 - p_n$);

W_m – выгода (прибль) нарушителя в случае успешной реализации КА, с учетом затрат на реализацию КА, определяемая по формуле $W_m = W_{mpj} - C_j$;

C_j – стоимость использованного метода КА;

W_{mpj} – выручка нарушителя в случае успешной реализации КА;

W_j – текущий доход нарушителя от легальной деятельности;

F – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте).

4. Оценку вероятности достаточности ожидаемой полезности КА с точки зрения нарушителя, в которой учитывается возможность проведения незаметной КА, можно рассчитывать по формуле (1.1). При этом для нахождения оценок значений параметров функций (1.4), (1.2), (1.3) достаточно использовать информацию из общедоступных источников.

Модель нарушителя, используемая в методике, и ее влияние на компьютерную атаку

В соответствии с нормативными документами ФСТЭК России [1, 2] при формировании модели угроз необходимо разрабатывать модель нарушителя.

Следуя [1], будем использовать следующую классификацию нарушителей, осуществляющих КА в сети Интернет:

– специальные службы иностранных государств;

– отдельные физические лица («хакеры»);

– конкурирующие организации.

Так как порядок этапов проведения КА не зависит от типа нарушителя, то можно использовать предложенную методологию для всех типов нарушителей, при необходимости, корректируя источники общедоступной информации.

Для подтверждения, данного утверждения, рассмотрим два крайних случая:

– нарушителя, не обладающего знаниями в области ИТ и ИБ (например, школьника или пенсионера);

– нарушителя, обладающего неограниченными ресурсами и возможностями получать знания (например, сотрудника специальной службы иностранного государства).

Нарушитель, не обладающий знаниями в области ИТ и ИБ

К данному типу нарушителей можно отнести, например, школьников и студентов младших курсов. Отличительной особенностью данного типа является не знание законодательства РФ, а также отсутствие легального текущего дохода. Поэтому в (1.4), (1.2) достаточно подставить следующие значения $F_j = 0$, $W_j = 0$.

Кроме того, в случае данного типа нарушителя источник с данными об КА можно заменить с данных с форумов DarkNet на данные из Интернета, например Youtube.

Нарушитель, обладающий неограниченным ресурсам и возможностями получать знания

К данному типу нарушителей следует отнести специальные службы иностранных государств. При определении ожидаемой полезности необходимо учитывать, что величина тяжести наказания F_j зависит не от Уголовного кодекса РФ, но от тяжести последствий для иностранного государства при выявлении его причастности к подобной деятельности. В связи с этим, можно сделать вывод, что для сокрытия своего типа нарушитель будет стараться использовать данные, как и любой другой нарушитель, т.е. методы DarkNet.

Это подтверждает и статистика по оценкам [17], количество совершенно нового ВПО, появившегося в период с 3 квартала 2016 г. по 2 квартал 2018 г., составило менее 10% от общего числа ВПО. Так как для реализации КА используется несколько методов КА, то в части этапов реализации КА данным типом нарушителя будут использоваться методы из общедоступных источников информации. Подтверждением данному высказыванию служит то, что многие специалисты считают КА ВПО Petya, реализованной специальными службами.

Таким образом, при прогнозировании вектора КА необходимо определить модель нарушителя, на основании которой необходимо выбирать наиболее подходящие общедоступные источники информации. Сама методология оценивания вероятностей КА при этом не изменится.

Методика прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя

Прогнозирование динамики развития КА реализуется на этапе теоретической и практической подготовки с точки зрения нарушителя. Расчет вероятности $P(EUA) = P(EU|A)\,P(A)$ реализуется выполнением последовательности действий, представленную на рис. 1.

Пример практического использования методики прогнозирования динамики компьютерной атаки

Проведем прогнозирование тренда КА в КФС на 2019 г., перечень КА для анализа представлен ниже:

– целевые КА на организации КФС;

– нецелевые (спам-атаки) на организации КФС;

– нецелевые КА на клиентов КФС через зараженные популярные сайты;

– нецелевые КА на клиентов КФС с использованием ВПО;

– нецелевые КА на клиентов с использованием социальной инженерии.

Для это будем использовать статистику Центрального банка за 2017, 2018, 2019 годы [17-20], а также данные новостных агрегаторов о КФС [21].

В качестве нарушителя рассмотрим нарушителя, имеющего доступ в DarkNet, но при этом не обладающего неограниченным ресурсом. Для оценки известности метода КА будем использовать статистику DarkNet [4, 5, 8, 9], для оценки заработной платы – легальной выгоды, воспользуемся данными с сайта Superjob [22].

Используя представленную выше методику получаем значения возможности реализации КА в КФС за 2017 и 2018 год в таблицах 1 и 2, соответственно.

Из таблицы 1 видно, что рентабельность целевых КА на КФС может быть оценена как $1/\alpha_j$, и отрицательна. Таким образом, реализация целевых КА на КФС в том виде, что они были в 2017 году в последующие годы не возможна $p(A) – 0$. Расчеты также показывают, что наиболее активно развиваются КА с использованием социальной инженерии. Это объясняется тем, что данный тип КА зачастую требует минимальных знаний в ИТ и ИБ сфере, используя стандартные мошеннические механизмы правонарушителей для получения конфиденциальной информации, тем самым увеличивая число нарушителей, использующих данный тип КА.

Из таблицы 2 видно, что действительно тип целевых КА на КФС существенно изменился: средняя сумма выручки нарушителя сократилась в 12 раз, так как

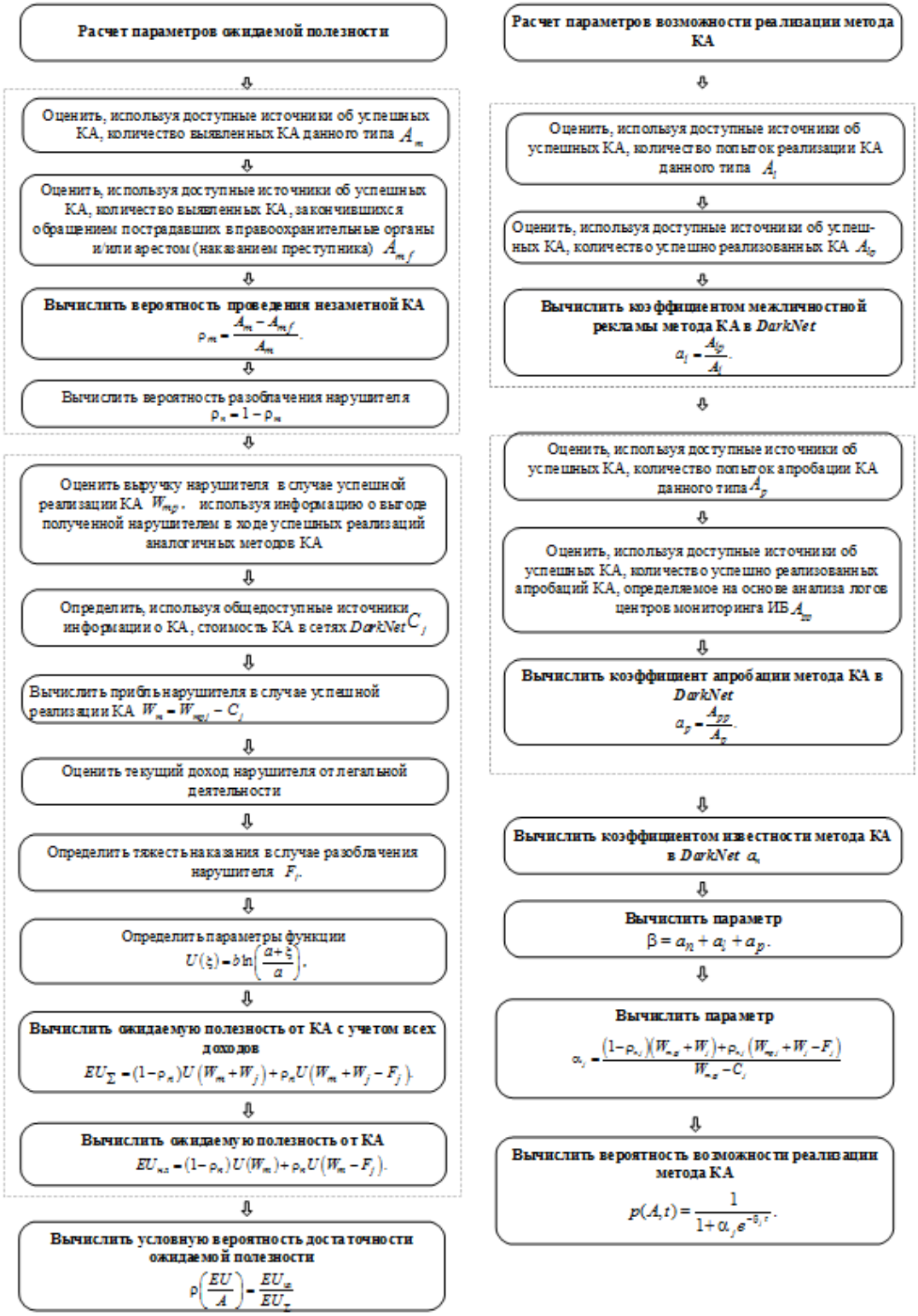


Рис. 1. Методика прогнозирования вектора КА

возросло число попыток замаскировать целевую КА. Однако, видоизменение целевой КА не помогло, так как число уголовных дел в отношении нарушителей, реализовывающих целевые КА на КФС, увеличилось. Логично предположить, что целевые КА на КФС продолжат видоизменяться. В том, числе путем изменения фокуса с КФС на клиентов КФС, о чем свидетельствует увеличение вероятности возможности реали-

Таблица 1

Возможность реализации КА в КФС за 2017 г.

j	Наименование КА	$P(A)$	α_j	β	a_n	a_l	A_{lp}	A_l
1	Целевые КА на организации КФС	0	-3,278	122,872	0,28	0,949	37	39
2	Нецелевые (спам-атаки) на организации КФС	0,499	1,000	112	0,12	1	200000	200000
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,494	1,023	140	0,4	1	481	481
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,499	1,001	112	0,12	1	63582	63582
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,500	0,999	129,996	0,3	0,999	27566	27567

Таблица 2

Возможность реализации КА в КФС за 2018 г.

j	Наименование КА	$P(A)$	α_j	β	a_n	a_l	A_{lp}	A_l
1	Целевые КА на организации КФС	0	-3,941833681	122,44	0,28	0,949	68	72
2	Нецелевые (спам-атаки) на организации КФС	0,499	1,00	112	0,12	1	300000	300000
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,498	1,01	140	0,4	1	2205	2205
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,500	0,999	111,99	0,12	1	1029436	1029438
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,500	1,00	130	0,3	0,999	36000	36000

зации нецелевых КА на клиентов КФС с использованием ВПО.

Возможность реализации КА с использованием социальной инженерии стабильно высока, что говорит, об активном распространении метода КА среди нарушителей. Это объясняется тем, что одни и те же методы социальной инженерии можно неоднократно применять, так как объектом КА зачастую является человек (в случае с другими КА из списка можно использовать специальные автоматические средства ЗИ, у которых возможно оперативно и централизованно поменять конфигурацию).

Анализ прогноза на 2019 год

Вероятность ожидаемой полезности при условии возможности реализации КА в 2017 и 2018 гг., а также прогнозное значение вероятности ожидаемой полезности при условии возможности реализации КА за 2019 г. представлены в таблице 3.

Данные, представленные в таблице 3, позволили дать следующий прогноз трендов КА на 2019 г.

1. Целевые КА на организации КФС в том виде, в котором они реализовывались в 2017 и 2018 гг. в 2019 г. реализовываться не будут, так как вероятность ожидаемой полезности при наличии возможности реализации КА данного вида равна нулю. Это означает, что группы злоумышленников будут видоизменять целевые КА (выгода с реализации КА, метод и т.п.), либо будут переходить на нецелевые КА.

2. Увеличится вероятность реализации нецелевых КА на клиентов КФС Об этом свидетельствует смеще-

Таблица 3

Вероятность ожидаемой полезности за 2017, 2018, 2019 гг.

j	Наименование КА	P(EUA) в 2017 г.	P(EUA) в 2018 г.	P(EUA) в 2019 г.
1	Целевые КА на организации КФС	0	0	0
2	Нецелевые (спам-атаки) на организации КФС	0,120	0,121	0,122
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,071	0,078	0,085
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,106	0,121	0,136
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,092	0,107	0,122

ние фокуса внимания нарушителей с КФС на иные сферы бизнеса, так как КФС сумел построить единую централизованную систему оповещения о новых методах КА и оперативного предупреждения инцидентов ИБ, в том числе блокировки КА на уровне операторов связи. В сфере КФС сформировалась практика обращения в правоохранительные органы и доведения дел до суда, чего не скажешь про иные сферы бизнеса.

3. Минимальное значение вероятности нецелевых КА со сравнению с другими КА из таблицы 3 на клиентов КФС через зараженные популярные сайты по сравнению с другими нецелевыми КА. Это объясняется наличием механизма блокировки КА на уровне операторов связи.

4. Увеличится вероятность реализации нецелевых атак на клиентов КФС с использованием ВПО. Увеличение вероятность КА данного типа может быть связано, с тем, что данные КА технологически похожи на целевые КА, при этом они с точки зрения нарушителя не обладают ограничениями целевых КА.

5. Увеличится вероятность реализации нецелевых атак на клиентов с использованием социальной инженерии. Это объясняется тем, что данный тип КА зачастую требует минимальных знаний в ИТ и ИБ сфере, используя стандартные мошеннические механизмы правонарушителей для получения конфиденциальной информации, тем самым увеличивая число нарушителей, использующих данный тип КА. Одни и те же методы социальной инженерии можно неоднократно применять (рентабельность КА возрастает), так как объектом КА зачастую является человек (в случае с другими КА из списка можно использовать специальные автоматические средства ЗИ, у которых возможно оперативно и централизовано поменять конфигурацию).

В связи с тем, что в отчете Банка России [20, 21] не представлены количественные значения показателей КА за 2019 г., но только качественные описания фактических векторов КА, проведем сравнение спрогнозированной в динамики изменений вероятности КА с аналогичными данными, представленными в отчете.

Выводы

Результаты сравнения показывают, что прогноз динамики изменения векторов КА оказался верным по:

– целевым КА на организации КФС;

– нецелевым (спам-атаки) КА на организации КФС;

– нецелевым КА на клиентов КФС через зараженные популярные сайты;

– нецелевым КА на клиентов КФС с использованием ВПО;

– нецелевым атакам на клиентов с использованием социальной инженерии.

В 2019 г. по данным отчета Банка России:

1. Наблюдалось снижение количества попыток КА на организации КФС. Произошло смещение фокуса внимания злоумышленников с организаций кредитно-финансового сектора на их клиентов. В частности, сохранялась высокая интенсивность распространения нарушителями ВПО класса ransomware (целевых КА), но уже не на КФС.

2. Одним из основных инструментов компьютерных преступников, по-прежнему, оставалось ВПО.

3. В 2019 г. в арсенале злоумышленников появился новый способ обмана жертв -У Банка России появились полномочия по инициированию снятия с делегирования мошеннических интернет ресурсов и построен процесс взаимодействия со всеми участниками процесса разделегирования. (Минимальное время разделегирования доменов фишинговых ресурсов составило 3 часа 3 дня, что стало возможным благодаря появлению дежурной службы, работающий в режиме 24/7/365.)

5. Был осуществлен переход 66% мошеннических ресурсов в юриспруденцию иностранных доменных зон. Что говорит об изменении тренда с нецелевых атак на клиентов КФС через зараженные популярные российские сайты, на западные сайты. (Отметим, что у Банка России нет компетенций на разделегирования фишинговых ресурсов за пределами доменных зон .ru, .рф, .su).

Таким образом, прогноз динамики КА в 2019 г. оказался не противоречащим соответствующим данным Банка России, что подтверждает работоспособность предложенной методики прогнозирования вектора КА.

Выводы

1. Предложена методика прогнозирования векторов КА, позволяющая выявлять тренды развития КА с точки зрения нарушителя.

2. Проведена оценка результатов практической апробации, которая подтвердила, что вектор КА определяется:

2.1. Вероятностью разоблачения нарушителя (вероятность проведения незаметной КА) и тяжестью наказания, для нарушителя. Осуществление защиты от КА возможно за счет изменения восприятия преступником возможностей (в том числе, соотношения между выгодой и потерями) совершения преступления путем повышения возможности разоблачения нарушителя.

2.2. Характеристиками самой КА, в частности, экономичностью и рентабельностью реализации метода КА, наличием рекламы в DarkNet и данными межличностного взаимодействия нарушителей и апробации (совместимости с инфраструктурой атакуемых организаций, простотой реализации, наличием средств ЗИ и методов обнаружения КА).

2.3. На текущий момент доходы от легальной деятельности существенно ниже выручки нарушителя от реализации КА.

Литература

1. Методический документ: Методика оценки угроз безопасности информации: [утвержден ФСТЭК России 5 февраля 2021 г.]. – Доступ из справочно-правовой системы Гарант. – Текст: электронный.

2. Банк данных угроз БИ ФСТЭК России: [сайт]. – URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2019). – Текст: электронный.

3. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2021. — Т. 28. № 2. — С. 6-20.

4. Computer attack`s probability function / Makarova O., Porshnev S. // Lecture Notes in Electrical Engineering. Advances in Automation II. — 2021. — Vol. 729. — pp. 560-568.

5. Оценивание вероятностей компьютерных атак на основе функций / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 2. — С. 86-96.

6. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information / Makarova Olga; Porshnev Sergey // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2020. — No. 9117676 — pp. 593-596.

7. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 1. — С. 6-18.

8. Determining the Choice of Attack Methods Approach / Makarova Olga // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. — 2021. — No. 9455072 — pp. 399-402.

9. Mathematical Model of the Computer Attack Implementation Possibility by an Intruder / Makarova Olga; Porshnev Sergey // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455045 — pp. 395-398.

10. Simulation of Computer Attack Scenarios for Industrial Robots from the Point of Intruder View / O. Makarova and M. Lihota // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455052 — pp. 474-477.

11. Белокурова, Е. В. Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем / Е. В. Белокурова, А. А. Дерканосова, А. А. Змеев [и др.]. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2015. – 6 с. – URL: https://cyberleninka.ru/article/n/sposoby-otsenki-ugroz-bezopasnosti-konfidentsialnoy-informatsii-dlya-informatsionno-telekommunikatsionnyh-sistem/viewer (дата обращения: 08.07.2021).

12. Налини М. Digital risk management for data attacks against state evaluation = Цифровое управление рисками для атак на данные против оценки состояния / М. Налини, А. Чакрам // International Journal of Innovative Technology and Exploring Engineering (IJITEE). – 2020. – № 88. – DOI: https://doi.org/10.35940/ijitee.I1130.0789S419. – Текст: электронный (дата обращения: 08.07.2021).

13. Зикратов И. А. Evaluation of information security in cloud computing based on the bayesian approach = Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода / И. А. Зикратов, С. В. Одегов. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2012. – 6 с. – URL: https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda/viewer (дата обращения: 08.07.2021).

14. Скворцова М. А. Разработка системы поддержки принятия решения для оценки рисков и угроз национальной безопасности / М. А. Скворцова, В. И. Терехов. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2018. – 11 с. – URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-podderzhki-prinyatiya-resheniya-dlya-otsenki-riskov-i-ugroz-natsionalnoy-bezopasnosti/viewer (дата обращения: 08.07.2021).

15. Кузнецов Н. А. Модель автоматизированной системы оптимизации параметров управления рисками в терминах угроз, уязвимостей и резервов / Н. А. Кузнецов, А. А. Мозоль. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2019. – 7 с. – URL: https://cyberleninka.ru/article/n/model-avtomatizirovannoy-sistemy-optimizatsii-parametrov-upravleniya-riskami-v-terminah-ugroz-uyazvimostey-i-rezervov/viewer (дата обращения: 08.07.2021).

16. Хагерстранд Т. Innovation diffusion as a spatial process= Дифуззия инновации как пространственный процесс / Т. Хагерстранд // Chicago, University of Chicago Press. – 1967. – DOI: https://doi.org/10.1111/j.1538-4632.1969.tb00626.x. – Текст: электронный (дата обращения: 08.07.2021).

17. Чои С. A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments = Исследование по анализу информации о поведении вредоносного кода для прогнозирования угроз безопасности в новых средах / С. Чои, Т. Ли, Д. Квак // KSII Transactions on Internet and Information Systems. – 2019. – № 13 (3). – С. 1611–1625. – DOI: https://doi.org/10.3837/tiis.2019.03.028. – Текст: электронный (дата обращения: 08.07.2021).

18. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 01.09.2017 – 31.08.2018. – Текст. Изображение: электронные // Банк России: [сайт]. – 2018. – URL: http://www.cbr.ru/Collection/Collection/File/32088/survey_0917_0818.pdf (дата обращения: 27.04.2020).

19. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году. – Текст. Изображение: электронные // Банк России [сайт]. – 2018. – URL: http://www.cbr.ru/collection/collection/file/32085/dib_2018_20190704.pdf (дата обращения: 27.04.2020).

20. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 01.09.2018 – 31.08.2019. – Текст. Изображение: электронные // Банк России: [сайт]. – 2019. – URL: http://www.cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF (дата обращения: 17.11.2019).

21. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах. – Текст. Изображение: электронные // Банк России: [сайт]. – 2021. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 08.07.2021).

22. Зарплатный индекс Superjob сферы «Информационные технологии». – Текст. Изображение: электронные // SuperJob: [сайт]. – 2017. – URL: https://www.superjob.ru/paymentindex/it/#/31 (дата обращения: 08.07.2021).

23. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2021. — Т. 28. № 2. — С. 6-20. (1,5 п.л. / 0,75 п.л.)

References

1 Metodicheskiy dokument: Metodika otsenki ugroz bezopasnosti informatsii: [utverzhden FSTEK Rossii 5 fevralya 2021 g.]. – Dostup iz spravochno-pravovoy sistemy Garant. – Tekst: elektronnyy.

2 Bank dannykh ugroz BI FSTEK Rossii: [sayt]. – URL: https://bdu.fstec.ru/ (data obrashcheniya: 17.11.2019). – Tekst: elektronnyy.

3 Opredeleniye parametrov, vliyayushchikh na vozmozhnost' realizatsii komp'yuternoy ataki narushitelem / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2021. — T. 28. № 2. — S. 6-20.

4 Computer attack`s probability function / Makarova O., Porshnev S. // Lecture Notes in Electrical Engineering. Advances in Automation II. — 2021. — Vol. 729. — pp. 560-568.

5 Otsenivaniye veroyatnostey komp'yuternykh atak na osnove funktsiy / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2020. — T. 27. № 2. — S. 86-96.

6 Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information / Makarova Olga; Porshnev Sergey // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2020. — No. 9117676 — pp. 593-596.

7 Otsenivaniye veroyatnostey komp'yuternykh atak na osnove metoda analiza iyerarkhiy s dinamicheskimi prioritetami i predpochteniyami / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2020. — T. 27. № 1. — S. 6-18.

8 Determining the Choice of Attack Methods Approach / Makarova Olga // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. — 2021. — No. 9455072 — pp. 399-402.

9 Mathematical Model of the Computer Attack Implementation Possibility by an Intruder / Makarova Olga; Porshnev Sergey // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455045 — pp. 395-398.

10 Simulation of Computer Attack Scenarios for Industrial Robots from the Point of Intruder View / O. Makarova and M. Lihota // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455052 — pp. 474-477.

11 Belokurova, Ye. V. Sposoby otsenki ugroz bezopasnosti konfidentsial'noy informatsii dlya informatsionno-telekommunikatsionnykh sistem / Ye. V. Belokurova, A. A. Derkanosova, A. A. Zmeyev [i dr.]. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2015. – 6 s. – URL: https://cyberleninka.ru/article/n/sposoby-otsenki-ugroz-bezopasnosti-konfidentsialnoy-informatsii-dlya-informatsionno-telekommunikatsionnyh-sistem/viewer (data obrashcheniya: 08.07.2021).

12 Nalini M. Digital risk management for data attacks against state evaluation = Tsifrovoye upravleniye riskami dlya atak na dannyye protiv otsenki sostoyaniya / M. Nalini, A. Chakram // International Journal of Innovative Technology and Exploring Engineering (IJITEE). – 2020. – № 88. – DOI: https://doi.org/10.35940/ijitee.I1130.0789S419. – Tekst: elektronnyy (data obrashcheniya: 08.07.2021).

13 Zikratov I. A. Evaluation of information security in cloud computing based on the bayesian approach = Otsenka informatsionnoy bezopasnosti v oblachnykh vychisleniyakh na osnove bayyesovskogo podkhoda / I. A. Zikratov, S. V. Odegov. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2012. – 6 s. – URL: https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda/viewer (data obrashcheniya: 08.07.2021).

14 Skvortsova M. A. Razrabotka sistemy podderzhki prinyatiya resheniya dlya otsenki riskov i ugroz natsional'noy bezopasnosti / M. A. Skvortsova, V. I. Terekhov. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2018. – 11 s. – URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-podderzhki-prinyatiya-resheniya-dlya-otsenki-riskov-i-ugroz-natsionalnoy-bezopasnosti/viewer (data obrashcheniya: 08.07.2021).

15 Kuznetsov N. A. Model' avtomatizirovannoy sistemy optimizatsii parametrov upravleniya riskami v terminakh ugroz, uyazvimostey i rezervov / N. A. Kuznetsov, A. A. Mozol'. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2019. – 7 s. – URL: https://cyberleninka.ru/article/n/model-avtomatizirovannoy-sistemy-optimizatsii-parametrov-upravleniya-riskami-v-terminah-ugroz-uyazvimostey-i-rezervov/viewer (data obrashcheniya: 08.07.2021).

16 Khagerstrand T. Innovation diffusion as a spatial process= Difuzziya innovatsii kak prostranstvennyy protsess / T. Khagerstrand // Chicago, University of Chicago Press. – 1967. – DOI: https://doi.org/10.1111/j.1538-4632.1969.tb00626.x. – Tekst: elektronnyy (data obrashcheniya: 08.07.2021).

17 Choi S. A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments = Issledovaniye po analizu informatsii o povedenii vredonosnogo koda dlya prognozirovaniya ugroz bezopasnosti v novykh sredakh / S. Choi, T. Li, D. Kvak // KSII Transactions on Internet and Information Systems. – 2019. – № 13 (3). – S. 1611–1625. – DOI: https://doi.org/10.3837/tiis.2019.03.028. – Tekst: elektronnyy (data obrashcheniya: 08.07.2021).

18 Otchet tsentra monitoringa i reagirovaniya na komp'yuternyye ataki v kreditno-finansovoy sfere departamenta informatsionnoy bezopasnosti Banka Rossii 01.09.2017 – 31.08.2018. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii: [sayt]. – 2018. – URL: http://www.cbr.ru/Collection/Collection/File/32088/survey_0917_0818.pdf (data obrashcheniya: 27.04.2020).

19 Obzor osnovnykh tipov komp'yuternykh atak v kreditno-finansovoy sfere v 2018 godu. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii [sayt]. – 2018. – URL: http://www.cbr.ru/collection/collection/file/32085/dib_2018_20190704.pdf (data obrashcheniya: 27.04.2020).

20 Otchet tsentra monitoringa i reagirovaniya na komp'yuternyye ataki v kreditno-finansovoy sfere departamenta informatsionnoy bezopasnosti Banka Rossii 01.09.2018 – 31.08.2019. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii: [sayt]. – 2019. – URL: http://www.cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF (data obrashcheniya: 17.11.2019).

21 Osnovnyye tipy komp'yuternykh atak v kreditno-finansovoy sfere v 2019–2020 godakh. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii: [sayt]. – 2021. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (data obrashcheniya: 08.07.2021).

22 Zarplatnyy indeks Superjob sfery «Informatsionnyye tekhnologii». – Tekst. Izobrazheniye: elektronnyye // SuperJob: [sayt]. – 2017. – URL: https://www.superjob.ru/paymentindex/it/#/31 (data obrashcheniya: 08.07.2021).

23 Opredeleniye parametrov, vliyayushchikh na vozmozhnost' realizatsii komp'yuternoy ataki narushitelem / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2021. — T. 28. № 2. — S. 6-20. (1,5 p.l. / 0,75 p.l.)

МАКАРОВА Ольга Сергеевна, кандидат технических наук, руководитель регионального представительства в Уральском федеральном округе кампании «ИнфоТекс», старший преподаватель Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 2, e-mail: o.s.makarova@urfu.ru

MAKAROVA Olga Sergeevna, Candidate of Technical Sciences, Head of the Regional Representative Office of the InfoTeKS company in the Ural Federal District, Senior Lecturer of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin», 620002, Yekaterinburg, st. Mira, 32, e-mail: o.s.makarova@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. e-mail: s.v.porshnev@urfu.ru

УДК 004.891.3 Вестник УрФО № 1(43) / 2022, с. 74–83

Старун И.Г., Югансон А.Н.

DOI: 10.14529/secur220109

РАЗРАБОТКА АЛГОРИТМА КЛАССИФИКАЦИИ ШИФРОВАННОГО ТРАФИКА НА ОСНОВЕ LIGHTGBM[1]

С ростом количества угроз в сети Интернет растет и популярность технологии шифрования. При этом часть полезной нагрузки в результате шифрования перестает быть видимой. Для эффективной реализации многих сценариев обеспечения ИБ требуется идентификация протокола шифрования и типа приложения, поэтому актуальной становится задача классификации шифрованного трафика. Лидирующее по популярности место среди способов классификации занимает машинное обучение. При этом наилучшие результаты достигаются с помощью глубокого обучения, но этот подход имеет и обратную сторону – высокую вычислительная сложность, требующую больших ресурсов для работы в режиме реального времени. Поэтому в данном исследовании внимание сфокусировано на классификации шифрованного трафика с помощью классических алгоритмов машинного обучения. Рассмотрена первая часть сценария классификации – разделение трафика на VPN и non-VPN. Предложен алгоритм поиска оптимальной модели с помощью AutoML. В результате получена модель на основе алгоритма LightGBM. Эксперименты проводились на основе известного набора данных ISCXVPN2016. Оценка качества на тестовой выборке показала следующие результаты: Accuracy = 94.08%, Precision = 92.85%, Recall = 96.07%, F1-measure = 94.43%. Эти оценки превосходят предыдущие решения по 3 из 4 ключевых метрик классификации.

Ключевые слова: *шифрованный трафик, классификация трафика, машинное обучение, VPN, AutoML, градиентный бустинг, LightGBM, информационная безопасность.*

Starun I.G., Iuganson A.N.

DEVELOPMENT OF THE ALGORITHM FOR CLASSIFICATION OF ENCRYPTED TRAFFIC BASED ON LIGHTGBM

As the number of threats on the Internet grows, so does the popularity of encryption technology. In this case, part of the payload because of encryption ceases to be visible. The effective implementation of many information security scenarios requires identification of the encryption protocol and application type, so the task of classifying encrypted traffic becomes relevant. Machine learning is one of the most popular classification methods. At the same time, the best results are achieved using deep learning, but this approach also has a downside - high computational complexity, which requires large resources to work in real time. Therefore, in this study, attention is focused on the classification of encrypted traffic using classical machine learning algorithms. The first part of the classification scenario is considered – the division of traffic into VPN and non-VPN. An algorithm for finding the optimal model using AutoML is proposed. As a result, a model based on the LightGBM algorithm was obtained. The experiments were carried out on the well-known ISCXVPN2016 dataset. The quality assessment on the test sample showed the following results: Accuracy = 94.08%, Precision = 92.85%, Recall = 96.07%, F1-measure = 94.43%. These scores outperform previous solutions on 3 out of 4 key classification metrics.

Keywords: *encrypted traffic, traffic classification, machine learning, VPN, AutoML, gradient boosting, LightGBM, information security.*

[1] Работа выполнена в Университете ИТМО при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках проекта 2019-0898 «Многоуровневое управление сложными техническими системами».

Введение

Количество шифрованного трафика в Интернете растет от года к году, а доля использования HTTPS протокола приближается к 90% и продолжает расти. Такая популярность шифрования связана с возросшей потребностью в обеспечении информационной безопасности, а использование технологии VPN также дает пользователям возможность обходить местные блокировки ресурсов и анонимизировать свой цифровой след [1, 16–17]. В результате шифрования часть сведений перестает быть видимой, что усложняет задачу классификации трафика. Для эффективной реализации многих сценариев защиты от угроз ИБ в сетях при анализе сетевого трафика зачастую требуется идентификация протокола шифрования и типа приложения, к которому этот трафик относится. Такая классификация полезна не только для предотвращения атак и обнаружения аномалий, но и для анализа поведения пользователя, управления трафиком, контроля производительности приложений [4, 13].

Выделяют 3 подхода к классификации сетевого трафика – на основе анализа портов [5, 6], путем анализа полезной нагрузки [5, 7–8] и с помощью машинного обучения. Первый сопоставляет каждое приложение с соответствующим номером порта (например, порт 20 для FTP). Актуальность такого подхода заметно снизилась из-за внедрения динамического распределения портов. Второй способ слабо подходит для шифрованного трафика, так как выделить полезную нагрузку после шифрования практически невозможно. Поэтому наиболее популярным подходом к классификации шифрованного трафика в последние годы стало использование машинного обучения. Его можно разделить на 2 большие группы: классификация на основе классических алгоритмов и глубокое обучение (deep learning).

Широкое применение для решения задачи классификации шифрованного трафика приобрели методы глубокого обучения с помощью нейросетей. С их помощью достигаются наилучшие результаты. Однако у их использования есть и обратная сторона – высокая вычислительная сложность. Если крупные корпорации и компании могут себе позволить использование нейросетей для анализа трафика, то для малого и среднего бизнеса зачастую это становится непозволительной роскошью. Следовательно, при выборе метода анализа трафика необходимо достичь баланса между качеством классификации и вычислительной сложностью [2].

Помимо глубокого обучения, задачи классификации решаются с помощью классических алгоритмов машинного обучения, таких как логистическая регрессия, деревья решений, случайный лес, градиентный бустинг и других. Модели на основе этих алгоритмов значительно менее требовательны к вычислительным ресурсам, поэтому могут использоваться пользователями с более низким порогом входа.

Предметом настоящего исследования является классификация шифрованного трафика с помощью классических алгоритмов машинного обучения без использования deep learning. Предложен алгоритм поиска оптимальной модели с применением инструментов AutoML для тонкой настройки алгоритма градиентного бустинга LightGBM и выбора признаков на основе оценки их влияния на итоговую модель.

Дальнейшая часть статьи организована следующим образом. Раздел 2 представляет собой обзор предыдущих работ. В разделе 3 описывается набор данных, на основе которого проводились эксперименты. Четвертый раздел посвящен методологии исследования. В разделе 5 представлены результаты эксперимента. Шестая часть работы отведена под обсуждение полученных результатов и их сравнение с предыдущими решениями. В заключительной части подводятся итоги и обсуждаются дальнейшие перспективы.

Обзор предыдущих работ

Первая статья, в которой упоминается датасет ISCXVPN2016, была опубликована в 2016 году. Авторы сгенерировали большой объем шифрованного трафика, извлекли из него временные признаки и на их основе построили классификаторы. В качестве метрик были выбраны Precision и Recall. В задаче разделения трафика на VPN и non-VPN лучший результат был достигнут при использовании алгоритмов KNN и C4.5 – 0.89–0.9 в зависимости от вида трафика [9].

Большое количество работ посвящено классификации с помощью глубокого обучения [18-23]. Целью настоящего исследования является повышение качества классификации шифрованного трафика в условиях ограниченных вычислительных мощностей, поэтому было принято решение отказаться от использования нейронных сетей. К тому же существует мнение, что высокие показатели, демонстрируемые нейронными сетями, связаны с их способностью к адаптации к конкретному набору данных [15], что затрудняет масштабирование и перенос модели в новые условия, так как при этом результаты могут значительно упасть. Однако среди подобных работ отдельно стоит отметить статью [3], в которой авторы первыми предложили использовать AutoML для поиска оптимального решения данной задачи. Они применили его для получения наиболее эффективной архитектуры нейронной сети. В настоящем исследовании предложенный подход был адаптирован для тонкой настройки гиперпараметров модели.

В статье [10] авторы сосредоточились на второй части задачи классификации шифрованного трафика – идентификации приложения, сгенерировавшего шифрованный трафик, уже после разделения на VPN и non-VPN. В качестве основной метрики была ис-

пользована доля правильных ответов (Accuracy), а наилучшие результаты показали алгоритмы на основе градиентного бустинга – 89,03% для VPN и 93,19% для non-VPN.

В работе [11] авторы поднимают тему эффективного отбора признаков (Feature selection) и сокращения размерности для снижения вычислительной сложности итоговых моделей. С этой целью использован метод анализа основных компонентов (PCA) и метод опорных векторов (SVM) для выбора признаков из набора данных. Другой подход к сокращению сложности вычислений рассмотрен в [12]. Авторы предложили предварительно отбирать ключевые признаки методами дисперсионного анализа (ANOVA) и опорных векторов (SVM).

Переход от тяжелых нейронных сетей к усовершенствованной предобработке данных (временных признаков) предложен в статье [13]. Авторы предварительно используют метод DSSR для перемасштабирования временных диапазонов, чтобы затем использовать стандартные классификаторы. В комбинации с корреляционным анализом для выбора итогового набора признаков получены результаты, значительно превышающие предшественников. Основным недостатком предложенного метода является то, что он может преобразовывать признаки только поблочно, что вызывает задержку обнаружения, зависящую от длины окна. К тому же требует отдельного внимания вопрос утечки информации (Data leakage) о распределении в тестовой выборке в обучающий набор, так как в исследовании сначала реализовано преобразование данных, а уже затем разделение на Train и Test.

В одной из последних на момент проведения исследования работ [14] реализована комбинация нескольких методов машинного обучения для получения оптимальной модели. Авторы сначала нормализуют данные, затем выбирают 15 признаков, оказывающих наибольшее значение на результат. Затем данные балансируются, чтобы избежать проблемы несбалансированности классов, после чего подбираются оптимальные гиперпараметры модели. Лучший результат был получен с помощью алгоритма XGBoost – каждая из метрик precision, recall, accuracy и f1-measure немного превысила 93%.

Описание набора данных

Как было сказано выше, набор данных ISCXVPN2016 был представлен и описан в исследовании [9]. Чтобы создать репрезентативный набор данных, авторы зафиксировали реальный трафик, созданный участниками лаборатории. Они создали учетные записи для пользователей Алисы и Боба, чтобы они могли пользоваться такими сервисами, как Skype, Facebook и т. д. Полный список из 7 захваченных протоколов и приложений представлен в таблице 1. Для каждого из них трафик был сгенерирован двумя способами: путем обычного сеанса и сеанса через VPN. Таким образом, был получен набор из 14 категорий трафика общим объемом 28 ГБ. Для захвата использовались утилиты Wireshark и tcpdump.

Таблица 1

Перечень захваченных протоколов и приложений для ISCXVPN2016

Трафик	Содержимое
Web browsing	Firefox и Chrome
Email	SMPTS, POP3S и IMAPS
Chat	ICQ, AIM, Skype, Facebook и Hangouts
File Transfer	Skype, FTPS и SFTP с помощью Filezilla и внешней службы
Streaming	Vimeo и Youtube
VoIP	Facebook, Skype и голосовые звонки Hangouts (длительностью 1 час)
P2P	uTorrent и Transmission (Bittorrent)

Сгенерированный трафик далее рассматривался как двунаправленный поток, где под потоком следует понимать последовательность пакетов с одинаковыми значениями исходного IP-адреса, IP-адреса назначения, исходного порта, порта назначения и протокола (TCP или UDP). С помощью программы ISCXFlowMeter потоки разбивались на отрезки одинаковой временной продолжительности (timeout), по которым затем рассчитывались значения признаков. Полный список полученных функций и их описание представлено в таблице 2. Всего было использовано 4 значения timeout – 15, 30, 60 и 120 секунд.

Затем в оригинальной статье авторы выделили и протестировали 2 сценария классификации:

1. Сценарий А: сначала реализуется классификация трафика на VPN и non-VPN (сценарий А1), а затем проводится раздельная классификация этих двух видов трафика по типам приложений и протоколов (сценарий А2).

2. Сценарий Б: единый набор трафика сразу классифицируется по типам приложений и протоколов без предварительного разделения на VPN и non-VPN.

Настоящее исследование сфокусировано только на сценарии А1, а именно на задаче разделения шиф-

Таблица 2

Список временных признаков в ISCXVPN2016

Группа признаков	Признаки	Описание
Duration	duration	Длительность потока
Fiat (Forward Inter Arrival Time)	total_fiat, max_fiat, min_fiat, mean_fiat,	Время между двумя пакетами, отправляемыми в прямом направлении (всего, минимальное, максимальное, среднее)
Biat (Backward Inter Arrival Time)	total_biat, max_biat, min_biat, mean_biat	Время между двумя пакетами, отправляемыми в обратном направлении (всего, минимальное, максимальное, среднее)
Flowiat (Flow Inter Arrival Time)	mean_flowiat, max_flowiat, min_flowiat, std_flowiat	Время между двумя пакетами, отправленными в любом направлении (среднее, минимальное, максимальное, стандартное отклонение)
Active	mean_active, max_active, min_active, std_active	Время, в течение которого поток был активен до перехода в режим ожидания (среднее, минимальное, максимальное, стандартное отклонение)
Idle	mean_idle, max_idle, min_idle, std_idle	Время, в течение которого поток простаивал до того, как стал активным (среднее, минимальное, максимальное, стандартное отклонение)
Fb-psec	FlowBytesPerSecond	Количество байт потока в секунду
Fp-psec	FlowPktsPerSecond	Количество пакетов потока в секунду

рованного трафика на VPN и non-VPN. Этот этап классификации напрямую влияет на общий процесс, так как чем точнее предварительная классификация трафика, тем качественнее данные, поступающие на вход сценария A2.

Этапы проведения исследования (методология)

Для проведения исследования был использован язык программирования Python 3.8. Всего для получения итоговой модели классификации было выполнено 7 шагов:

1. Разделение исходного набора данных на обучающую и тестовую выборки в соотношении 80:20 с помощью функции train_test_split из библиотеки sklearn. При этом проводилась стратификация по целевому признаку, чтобы представленность каждого класса в выборках была сопоставимой. Тестовая выборка в дальнейшем использовалась только на этапе оценки итоговой модели.

2. Стандартизация данных с помощью StandartScaler по формуле (1):

$$x_{norm_i} = \frac{(x_i - x_{mean})}{SD}, \quad (1)$$

где x_i – исходное значение признака в выборке, x_{mean} – среднее значение признака в обучающем наборе, SD – стандартное отклонение признака в обучающем наборе.

3. Поиск оптимальной модели и ее гиперпараметров с помощью LightAutoML. Рассматривались такие модели, как CatboostClassifier, LGBMClassifier и линейные классификаторы. При этом комбинация нескольких моделей (бэггинг) не рассматривалась, чтобы не слишком усложнять модель.

4. Выбор признаков (Feature selection) с помощью LightAutoML. Использовался быстрый метод, который рассчитывает важность функций по встроенному методу LGBM.

5. Подбор оставшихся гиперпараметров. Этот шаг необходим ввиду того, что инструмент LightAutoML для экономии времени уделяет недостаточно внимания подбору некоторых ключевых параметров, таких как количество деревьев (num_estimators), скорость обучения (learning_rate) и максимальная глубина дерева (max_depth).

5. Компоновка итоговой модели и ее обучение на тренировочной выборке. Выбор оптимальной границы разделения классов (threshold).

6. Оценка качества итоговой модели на тестовой выборке. В качестве метрик использовались классические метрики для задачи классификации, которые уже упоминались в работе: Accuracy, Precision, Recall и F1-Measure.

Результаты исследования

Как и в большинстве предыдущих исследований, для сценария A1 наиболее качественные решения были получены при обработке потоков с таймаутом в 15 секунд.

Таблица 3

Оптимальные гиперпараметры модели LGBMClassifier

Гиперпараметр	Значение
feature_fraction	0.6872700594236812
num_leaves	244
bagging_fraction	0.8659969709057025
min_sum_hessian_in_leaf	0.24810409748678125
reg_alpha	2.5361081166471375e-07
reg_lambda	2.5348407664333426e-07
learning_rate	0.15
max_depth	50
num_estimators	2300

Наилучшие результаты были продемонстрированы моделью градиентного бустинга LGBMClassifier. Оптимальные гиперпараметры для модели представлены в таблице 3.

При этом оптимальная граница разделения классов на обучающем наборе составила 0.42. В дальнейшем она была использована при оценке итоговой модели.

Оценка важности признаков (feature importance) для модели представлена на рис. 1. Из исходных 25 признаков было принято решение оставить первые 17 по важности, так как в этом случае достигались лучшие метрики на обучающем наборе.

Итоговый перечень выбранных для модели признаков выглядит следующим образом: 'duration', 'total_fiat', 'total_biat', 'min_fiat', 'min_biat', 'max_fiat', 'max_biat', 'mean_fiat', 'mean_biat', 'flowPktsPerSecond', 'flowBytesPerSecond', 'min_flowiat', 'mean_active', 'mean_idle', 'max_flowiat', 'mean_flowiat' и 'std_flowiat'.

Для оценки качества модели использовались

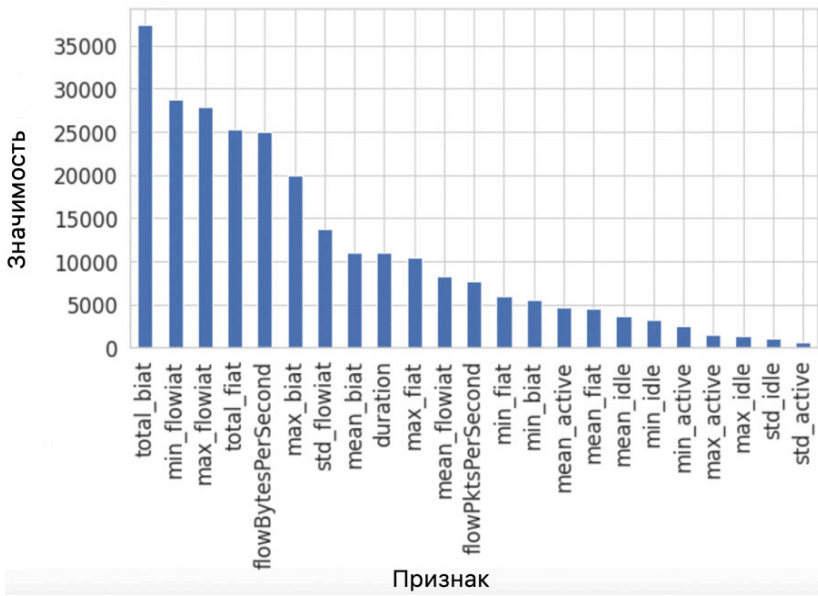


Рис. 1. Оценка важности признаков для модели встроенным методом LGBM

стандартные метрики классификации – Accuracy (2), Precision (3), Recall (4) и F1-measure (5).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (2)$$

$$Precision = \frac{TP}{TP + FP}, \quad (3)$$

$$Accuracy = \frac{TP}{TP + FN}, \quad (4)$$

$$F_1 - measure = \frac{Precision * Recall}{Precision + Recall}, \quad (5)$$

где TP – True Positive – количество истинно-положительных ответов, TN – True Negative – количество истинно-отрицательных ответов, FN – False Negative – количество ложноотрицательных ответов, FP – False Positive – количество ложноположительных ответов.

Оценка качества модели на тестовой выборке

показала следующие результаты: Accuracy = 94.08%, Precision = 92.85%, Recall = 96.07%, F1-measure = 94.43%.

ROC-кривая итоговой модели представлена на рисунке 2. Площадь под графиком, или AUC, составляет 0.98, что что эквивалентно доле пар объектов противоположных классов (VPN и non-VPN), которые модель верно упорядочила.

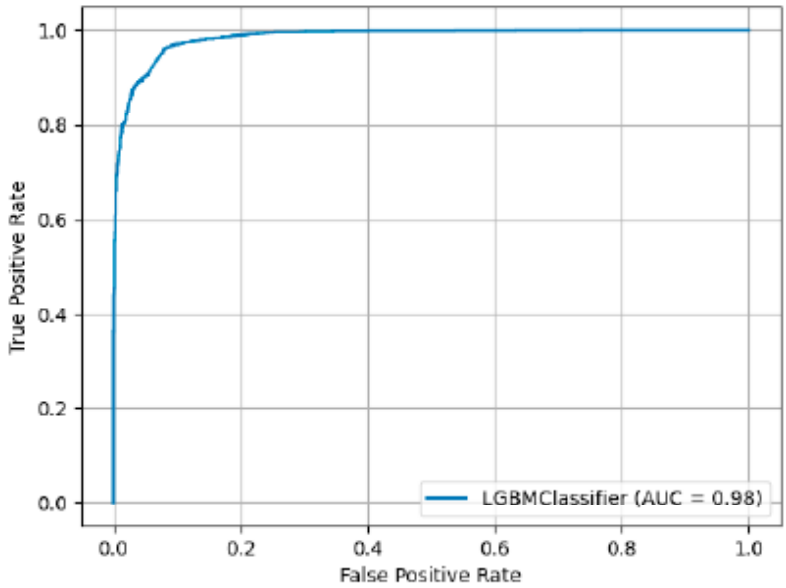


Рис. 2. ROC-AUC кривая полученной модели

Таблица 4

Сравнение качества классификации с другими решениями

Исследование	Год	Количество признаков	Accuracy	Precision	Recall	F1-measure
[9]	2016	25	-	90.6%	-	-
[3]	2021	25	-	85.21%	84.91%	85.57%
[10]	2021	8	88%	-	-	-
[14]	2021	15	93.02%	93.04%	93.02%	93.03%
Настоящее исследование	2022	17	94.09%	92.85%	96.07%	94.43%

Обсуждение результатов

Сравнение качества классификации предложенной модели с другими решениями без использования глубокого обучения представлено в таблице 4 и на рис. 3. Прочерки в таблице и пустые колонки на графике означают отсутствие данных.

Таким образом, предложенное решение превосходит предыдущие исследования по 3 из 4 ключевых метрик (Accuracy, Recall и F1-measure), незначительно уступая лишь по метрике Precision работе [14]. Полученная модель демонстрирует лучшую долю правильных ответов, а также лучшее гармоническое среднее между точностью и полнотой.

Важно отметить, что в зависимости от приоритетов классификации можно влиять на метрики Precision и Recall с помощью сдвига границы классификации. Предложенное в работе значение threshold, равное 0.42, можно считать оптимальным для полученной модели.

Еще одно интересное замечание связано с тем, как перекликается выбор признаков в текущем исследовании с работой [14]. Там авторы остановились на 15 лучших признаках, из которых 13 входят в полученный в настоящей работе итоговый список. При этом их эксперименты показали, что группы признаков Active и Idle не оказывают значительного влияния на качество классификации, в то время как в текущем исследовании было принято включить их в итоговую модель как значимые.

Заключение

Предложенный в работе алгоритм подбора оптимальной модели для классификации шифрованного трафика показал высокие результаты, опережая по большинству ключевых метрик предыдущие решения на основе классического машинного обучения. Это говорит о высокой эффективности AutoML подхода для поиска оптимальных параметров алгоритмов машин-

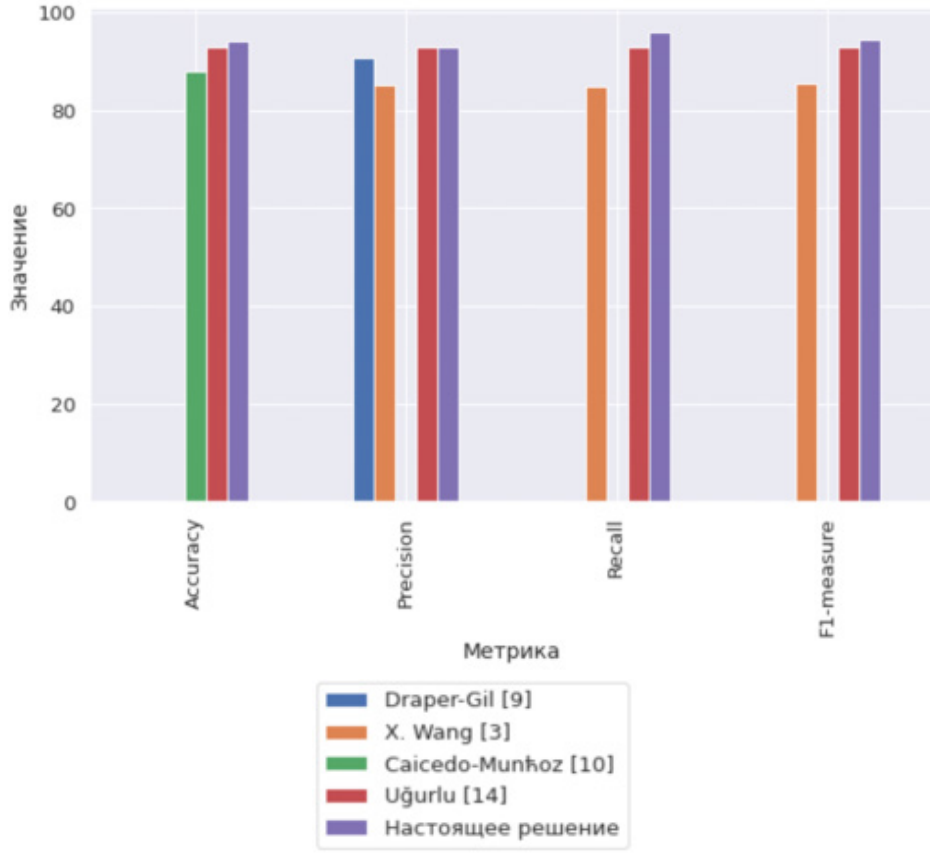


Рис. 3. Сравнение с существующими решениями

ного обучения и выбора признаков. Еще одной ключевой особенностью разработанного решения является выбор алгоритма LightGBM в качестве классификатора. В предыдущих работах также фигурировали алгоритмы на основе градиентного бустинга, но предпочтение отдавалось моделям CatBoost и XGBoost.

Дальнейшие исследования будут сосредоточены на второй части сценария A для идентификации конкретного приложения или протокола, сгенерировавшего шифрованный трафик.

Литература

1. Старун И.Г., Югансон А.Н., Гатчин Ю.А. Построение математической модели расчета комплексной оценки VPN: ст. - Вестник ТГТУ, том. 25, выпуск 4, 2019, с. 535-546.

2. Lu,B.; Luktarhan,N.; Ding, C; Zhang,W. ICLSTM: Encrypted Traffic Service Identification Based on Inception-LSTM Neural Network. Symmetry, 2021, 13, 1080. https:// doi.org/10.3390/sym13061080

3. X. Wang et al., "Evolutionary Algorithm-Based and Network Architecture Search-Enabled Multiobjective Traffic Classification," in IEEE Access, vol. 9, pp. 52310-52325, 2021

4. B. Yamansavascilar, M. A. Guvensan, A. G. Yavuz, and M. E. Karsligil, "Application identification via network traffic classification", In: Proc. of 2017 Int. Conf. Comput. Netw. Commun. ICNC 2017, pp. 843–848, 2017.

5. Megantara, A.A., Ahmad, T. ANOVA-SVM for Selecting Subset Features in Encrypted Internet Traffic Classification (2021) International Journal of Intelligent Engineering and Systems, 14 (2), pp. 536-546.

6. G. Cheng and S. Wang, "Traffic classification based on port connection pattern", In: Proc. of 2011 Int. Conf. Comput. Sci. Serv. Syst. CSSS 2011 - Proc., pp. 914–917, 2011.

7. H. K. Lim, J. B. Kim, K. Kim, Y. G. Hong, and Y. H. Han, "Payload-based traffic classification using multi-layer LSTM in software defined networks", Appl. Sci., Vol. 9, No. 12, 2019.

8. F. Dehghani, N. Movahhedinia, M. R. Khayyambashi, and S. Kianian, "Real-time traffic classification

based on statistical and payload content features", In: Proc. of - 2010 2nd Int. Work. Intell. Syst. Appl. ISA 2010, pp. 26–29, 2010.

9. G. Draper-Gil, A. H. Lashkari, M. Mamun, and A. A. Ghorbani,"Characterization of encrypted and VPN traffic using time-related features," in Proc. 2nd Int. Conf. Inf. Syst. Security Privacy, 2016,pp. 407–414

10. Caicedo-Munћoz JA, Espino AL, Corrales JC, RendoћЬn A.QoS-Classifier for VPN and Non-VPN tranћAic based on time-related features.Computer Networks 2018; 144: 271-279. doi: 10.1016/j.comnet.2018.08.008

11. A. Saber, B. Fergani, and M. Abbas, "Encrypted Traffic Classification: Combining Over-and Under-Sampling through a PCA-SVM", In: Proc. of - PAIS 2018 Int. Conf. Pattern Anal. Intell. Syst., pp. 1–5, 2018.

12. Achmad Akbar Megantara, Tohari Ahmad, ANOVA-SVM for Selecting Subset Features in Encrypted Internet Traffic Classification. International Journal of Intelligent Engineering and Systems, Vol.14, No.2, 2021

13. R. Nigmatullin, A. Ivchenko and S. Dorokhin, "Differentiation of Sliding Rescaled Ranges: New Approach to Encrypted and VPN Traffic Detection," 2020 International Conference Engineering and Telecommunication (En&T), 2020, pp. 1-5, doi: 10.1109/EnT50437.2020.9431285

14. Uğurlu, M., Doğru, İ.A., Arslan, R.S. A new classification method for encrypted internet traffic using machine learning (2021) Turkish Journal of Electrical Engineering and Computer Sciences, 25 (9), pp. 2450-2468.

15. Felipe Peter. Analysis of the ISCX VPN-nonVPN Dataset 2016 for Encrypted Network Traffic Classification, Tsinghua University, [Электронный ресурс] - pp. 1-5, 2018

16. A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients / V. C. Perta [et al.] // Proceedings of Conference: 15th Privacy Enhancing Technologies, 30 June – 02 July 2015, Philadelphia, USA. – Philadelphia, 2015. – P. 77 – 91.

17. Brissaud P, Francћlois J, Chrisment I, Cholez T, Bettan O. Transparent and Service-Agnostic Monitoring of Encrypted Web TranћAic. IEEE Transactions on Network and Service Management 2019; 16 (3): 842-856

18. Lu, B., Luktarhan, N., Ding, C., Zhang, W. ICLSTM: Encrypted traffic service identification based on inception-LSTM neural network (2021) Symmetry, 13 (6), ст. № 1080

19. Wang, W.; Zhu, M.; Wang, J.; Zeng, X.; Yang, Z. End-to-end encrypted traffic classification with one-dimensional convolution neural networks. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; pp. 43–48.

20. Lotfollahi, M.; Siavoshani, M.J.; Zade, R.S.H.; Saberian, M. Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Comput. 2020, 24, 1999–2012.

21. Zou, Z.; Ge, J.; Zheng, H.; Wu, Y.; Han, C.; Yao, Z. Encrypted Traffic Classification with a Convolutional Long Short-Term Memory Neural Network. In Proceedings of the 20th IEEE International Conference on High Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018, Exeter, UK, 28–30 June 2018; pp. 329–334.

22. Xu, L.; Dou, D.; Chao, H.J. ETCNet: Encrypted Traffic Classification Using Siamese Convolutional Networks. In Proceedings of the Workshop on Network Application Integration/CoDesign (NAI'20), Virtual Event, New York, NY, USA, 14 August 2020; ACM: New York, NY, USA, 2020; p. 3.

23. Song, M.; Ran, J.; Li, S. Encrypted Traffic Classification Based on Text Convolution Neural Networks. In Proceedings of the 2019, IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 19–20 October 2019; pp. 432–436.

References

1. Starun I.G., Iuganson A.N., Gatchin Ju.A. Postroenie matematicheskoj modeli rascheta kompleksnoj ocenki VPN: st. - Vestnik TGTU, tom. 25, vypusk 4, 2019, s. 535-546.

2. Lu,B.; Luktarhan,N.; Ding, C; Zhang,W. ICLSTM: Encrypted Traffic Service Identification Based on Inception-LSTM Neural Network. Symmetry, 2021, 13, 1080. https:// doi.org/10.3390/sym13061080

3. X. Wang et al., "Evolutionary Algorithm-Based and Network Architecture Search-Enabled Multiobjective Traffic Classification," in IEEE Access, vol. 9, pp. 52310-52325, 2021

4. B. Yamansavascilar, M. A. Guvensan, A. G. Yavuz, and M. E. Karsligil, "Application identification via network traffic classification", In: Proc. of 2017 Int. Conf. Comput. Netw. Commun. ICNC 2017, pp. 843–848, 2017.

5. Megantara, A.A., Ahmad, T. ANOVA-SVM for Selecting Subset Features in Encrypted Internet Traffic Classification (2021) International Journal of Intelligent Engineering and Systems, 14 (2), pp. 536-546.

6. G. Cheng and S. Wang, "Traffic classification based on port connection pattern", In: Proc. of 2011 Int. Conf. Comput. Sci. Serv. Syst. CSSS 2011 - Proc., pp. 914–917, 2011.

7. H. K. Lim, J. B. Kim, K. Kim, Y. G. Hong, and Y. H. Han, "Payload-based traffic classification using multi-layer LSTM in software defined networks", Appl. Sci., Vol. 9, No. 12, 2019.

8. F. Dehghani, N. Movahhedinia, M. R. Khayyambashi, and S. Kianian, "Real-time traffic classification based on statistical and payload content features", In: Proc. of - 2010 2nd Int. Work. Intell. Syst. Appl. ISA 2010, pp. 26–29, 2010.

9. G. Draper-Gil, A. H. Lashkari, M. Mamun, and A. A. Ghorbani,"Characterization of encrypted and VPN traffic using time-related features," in Proc. 2nd Int. Conf. Inf. Syst. Security Privacy, 2016,pp. 407–414

10. Caicedo-Munђoz JA, Espino AL, Corrales JC, RendoђБn A.QoS-Classifier for VPN and Non-VPN traпђAic based on time-related features.Computer Networks 2018; 144: 271-279. doi: 10.1016/j.comnet.2018.08.008

11. A. Saber, B. Fergani, and M. Abbas, "Encrypted Traffic Classification: Combining Over-and Under-Sampling through a PCA-SVM", In: Proc. of - PAIS 2018 Int. Conf. Pattern Anal. Intell. Syst., pp. 1–5, 2018.

12. Achmad Akbar Megantara, Tohari Ahmad, ANOVA-SVM for Selecting Subset Features in Encrypted Internet Traffic Classification. International Journal of Intelligent Engineering and Systems, Vol.14, No.2, 2021

13. R. Nigmatullin, A. Ivchenko and S. Dorokhin, "Differentiation of Sliding Rescaled Ranges: New Approach to Encrypted and VPN Traffic Detection," 2020 International Conference Engineering and Telecommunication (En&T), 2020, pp. 1-5, doi: 10.1109/EnT50437.2020.9431285

14. Uğurlu, M., Doğru, İ.A., Arslan, R.S. A new classification method for encrypted internet traffic using machine learning (2021) Turkish Journal of Electrical Engineering and Computer Sciences, 25 (9), pp. 2450-2468.

15. Felipe Peter. Analysis of the ISCX VPN-nonVPN Dataset 2016 for Encrypted Network Traffic Classification, Tsinghua University, [Электронный ресурс] - pp. 1-5, 2018

16. A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients / V. C. Perta [et al.] // Proceedings of Conference: 15th Privacy Enhancing Technologies, 30 June – 02 July 2015, Philadelphia, USA. – Philadelphia, 2015. – P. 77 – 91.

17. Brissaud P, Francђlois J, Chrisment I, Cholez T, Bettan O. Transparent and Service-Agnostic Monitoring of Encrypted Web TraпђAic. IEEE Transactions on Network and Service Management 2019; 16 (3): 842-856

18. Lu, B., Luktarhan, N., Ding, C., Zhang, W. ICLSTM: Encrypted traffic service identification based on inception-LSTM neural network (2021) Symmetry, 13 (6), ст. № 1080

19. Wang, W.; Zhu, M.; Wang, J.; Zeng, X.; Yang, Z. End-to-end encrypted traffic classification with one-dimensional convolution neural networks. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; pp. 43–48.

20. Lotfollahi, M.; Siavoshani, M.J.; Zade, R.S.H.; Saberian, M. Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Comput. 2020, 24, 1999–2012.

21. Zou, Z.; Ge, J.; Zheng, H.; Wu, Y.; Han, C.; Yao, Z. Encrypted Traffic Classification with a Convolutional Long Short-Term Memory Neural Network. In Proceedings of the 20th IEEE International Conference on High Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018, Exeter, UK, 28–30 June 2018; pp. 329–334.

22. Xu, L.; Dou, D.; Chao, H.J. ETCNet: Encrypted Traffic Classification Using Siamese Convolutional Networks. In Proceedings of the Workshop on Network Application Integration/CoDesign (NAI'20), Virtual Event, New York, NY, USA, 14 August 2020; ACM: New York, NY, USA, 2020; p. 3.

23. Song, M.; Ran, J.; Li, S. Encrypted Traffic Classification Based on Text Convolution Neural Networks. In Proceedings of the 2019, IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 19–20 October 2019; pp. 432–436.

СТАРУН Игорь Геннадьевич, магистрант факультета безопасности информационных технологий федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО». Россия, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А. E-mail: starun.igor@yandex.ru.

STARUN Igor Gennadievich, master student of the Faculty of Secure Information Technologies of the Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO", Russia, 197101, St. Petersburg, Kronverksky pr., 49, lit. A. E-mail: starun.igor@yandex.ru.

ЮГАНСОН Андрей Николаевич, кандидат технических наук, доцент факультета безопасности информационных технологий федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО». Россия, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А. E-mail: a_yougunson@corp.itmo.ru.

IUGANSON Andrey Nikolaevich, Ph.D., Associate Professor of the Faculty of Secure Information Technologies of the Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO", Russia, 197101, St. Petersburg, Kronverksky pr., 49, lit. A. E-mail: a_yougunson@corp.itmo.ru.

УДК 004.588 Вестник УрФО № 1(43) / 2022, с. 84–89

Астахова Л.В., Уторов О.Р.

DOI: 10.14529/secur220110

БУДУЩИЙ СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ КАК СУБЪЕКТ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Современная практика обеспечения информационной безопасности остро нуждается в специалистах по защите информации как результативных субъектах образовательных процессов. При этом наблюдается недостаточное внимание к этому вопросу в системе их профессиональной подготовки в вузе. Цель статьи – выявить факторы, требующие развития педагогической компетентности будущих специалистов по защите информации в вузе, и показать возможности усиления их образовательной субъектности в процессе обучения. В статье обосновано, что усилению субъектности будущего специалиста по защите информации в информационно-образовательном процессе в вузе способствуют: глобальная тенденция усиления субъектности студента в информационно-образовательном процессе в вузе и императивы личностного саморазвития специалистов по защите информации в современной цифровой культуре; требования ФГОС ВО 3++ по информационной безопасности, включающих образование в число областей будущей профессиональной деятельности выпускников; специфика содержания профессиональной деятельности специалиста по защите информации, связанная с необходимостью обучать сотрудников, повышать их осведомленность в области информационной безопасности организации. Предложены меры формирования и развития статуса будущего специалиста в области защиты информации, обучающегося в вузе, как субъекта образовательной деятельности.

Ключевые слова: *информационная безопасность, специалист, субъект, образовательная деятельность, педагогическая компетенция.*

Astakhova L.V., Utorov O.R.

FUTURE SECURITY SPECIALIST AS A SUBJECT OF EDUCATIONAL ACTIVITY

The modern practice of ensuring information security is in dire need of information security specialists as effective subjects of educational processes. At the same time, there is insufficient attention to this issue in the system of their professional training at the university. The purpose of the article is to identify factors that require the development of pedagogical competence of future information security specialists at a university, and to show the possibilities of strengthening their educational subjectivity in the learning process. The article substantiates that the strengthening of the subjectivity of the future information security specialist in the information and educational process at the university is facilitated by: the global trend of strengthening the subjectivity of the student in the information and educational process at the university and the imperatives of personal self-development of information security specialists in modern digital culture; the requirements of federal state educational standards 3++ on information security, including education among the areas of future professional activity of graduates; the specifics of the content of the professional activity of an information security specialist, associated with the need to train employees, increase their awareness in the field of information security of the organization. Measures for the formation and development of the status of a future specialist in the field of information security studying at a university as a subject of educational activity are proposed.

Keywords: *information security, specialist, subject, educational activity, pedagogical competence.*

Введение. В национальной программе «Цифровая экономика Российской Федерации» заявлена острая потребность в «адаптивных, практико-ориентированных и гибких образовательных *программах* высшего образования, которые обеспечивают получение студентами профессиональных компетенций, отвечающих актуальным требования рынка труда, в том числе в области *цифровой экономики*» [1]. Необхо-

димы специалисты, способные постоянно осваивать новые цифровые технологии как самостоятельно, так и с использованием институциональных форм обучения. Однако, к сожалению, спрос на таких работников в настоящее время превышает не только фактическое предложение, но и соответствующий потенциал систем образования и профессиональной подготовки и в России, и за рубежом [2]. Не является исключением и сфера образования в области информационной безопасности. Современная практика обеспечения информационной безопасности остро нуждается в специалистах по защите информации как результативных субъектах образовательных процессов. Этим обусловлена цель настоящей статьи – выявить факторы, требующие развития педагогической компетентности будущих специалистов по защите информации в вузе, и показать возможности усиления их образовательной субъектности в процессе обучения.

Факторы усиления статуса будущего специалиста по защите информации как субъекта образовательной деятельности. К их числу мы относим два фактора: общий и особенный.

1 фактор – современная тенденция усиления субъектности студента вуза. Статус студента эволюционирует. Если раньше за ним был закреплен статус обучающегося, т.е. объекта обучения, то сегодняшние реалии требуют рассматривать его как самостоятельного субъекта образования - субъекта системных информационных образовательных процессов [3].

Ученые активно обсуждают условия формирования самостоятельного зрелого мышления, развития субъектности и подлинной автономии индивида [4]. Поскольку будущее образование будет больше направлено на общение и интерактивность, а не на односторонний процесс потребления информации [5], стало очевидно, что взаимоотношения «обучающий-обучающийся» изменились, классические принципы передачи знаний от учителя к ученику, от старшего к младшему изжили себя [6]. Однако классический передаточный, субъект-обьектный (студент – объект, преподаватель – субъект) характер образования не учитывает самого обучающегося в образовании, его миссию, предназначение, особенности, создает предпосылки для утраты самоидентичности человека, его внутреннего пространства [7]. К сожалению, этот подход продолжает доминировать в процессе подготовки специалистов по защите информации.

И это не удивительно, поскольку он до сих пор доминирует и в педагогической науке. Так, автор включает в число структурных составляющих обучения как информационного процесса: обучающего как источник информации, обучающегося как приемника информации, контекст (договоренность о теме сообщения), сообщение (содержание информации), код (язык представления информации), каналы связи (пути и средства передачи и приема информации), информационный фильтр обучающего (программа научения), информационный фильтр обучающегося (субъективная программа учения), сеть шумов при передаче информации для субъектов процесса обучения (помехи, искажающие передаваемые и получаемые сведения и приводящие к потере информации) [8]. Как видим, роль обучающегося ограничена исключительно пассивным получением информации.

Между тем, статус пассивного приемника информации в образовании уже не устраивает студента, не мотивирует его к учению. Усиление внимания к обучающемуся не как к традиционному объекту, а как к субъекту образования – императив современной культуры. В контексте информационного подхода он уже является не только потребителем, получателем, но и полноправным создателем, отправителем информации. При этом в роли получателя выступает не только преподаватель, но и другие обучающиеся (студенты учебной группы), а также члены профессионального сообщества [3].

Императивом современной цифровой среды является единство потребительской, репродуктивной и созидательной составляющих информационно-образовательной деятельности [9]. В процессе освоения образовательной программы студент должен не только потреблять и передавать чужую информацию, но и создавать и представлять собственные информационные продукты, в которых присутствуют элементы анализа, сравнения, генерации нового знания и собственного мнения. И именно эта составляющая образовательной деятельности студента должна доминировать в условиях цифровой культуры.

Становится все более очевидно, что подлинный прогресс заключается не в глобализации и цифровизации, не в развитии науки, техники и новейших технологий, но, прежде всего, - в развитии общества и личности, в повышении уровня ответственности, сознания, морали, определяющих поведение людей [10]. Поэтому сегодня столь важное значение имеет не только педагогическое воздействие со стороны преподавателя, но и саморазвитие личности будущего специалиста, в том числе – специалиста по защите информации. Он должен иметь возможность построения индивидуальных образовательных траекторий, которые зависят от специфики конкретной отрасли и вида деятельности по обеспечению информационной безопасности. Миссия вуза - развитие способности выпускника к прогнозированию путей развития своей личности, к рефлексии, самопознанию, самопрограммированию. Только сам студент может знать о своих сильных и слабых сторонах и принимать решения о способах, методах и формах самосовершенствования в профессии. Однако для реализации этой деятельности студент должен в стенах вуза освоить

навыки выбора и использования этих форм, методов, цифровых технологий.

Изменение статуса студента влияет и на статус преподавателя. Зарубежные эксперты, обосновывая продуктивную педагогику как основу для фундаментальной реорганизации педагогического образования [11], называют ее сущностным свойством не обучение студентов, а управление ими.

Если первый фактор усиления субъектности студента является общим для всех образовательных направлений в условиях цифровой культуры, то второй - специфичен для будущего специалиста по защите информации.

2 фактор – наличие образовательного компонента в структуре профессиональной деятельности специалиста в области информационной безопасности.

Во-первых, в ФГОС 3++ по информационной безопасности образование включено в число областей профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата, магистратуры и специалитета по информационной безопасности могут осуществлять профессиональную деятельность [12,13,14]. Логично предположить, что выпускник после окончания вуза должен быть готов к работе в сферах профессионального и дополнительного профессионального образования, т.е. быть способен оказывать образовательные услуги по информационной безопасности в вузах, техникумах, в учебных центрах, имеющих лицензии на образовательную деятельность. Однако, в перечне компетенций, перечисленных в стандартах, соответствующие компетенции отсутствуют. Этот недостаток актуализирует задачу формулировки таких компетенций для разработчиков ФГОС ВО по информационной безопасности.

Во-вторых, все более актуализируется педагогическая специфика содержания профессиональной деятельности специалиста по защите информации. Она обладает ярко выраженными особенностями, которые обусловлены присутствием в структуре его деятельности такого источника угроз защищаемой информации, как люди. Ежегодные аналитические отчеты свидетельствуют о том, что подавляющее большинство инцидентов информационной безопасности происходит по вине человека. Аксиомой в сфере информационной безопасности является факт, что причины, по которым человек может оказывать дестабилизирующие воздействия на защищаемую информацию, могут быть преднамеренные (сознательно спланированное, умышленное стремление нанести вред) и непреднамеренные (отсутствие знания правил информационной безопасности, халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе, небрежность), и требуют разного рода управленческих воздействий на них. При непреднамеренных причинах инцидентов информационной безопасности специалист по защите информации должен предпринять педагогические действия, связанные преимущественно с повышением осведомленности сотрудников об информационной безопасности организации. Повышение осведомленности работников компании в области информационной безопасности - это целенаправленный, организованный, планомерно и систематически осуществляемый процесс повышения уровня знаний работников и формирования необходимых навыков в области информационной безопасности, создания корпоративной культуры в данной области и атмосферы осознания необходимости соблюдения требований информационной безопасности. Цели и основные требования к этому процессу определены в международных и российских стандартах (ГОСТ Р ИСО/МЭК серии 27000 по управлению информационной безопасностью, СТО БР ИББС и др.) и нормативных документах по обеспечению информационной безопасности (ФЗ от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и др.).

Принципиально иные педагогические действия специалист по защите информации должен предпринять для профилактики и предупреждения преднамеренных причин инцидентов информационной безопасности. К преднамеренным воздействиям на защищаемую информацию относят воздействия внешних и внутренних потенциальных и реальных злоумышленников, – лиц, способных совершать и совершающих действия, не соответствующие правовым и нравственным нормам, т. е. лиц с девиантным типом поведения. Для противодействия таким типам нарушителей специалисту по защите информации необходимы педагогические компетенции, связанные в большей степени с профилактикой их девиантного поведения и гармонизацией корпоративной среды. К их числу следует отнести способность: формировать мотивацию сотрудников не нарушать Политику информационной безопасности организации, культивировать в организации ценностно-ориентированные нормы поведения, информационной этики; поддерживать благоприятную социокультурную среду организации; повышать уровень ее корпоративной культуры и лояльности персонала; заботиться о личностном развитии сотрудников [15].Очевидно, что без целенаправленной вузовской подготовки студентов к этим направлениям профессиональной деятельности весьма недальновидно рассчитывать на успешный результат в процессе их трудовой деятельности. Однако сегодня в профильных учебных планах не предусмотрено дисциплин на освоение столь многослойного по своей междисциплинарности вида деятельности. Это позволяет говорить об острой акту-

альности задачи развития соответствующих компетенций студентов для вузов, осуществляющих подготовку кадров по информационной безопасности.

Выводы. Усилению субъектности будущего специалиста по защите информации в информационно-образовательном процессе в вузе способствуют: глобальная тенденция усиления субъектности студента в информационно-образовательном процессе в вузе и императивы личностного саморазвития специалистов по защите информации в современной цифровой культуре; требования стандартов ФГОС ВО 3++ по информационной безопасности, включающих образование в число областей будущей профессиональной деятельности выпускников; специфика содержания профессиональной деятельности специалиста по защите информации, связанная с необходимостью обучать сотрудников, повышать их осведомленность в области ИБ и развивать культуру ИБ организации. Обоснованные факторы имеют объективный характер, и для их реализации в образовательных программах в процессе подготовки специалистов по защите информации необходима целенаправленная работа разработчиков федеральных государственных стандартов высшего образования и выпускающих кафедр вузов. В стандарты должны быть включены соответствующие педагогические компетенции, которые будут направлены на развитие способности студента выступать субъектом образовательной деятельности как в стенах вуза, так и за его пределами, а также по месту трудоустройства. Выпускающим кафедрам в рамках подготовки бакалавров согласно ФГОС 3++ целесообразно открывать специализацию «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и в ее рамках обратить внимание на содержание и организацию повышения осведомленности об информационной безопасности сотрудников организации как на объект освоения. В учебные планы по специальностям группы «Информационная безопасность» стоит включать отдельную дисциплину, посвященную педагогическим технологиям в профессиональной деятельности. Возможен также вариант включения соответствующих модулей в организационно-управленческие дисциплины. В конечном итоге названные меры способны повысить результативность деятельности по обеспечению информационной безопасности любой организации.

Литература

1. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам. Протокол от 24 декабря 2018 г. №16). - URL: http://government.ru/info/35568/ (дата обращения: 19.02.2022).

2. Kergroach S. Industry 4.0: New Challenges and Opportunities for the Labour Market // Foresight and STI Governance. – 2017. - Т. 11, № 4. - С. 6–8. DOI: 10.17323/2500-2597.2017.4.6.8

3. Астахова, Л. В. Новые требования информационного подхода к образованию / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2022. – № 1. – С. 15-21. – DOI 10.36535/0548-0019-2022-01-2.

4. Сохраняева, Т. В. Эмансипирующий потенциал образования: критическая традиция в философии образования / Т. В. Сохраняева, И. Д. Замоткин // Вопросы философии. – 2021. – № 1. – С. 192-202. – DOI 10.21146/0042-8744-2021-1-192-202.

5. Kostova-Panayotova, M. Education in University - from Knowledge to Communication / M. Kostova-Panayotova // Foreign Language Teaching. – 2017. – Vol. 44. – No 6. – P. 631-637.

6. Савчук, В. В. Медиаобразование - эпифеномен цифровизации / В. В. Савчук // Вопросы философии. – 2020. – № 5. – С. 83-86. – DOI 10.21146/0042-8744-2020-5-83-86.

7. Король, А. Д. Самоидентичность человека как проблема образовательного пространства и времени / А. Д. Король // Вопросы философии. – 2021. – № 5. – С. 26-35. – DOI 10.21146/0042-8744-2021-5-26-35.

8. Казакевич, В. М. Обучение как информационно-коммуникационный процесс / В. М. Казакевич // Отечественная и зарубежная педагогика. – 2019. – Т. 1. – № 3(60). – С. 151-164. – DOI 10.24411/2224-0772-2019-10024.

9. Astakhova, L. V. Information Psychological Theory of the Spiritual Development of a Personality in the Digital Culture Era (to the 95th anniversary of the birth of Yu.S. Zubov) / L. V. Astakhova // Scientific and Technical Information Processing. – 2019. – Vol. 46. – No 2. – P. 84-89. – DOI 10.3103/S0147688219020072.

10. Чумаков, А. Н. Глобализация и цифровизация: социальные последствия кумулятивного взаимодействия / А. Н. Чумаков // Вопросы философии. – 2021. – № 8. – С. 36-46. – DOI 10.21146/0042-8744-2021-8-36-46.

11. Jennifer M. Gore, Tom Griffiths, James G. Ladwig, Towards better teaching: productive pedagogy as a framework for teacher education // Teaching and Teacher Education. – 2004. – Т. 20, № 4. – С. 375-387, ISSN

0742-051X. - URL: https://doi.org/10.1016/j.tate.2004.02.010. (https://www.sciencedirect.com/science/article/pii/S0742051X04000204) (дата обращения: 19.02.2022).

12. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки10.03.01 Информационная безопасность УТВЕРЖДЕН приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427 - URL: https://fgosvo.ru/fgosvo/index/24/10 (дата обращения: 19.02.2022).

13. Федеральный государственный образовательный стандарт высшего образования -магистратура по направлению подготовки10.04.01 Информационная безопасность УТВЕРЖДЕН приказом Министерства науки и высшего образования Российской Федерацииот 26 ноября 2020 г. N 1455. - URL: https://fgosvo.ru/fgosvo/index/25/37 (дата обращения: 19.02.2022).

14. Федеральный государственный образовательный стандарт высшего образования - специалитет по специальности10.05.03 Информационная безопасность автоматизированных систем. Утвержден приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. N 1457. - URL: https://fgosvo.ru/fgosvo/index/26/60 (дата обращения: 19.02.2022).

15. Астахова, Л. В. Педагогическая компетенция будущего специалиста по защите информации в вузе: проблема развития и понятие / Л. В. Астахова // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2014. – Т. 6. – № 1. – С. 69-76.

References

1. Pasport natsional'noy programmy "Tsifrovaya ekonomika Rossiyskoy Federatsii" (utv. prezidiumom Soveta pri Prezidente Rossiyskoy Federatsii po strategicheskomu razvitiyu i natsional'nym proyektam. Protokol ot 24 dekabrya 2018 g. №16). - URL: http://government.ru/info/35568/ (data obrashcheniya: 19.02.2022).

2. Kergroach S. Industry 4.0: New Challenges and Opportunities for the Labor Market // Foresight and STI Governance. - 2017. - T. 11, No. 4. - S. 6–8. DOI: 10.17323/2500-2597.2017.4.6.8

3. Astakhova, L. V. Novyye trebovaniya informatsionnogo podkhoda k obrazovaniyu / L. V. Astakhova // Nauchno-tekhnicheskaya informatsiya. Seriya 1: Organizatsiya i metodika informatsionnoy raboty. – 2022. – № 1. – S. 15-21. – DOI 10.36535/0548-0019-2022-01-2.

4. Sokhranyayeva, T. V. Emansipiruyushchiy potentsial obrazovaniya: kriticheskaya traditsiya v filosofii obrazovaniya / T. V. Sokhranyayeva, I. D. Zamotkin // Voprosy filosofii. – 2021. – № 1. – S. 192-202. – DOI 10.21146/0042-8744-2021-1-192-202.

5. Kostova-Panayotova, M. Education in University - from Knowledge to Communication / M. Kostova-Panayotova // Foreign Language Teaching. - 2017. - Vol. 44. - No 6. - P. 631-637.

6. Savchuk, V. V. Mediaobrazovaniye - epifenomen tsifrovizatsii / V. V. Savchuk // Voprosy filosofii. – 2020. – № 5. – S. 83-86. – DOI 10.21146/0042-8744-2020-5-83-86.

7. Korol', A. D. Samoidentichnost' cheloveka kak problema obrazovatel'nogo prostranstva i vremeni / A. D. Korol' // Voprosy filosofii. – 2021. – № 5. – S. 26-35. – DOI 10.21146/0042-8744-2021-5-26-35.

8. Kazakevich, V. M. Obucheniye kak informatsionno-kommunikatsionnyy protsess / V. M. Kazakevich // Otechestvennaya i zarubezhnaya pedagogika. – 2019. – T. 1. – № 3(60). – S. 151-164. – DOI 10.24411/2224-0772-2019-10024.

9. Astakhova, L. V. Information Psychological Theory of the Spiritual Development of a Personality in the Digital Culture Era (to the 95th anniversary of the birth of Yu.S. Zubov) / L. V. Astakhova // Scientific and Technical Information Processing. - 2019. - Vol. 46. - No 2. - P. 84-89. – DOI 10.3103/S0147688219020072.

10. Chumakov, A. N. Globalizatsiya i tsifrovizatsiya: sotsial'nyye posledstviya kumulyativnogo vzaimodeystviya / A. N. Chumakov // Voprosy filosofii. – 2021. – № 8. – S. 36-46. – DOI 10.21146/0042-8744-2021-8-36-46.

11. Jennifer M. Gore, Tom Griffiths, James G. Ladwig, Towards better teaching: productive pedagogy as a framework for teacher education // Teaching and Teacher Education. - 2004. - T. 20, No. 4. - S. 375-387, ISSN 0742-051X. - URL: https://doi.org/10.1016/j.tate.2004.02.010. (https://www.sciencedirect.com/science/article/pii/S0742051X04000204) (accessed 2/19/2022).

12. Federal'nyy gosudarstvennyy obrazovatel'nyy standart vysshego obrazovaniya - bakalavriat po napravleniyu podgotovki10.03.01 Informatsionnaya bezopasnost' UTVERZHDEN prikazom Ministerstva nauki i vysshego obrazovaniya Rossiyskoy Federatsii ot 17 noyabrya 2020 g. N 1427 - URL: https://fgosvo.ru/fgosvo/index/24/10 (data obrashcheniya: 19.02.2022).

13. Federal'nyy gosudarstvennyy obrazovatel'nyy standart vysshego obrazovaniya -magistratura po napravleniyu podgotovki10.04.01 Informatsionnaya bezopasnost' UTVERZHDEN prikazom Ministerstva nauki i vysshego obrazovaniya Rossiyskoy Federatsiiot 26 noyabrya 2020 g. N 1455. - URL: https://fgosvo.ru/fgosvo/index/25/37 (data obrashcheniya: 19.02.2022).

14.Federal'nyy gosudarstvennyy obrazovatel'nyy standart vysshego obrazovaniya - spetsialitet po spetsial'nosti10.05.03 Informatsionnaya bezopasnost' avtomatizirovannykh sistem. Utverzhden prikazom Ministerstva nauki i vysshego obrazovaniya Rossiyskoy Federatsii ot 26 noyabrya 2020 g. N 1457. - URL: https://fgosvo.ru/fgosvo/index/26/60 (data obrashcheniya: 19.02.2022).

15. Astakhova, L. V. Pedagogicheskaya kompetentsiya budushchego spetsialista po zashchite informatsii v vuze: problema razvitiya i ponyatiye / L. V. Astakhova // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Obrazovaniye. Pedagogicheskiye nauki. – 2014. – T. 6. – № 1. – S. 69-76.

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: astakhovalv@susu.ru

ASTAKHOVA Liudmila Victorovna, Doctor of Pedagogy, Professor, Professor of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: astakhovalv@susu.ru

УТОРОВ Олег Равильевич, кандидат педагогических наук, доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: utorovor@susu.ru

UTOROV Oleg Ravilevich, Candidate of Pedagogical Sciences, Associate Professor of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: utorovor@susu.ru

УДК 004.492.2 Вестник УрФО № 1(43) / 2022, с. 90–96

Лебедев Д.В., Гузенкова Е.А.

DOI: 10.14529/secur220111

МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ СИСТЕМОЙ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ ПОСРЕДСТВОМ ПРОВЕДЕНИЯ АТАК НА УЯЗВИМУЮ СИСТЕМУ

В статье показан метод оценки эффективности использования систем предотвращения вторжений на примере комплекса для защиты сети «Континент 4». Система предотвращения вторжений представляет собой средство компьютерной и сетевой безопасности, обнаруживающее вторжения или нарушения безопасности с автоматической защитой от них.

Данный метод основывается на моделировании атак на уязвимую систему и включает в себя исследование информационной системы на наличие уязвимостей. Уязвимость представляет собой недостаток в системе, которая может использоваться для реализации угроз безопасности.

В результате данной работы был получен вывод о том, что системы предотвращения вторжений на примере комплекса «Континент 4» позволяют заблокировать многие атаки. Показанный метод позволяет определить эффективность использования систем предотвращения вторжений, а также определить объекты, требующие дополнительных мер по защите.

Ключевые слова: *информационная безопасность, программно-аппаратная защита информации, система предотвращения вторжений, система обнаружения вторжений, уязвимость, атака.*

Lebedev D.V., Guzenkova E.A.

METHOD FOR EVALUATING THE EFFECTIVENESS OF ENSURING THE SECURITY OF A COMPUTER NETWORK BY AN INTRUSION PREVENTION SYSTEM THROUGH ATTACKS ON A VULNERABLE SYSTEM

The article shows a method for evaluating the effectiveness of using intrusion prevention systems on the example of a complex for protecting the network «Continent 4». An intrusion prevention system is a computer and network security tool that detects intrusions or security breaches with automatic protection against them.

This method is based on modeling attacks on a vulnerable system and includes the study of the information system for vulnerabilities. A vulnerability is a flaw in a system that can be used to implement security threats.

As a result of this work, it was concluded that intrusion prevention systems, using the example of the complex «Continent 4», make it possible to block many attacks. The method shown makes it possible to determine the effec-

tiveness of the use of intrusion prevention systems, as well as to identify objects that require additional protection measures.

Keywords: *information security, hardware and software protection of information, intrusion prevention system, intrusion detection system, vulnerability, attack.*

Уязвимые системы являются частой проблемой, и своевременное их обновление помогает закрыть часть уязвимостей. Но существуют такие организации, которые используют неподдерживаемые устаревшие операционные системы, так как процесс обновления является невозможным или трудозатратным. Использование таких информационных ресурсов подвергает компании серьезному риску, поскольку злоумышленники могут взломать системы с помощью уязвимостей.

Для таких случаев одним из методов защиты являются системы предотвращения вторжений. Система предотвращения вторжений (IPS – Intrusion Prevention System) представляет собой средство компьютерной и сетевой безопасности, обнаруживающее вторжения или нарушения безопасности с автоматической защитой от них.

Системы предотвращения вторжений появились в результате развития нескольких независимых решений: межсетевых экранов (анализ сетевых пакетов) и систем обнаружения вторжений (анализ программ и файлов).

IPS, как правило, используют в составе межсетевого экрана следующего поколения (Next Generation Firewall).

Для проведения тестирования эффективности системы предотвращения вторжений был развернут тестовый стенд в виртуальной среде VMware, состоящий из следующих виртуальных машин:

1) Атакующий компьютер с операционной системой Kali Linux. Данная система представляет собой специально созданный дистрибутив с большим количеством программ для тестирования на проникновение.

2) Атакуемый компьютер Metasploitable 2 с умышленно уязвимой операционной системой Linux Ubuntu. Metasploitable представляет собой виртуальную машину, предназначенную для тестирования инструментов безопасности и демонстрации общих уязвимостей.

3) Система предотвращения вторжений в составе многофункционального межсетевого экрана «Континент 4».

«Континент 4» является решением класса NGFW и объединяет в себе функции межсетевого экрана, системы обнаружения и предотвращения вторжений, защиту от вредоносных веб-сайтов, виртуальной частной сети, поведенческого анализа и другие. [2]

На рисунке 1 показана схема виртуального стенда.

Для оценки эффективности системы предотвращения вторжений будет использоваться следующая последовательность действий: [1]

Рис.1. Схема виртуального стенда

1) Сканирование уязвимой защищаемой системы сканером nmap.

Nmap представляет собой утилиту для сканирования IP-сетей с целью определения открытых портов, версий программного обеспечения, операционных систем. В результате сканирования формируется список открытых портов и соответствующих им служб.

2) Сканирование уязвимой защищаемой системы сканером уязвимостей Nessus.

Nessus – программа для автоматического сканирования операционных систем с целью определения известных уязвимостей. В результате – формируется ранжированный список уязвимостей.

3) На основании сканирования системы формируется список доступных эксплойтов и атак в Metasploit (платформа для создания, тестирования и использования эксплойтов). Далее реализуются возможные атаки.

Атаки проводятся в условиях, где на атакующей машине Kali Linux указан маршрут до уязвимой системы и на межсетевом экране «Континент 4» разрешено прохождение всех сетевых пакетов. При этом активирован компонент системы предотвращения вторжений.

На рисунке 2 показано сравнение результатов сканирования сканером nmap без системы предотвращения вторжений и с активированным компонентом системы предотвращения вторжений.

На рисунке 3 показано сравнение результатов сканирования сканером Nessus без системы предот-

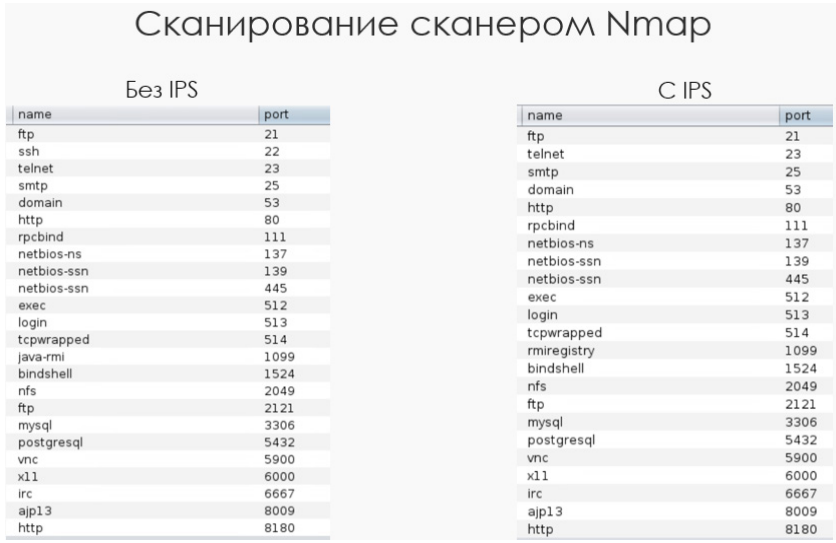


Рис. 2. Результаты сравнения сканирования сканером nmap

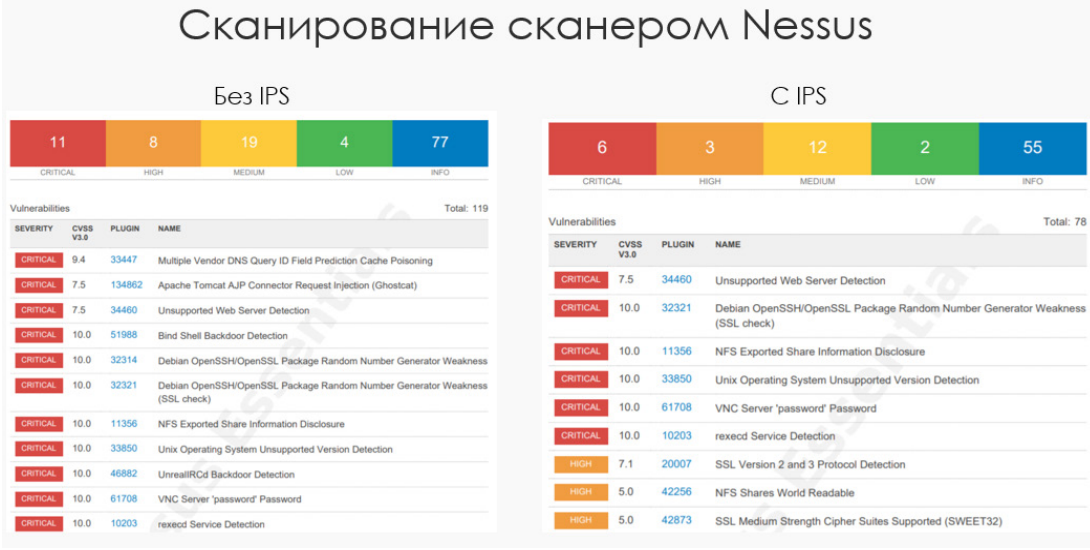


Рис. 3. Результат сравнения сканирования сканером Nessus

вращения вторжений и с активированным компонентом системы предотвращения вторжений.

При сканировании защищаемого ресурса сканерами nmap и Nessus система предотвращения вторжений сигнализировала об этом. Данные записи в журнале событий дают администратору возможность понять, что защищаемые ресурсы подвергаются сканированию, и предпринять необходимые действия для ликвидации и минимизации последствий.

Атаки на уязвимую систему осуществлялись согласно обнаруженным открытым портам, уязвимостям и сервисам в соответствии с рисунками 2 и 3. Далее описаны некоторые из проведенных атак

1) Атака на 21 порт.

2) 21 порт использует службу ftp. В Metasploitable 2 на данном порту работает ftp-сервер vsftpd.

Используя модуль сканирования в Metasploit, была проверена возможность анонимного доступа к ftp-серверу. Также был использован методом грубой силы для подбора логина и пароля (брутфорс-атака). Использование данных модулей показано на рисунке 4.

В результате было обнаружено, что на ftp-сервер возможен анонимный вход, а также подобраны пары логин/пароль.

Система предотвращения вторжений обнаружила брутфорс-атаку (рисунок 5).

Сканерами nmap и Nessus была определена используемая версию сервера. Для версии vsftpd 2.3.4 существует эксплойт, который позволяет злоумышленнику выполнить произвольный код на уязвимой системе. На рисунке 6 показан результат эксплуатации уязвимости. В результате система предотвраще-

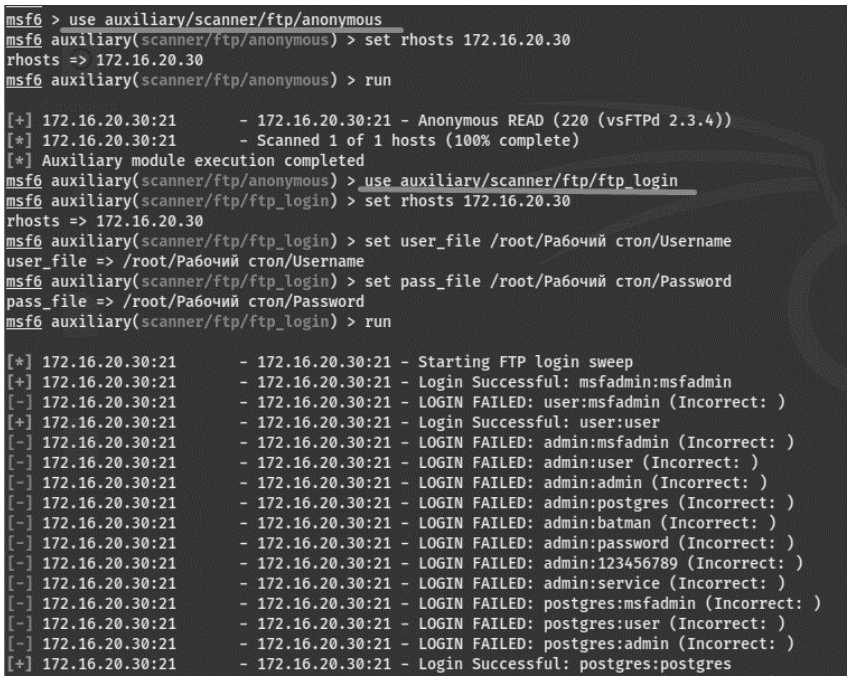


Рис.4. Результат сканирования FTP-сервера для подбора аутентификационных данных

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
15.07.2021 18:27:40.901	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	Potential FTP Brute-Force attempt response
15.07.2021 18:27:28.094	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	Potential FTP Brute-Force attempt response
15.07.2021 18:27:15.447	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	Potential FTP Brute-Force attempt response

Рис. 5. Обнаруженная брутфорс-атака на FTP-сервер

Рис. 6. Попытка эксплуатации уязвимости в сервере vsftpd

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
15.07.2021 18:37:56.546	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	id check returned root
15.07.2021 18:34:21.770	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	id check returned root

Рис. 7. Обнаруженная атака на FTP-сервер

ния вторжений обнаружила и заблокировала данную атаку (рисунок 7).

2) Атака на 80 порт

80 порт – порт протокола HTTP. Веб-страница Metasploitable работает на языке PHP в режиме CGI [3]. Режиме CGI описывает каким образом веб-сервер должен запускать прикладное программное обеспечение. Некоторые версии PHP в режиме CGI являются уязвимыми к эксплойту, который внедряет специальные аргументы, позволяющие предоставить доступ к системе. На рисунке 8 показано, что данный эксплойт не сработал, о чем свидетельствует запись в журнале событий в комплексе «Континент» (рисунок 9).

3) Атака на 8180 порт

Порт 8180 является альтернативным портом HTTP. В Metasploitable 2 на данном порту работает сервис Apache Tomcat. Для данного сервиса существует эксплойт, который загружает на сервер полезную нагрузку.

Атака, проведенная на уязвимый сервис (рису-

```
msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 172.16.20.30
rhosts => 172.16.20.30
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.10.1.240:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

Рис. 8. Атака, заблокированная системой предотвращения вторжений

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
16.07.2021 07:16:20.385	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	PHP //Input in HTTP POST
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	disable_functions PHP config option in uri
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	open_basedir PHP config option in uri
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	auto_prepend_file PHP config option in uri
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	safe_mode PHP config option in uri
16.07.2021 07:16:20.383	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	allow_url_include PHP config option in uri
16.07.2021 07:16:20.382	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	PHP tags in HTTP POST

Рис. 9. Заблокированная атака на PHP

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 172.16.20.30
rhosts => 172.16.20.30
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.10.1.240:4444
[*] Retrieving session ID and CSRF token...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

Рис. 10. Эксплуатация уязвимости для сервиса Apache Tomcat

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
16.07.2021 08:04:08.855	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	Incoming Basic Auth Base64 HTTP Password detected unencrypted
16.07.2021 08:04:08.854	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	Outgoing Basic Auth Base64 HTTP Password detected unencrypted

Рис. 11. Заблокированная атака на Apache Tomcat

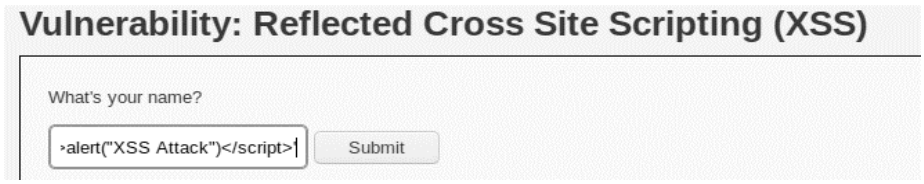


Рис. 12. Реализация XSS-атаки

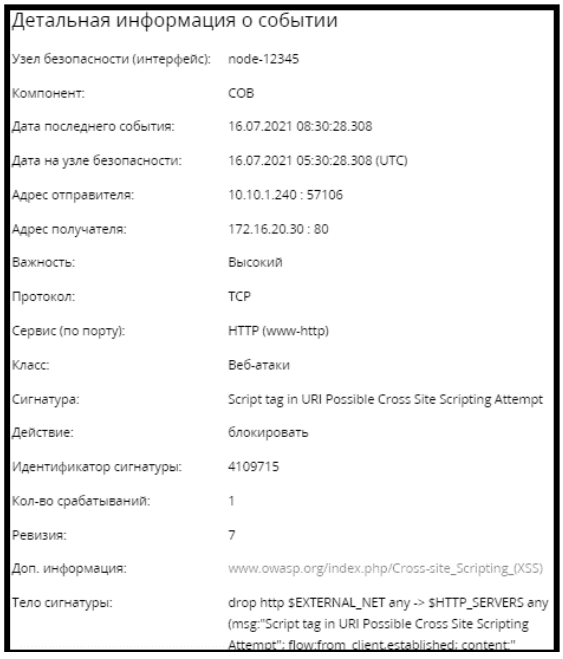
нок 10), была заблокирован системой предотвращения вторжений (рисунок 11).

4) Атака на веб-приложение

Metasploitable 2 содержит несколько уязвимых веб-приложений. Данные приложения используются для тренировки проведения веб-атак. Сервисы Mutillidae и DVWA позволяют воспроизвести атаки из OWASP top 10.

OWASP (открытый проект обеспечения безопасности веб-приложений) создал список из 10 самых опасных векторов атак на веб-приложения. Этот список получил название OWASP top 10.

Одной из атак из OWASP top 10 является XXS (межсайтовый скриптинг) [4]. Суть данной атаки заключается во внедрении вредоносного Java Script кода на исполнение в браузер пользователя. На рисунке 12 показана попытка реализации данной атаки. Система предотвращения вторжений заблокировала XSS-атаку, о чем свидетельствует запись в журнале событий на рисунке 13.


Детальная информация о событии

Узел безопасности (интерфейс):	node-12345
Компонент:	СОВ
Дата последнего события:	16.07.2021 08:30:28.308
Дата на узле безопасности:	16.07.2021 05:30:28.308 (UTC)
Адрес отправителя:	10.10.1.240 : 57106
Адрес получателя:	172.16.20.30 : 80
Важность:	Высокий
Протокол:	TCP
Сервис (по порту):	HTTP (www-http)
Класс:	Веб-атаки
Сигнатура:	Script tag in URI Possible Cross Site Scripting Attempt
Действие:	блокировать
Идентификатор сигнатуры:	4109715
Кол-во срабатываний:	1
Ревизия:	7
Доп. информация:	www.owasp.org/index.php/Cross-site_Scripting_(XSS)
Тело сигнатуры:	drop http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"Script tag in URI Possible Cross Site Scripting Attempt"; flow:from_client,established; content:"

Рис. 13. Заблокированная XSS-атака

Таблица 1

Результат применения системы предотвращения вторжений

№	Порт (сервис)	Наименование атаки/эксплойт	Действие
1	21 (FTP)	Брутфорс-атака на FTP-сервер	Обнаружил
2	21 (FTP)	Vsftpd_234_backdoor	Заблокировал
3	22 (SSH)	Брутфорс-атака на SSH	Обнаружил
4	23 (Telnet)	Брутфорс-атака Telnet	Обнаружил
5	80 (HTTP)	Php_cgi_arg_injection	Заблокировал
6	80 (HTTP)	SQL-инъекция	Не обнаружил
7	80 (HTTP)	XSS	Заблокировал
8	139/445 (NetBIOS)	Usermap_script	Заблокировал
9	1099 (RMI Rigestry)	Java_rmi_server	Заблокировал
10	1524	Bind shell-подключение	Не обнаружил
11	3306 (MySQL)	Удаленное выполнение команд в СУБД MySQL	Обнаружил
12	5432 (PostgreSQL)	Postgres_payload	Не обнаружил
13	5900 (VNC)	Подключение через VNC	Не обнаружил
14	6667 (IRC)	Unreal_ircd_3281_backdoor	Заблокировал
15	8180 (Apache Tomcat)	Tomcat_mgr_upload	Заблокировал

В таблице 1 представлены все проведенные атаки и результаты работы системы предотвращения вторжений «Континент 4».

Система предотвращения вторжений «Континент 4» заблокировала большую часть атак (73,3%). При этом проводимые атаки являются как протокольными (доступ по SSH, Telnet, VNC), то есть блокируются межсетевым экраном, так и эксплуатирующими уязвимости программного обеспечения (эксплойты, бэкдоры и др.).

Также некоторые атаки происходили на веб-приложения (SQL-инъекция, XSS). Для обеспечения безопасности веб-приложений принято использовать межсетевой экран веб-приложений (WAF). Тем не менее сетевая система предотвращения вторжений «Континент 4» смогла обнаружить и заблокировать некоторые атаки из данной категории.

В работе был продемонстрирован метод оценки эффективности использования системы предотвращения вторжений с целью повышения общей защищенности предприятия.

Таким образом можно сделать вывод, что хоть системы предотвращения и являются необходимым компонентом эшелонированной обороны предприятия, но использование данных систем не защищает

сеть организации на 100%. Информационная безопасность должна быть комплексной, поэтому необходимо брать во внимание и другие ее факторы, такие как обновление программного обеспечения, настройка межсетевого экрана, предоставление безопасного удаленного доступа к ресурсам предприятия и т.д. Однако, показанный в работе метод, позволяет оценить общий уровень защищенности системой предотвращения вторжений и определить объекты, требующие дополнительных мер по защите.

Литература

1. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. - 4-е изд. - СПб.: Питер, 2020. - 448 с.

2. Код безопасности. Продукты. Континент 4. [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/products/kontinent-4/, свободный. (дата обращения 24.10.2021)

3. Руководство по эксплуатации Metasploit. [Электронный ресурс]. – Режим доступа: https://docs.rapid7.com/metasploit, свободный. (дата обращения 25.10.2021)

4. OWASP. [Электронный ресурс]. – Режим доступа: https://owasp.org/, свободный. (дата обращения 30.10.2021)

References

1. Parasram Shiva, Zamm Aleks, Kheriyanto Tedi, Ali Shakil, Budu Damian, Yokhansen Dzherard, Allen Li. Kali Linux. Testirovaniye na proniknoveniye i bezopasnost'. - 4-ye izd. - SPb.: Piter, 2020. - 448 s.

2. Kod bezopasnosti. Produkty. Kontinent 4. [Elektronnyy resurs]. – Rezhim dostupa: https://www.securitycode.ru/products/kontinent-4/, svobodnyy. (data obrashcheniya 24.10.2021)/

3. Rukovodstvo po ekspluatatsii Metasploit. [Elektronnyy resurs]. – Rezhim dostupa: https://docs.rapid7.com/metasploit, svobodnyy. (data obrashcheniya 25.10.2021)/

4. OWASP. [Elektronnyy resurs]. – Rezhim dostupa: https://owasp.org/, svobodnyy. (data obrashcheniya 30.10.2021)/

ЛЕБЕДЕВ Дмитрий Валерьевич, студент кафедры информационных технологий и защиты информации, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: dmvlebedev@mail.ru

LEBEDEV Dmitriy Valerievich, student of the Department of Information Technology and Information Security, Ural State University of Railway Transport. 66 Kolmogorova str., Yekaterinburg, 620034. E-mail: dmvlebedev@mail.ru

ГУЗЕНКОВА Елена Алексеевна, старший преподаватель кафедры информационных технологий и защиты информации, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: sato-hany@ya.ru

GUZENKOVA Elena Alekseevna, Senior Lecturer of the Department of Information Technology and Information Security, Ural State University of Railway Transport. 66 Kolmogorova str., Yekaterinburg, 620034. E-mail: sato-hany@ya.ru

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(43) / 2022
Подписано в печать 30.03.2022.
Дата выхода в свет 30.03.2022. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 8.57. Тираж 100 экз.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(43) / 2022
Signed to print March 30, 2022.
Date of publication of the 30.03.2022. Format 70×108 1/16. Screen printing.
Conventional printed sheet 8.57. Circulation – 100 issues. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080