УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 22–29

Карелова О.Л., Лисин Г.А.

DOI: 10.14529/secur240103

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕЖСЕТЕВЫХ ЭКРАНОВ НОВОГО ПОКОЛЕНИЯ

В статье проведен сравнительный анализ межсетевых экранов нового поколения, реализованных в виде программно-аппаратных комплексов. Рассмотрены представленные на отечественном рынке варианты таких средств защиты информации, а также отобраны критерии их сравнения.

Для нахождения оптимального решения из имеющихся альтернатив использован метод анализа иерархий, учитывающий субъективную важность выбранных критериев.

В ходе исследования продемонстрирована эффективность данного метода в ситуациях, когда сравнение ведется по совокупности критериев и нет явного лидера по каждому из них.

По результатам анализа предложено воспользоваться многоступенчатым подходом для сравнения межсетевых экранов нового поколения. Прежде всего необходимо выбрать желаемую реализацию данных средств защиты (в виде программного обеспечения или программно-аппаратного комплекса) и определить подлежащую защите информации. На основании этих сведений следует отобрать необходимые критерии, по которым ведется сравнение, добавив в качестве одного из них полноту программного функционала, после чего целесообразно обратиться к методу анализа иерархий.

Ключевые слова: *информационная безопасность, средства защиты информации, межсетевой экран, UTM, NGFW, метод анализа иерархий, программно-аппаратный комплекс.*

Karelova O.L., Lisin G.A.

COMPARATIVE ANALYSIS OF NEW GENERATION FIREWALLS

The article provides a comparative analysis of new generation firewalls implemented in the form of software and hardware complexes. The variants of such information protection tools presented on the domestic market were reviewed, and criteria for their comparison were selected.

To find the most optimal solution from the available alternatives, the hierarchy analysis method was applied, taking into account the subjective importance of the selected criteria.

The study demonstrated the effectiveness of this method in situations where the comparison is based on a set of criteria and there is no clear leader for each of them.

Based on the results of the analysis, it was proposed to use a multi-step approach to compare new generation firewalls. First of all, it is necessary to choose the desired implementation

of these security measures (in the form of software or hardware and software complex) and determine the information to be protected. Based on this information, it is necessary to select the necessary criteria for comparison, adding the completeness of the software functionality to one of them, after which it is advisable to turn to the analytic hierarchy process.

Keywords: *information security, information security tools, firewall, UTM, NGFW, analytic hierarchy process, hardware and software complex.*

Введение

В настоящее время, как показывают недавние исследования [1], основную угрозу для бесперебойного функционирования корпоративных сетей организаций представляют вредоносные программы и направленные атаки, приводящие к сбоям в работе информационной системы компаний вне зависимости от формы их собственности и размера. Чтобы обезопасить внутренние ресурсы предприятий, ИТ-специалисты прибегают к различным организационным и техническим мерам. Одной из таких мер является внедрение различных средств программно-аппаратной защиты: систем защиты информации от несанкционированного доступа, антивирусных программ, межсетевых экранов, систем обнаружения и предотвращения вторжений, средств криптографической защиты информации и некоторых других [2].

В данной статье рассмотрено одно из таких средств – межсетевые экраны (файрволы, брандмауэры). В классическом понимании они представляют собой комплекс, предназначенный для защиты сети от различных видов угроз и атак путем контроля и фильтрации проходящего через него сетевого трафика. Файрволы работают на основе ряда правил и политик безопасности, которые определяют, в зависимости от адреса отправителя, используемых сетевых сервисов, портов и протоколов, какие пакеты могут свободно передаваться по сети, а какие должны блокироваться [3]. Кроме того, межсетевые экраны могут выполнять функцию NAT (Network Address Translation), сохраняя количество общедоступных адресов, используемых в компании, а также позволяя более строго контролировать доступ к ресурсам как с внутренней, так и с внешней стороны брандмауэра.

Однако помимо классических файрволов существуют их более усовершенствованные аналоги – универсальные шлюзы безопасности (UTM – Unified Threat Management) и межсетевые экраны нового поколения (NGFW – Next Generation Firewall). Строго говоря, между ними есть небольшая разница: несмотря на то, что они выполняют одни и те же функции, системы NGFW являются многопоточными, в то время как UTM-решения работают с одним потоком, что можно расценивать как их недостаток [4]. На практике же для многих компаний эта разница не является существенной, поэтому при принятии решения о приобретении данных средств защиты их рассматривают совместно, а выбор между ними осуществляется по принципу соотношения желаемой организацией функциональности к оптимальной для нее, с точки зрения пользователя, производительности.

В общем случае класс UTM/NGFW-решений сочетает в себе как базовые возможности привычного многим файрвола, так и некоторый дополнительный функционал: построение защищенных каналов связи (VPN), антивирусная фильтрация, обнаружение и предотвращение вторжений, инспектирование SSL трафика, контроль приложений, контент-фильтрация [5], благодаря которому снижается количество компонентов, необходимое для обеспечения информационной безопасности в целом. Наглядно сравнение функционала классических межсетевых экранов и решений следующего поколения представлено в табл. 1.

Так как межсетевые экраны нового поколения обладают рядом преимуществ по сравнению с классическими файрволами, многие компании, особенно крупные, отдают предпочтение именно более современным вариантам.

Отбор альтернатив

На сегодняшний день класс UTM/NGFW-решений представлен в виде программных и программно-аппаратных комплексов. Однако для того, чтобы не зависеть от технических характеристик компьютера или сервера, на которые устанавливается защитное программное обеспечение, для данного исследования был выбран исключительно второй вариант реализации межсетевых экранов нового поколения. Кроме того, анализ был ограничен крупными корпоративными решения-

Таблица 1

Сравнение файрволов с UTM/NGFW-решениями

Характеристика	Классический файрвол	Межсетевые экраны нового поколения
Контроль пакетов	✓	✓
Фильтрация трафика	✓	✓
NAT	✓	✓
VPN	×	✓
Антивирус	×	✓
Система обнаружения и предотвращения вторжений	×	✓
Инспектирование SSL трафика	×	✓
Контроль приложений	×	✓
Контент-фильтрация	×	✓
Глубокая инспекция пакетов	×	✓

ми с максимальной производительностью, рассчитанными на наибольшее число пользователей, так как малые и средние предприятия прибегают зачастую к классическим файрволам ввиду низкой стоимости последних.

В результате были отобраны и рассмотрены следующие альтернативы современных шлюзов безопасности:

A1 – Континент 4 IPC-R3000 от ООО «Код Безопасности» – российский межсетевой экран, обеспечивающий комплексную защиту сети. Данное решение гарантирует стабильно высокую пропускную способность и фиксированное время обработки данных вне зависимости от интенсивности трафика и количества правил. Имеет действующий сертификат ФСТЭК России [6].

A2 – UserGate F8000 от ООО «Юзергейт» – еще один отечественный межсетевой экран нового поколения, который работает на мощных платформах и процессорах, обеспечивая эффективность выполнения множества защитных функций даже для большого числа пользователей. В его состав входят все необходимые инструменты для защиты корпоративной сети от современных видов угроз и атак. Кроме того, он также сертифицирован ФСТЭК России [7].

A3 – ViPNet xFirewall 5 xF5000 Q2 от АО «ИнфоТеКС» – также российский современный шлюз безопасности, сочетающий в себе функции классического межсетевого экрана с расширенными функциями анализа и фильтрации трафика. Данное средство защиты информации также позволяет создать гранулированную политику безопасности на основе учетных записей пользователей. Является сертифицированным ФСТЭК России средством защиты [8, 9].

A4 – Traffic Inspector Next Generation L1500+-AQ от ООО «СМАРТ-СОФТ» – отечественный универсальный шлюз безопасности, который может являться единственным самодостаточным средством защиты сети организации. Одним из его главных достоинств является простота настройки, благодаря которой данное решение может начать полноценно функционировать за достаточно короткое время. Имеет сертификат соответствия ФСТЭК России [10].

A5 – Zyxel USG FLEX 700H от тайваньской компании Zyxel – данный универсальный шлюз безопасности обеспечивает достаточно хорошую производительность в UTM режиме, а также многоуровневую защиту сетевой инфраструктуры и подключенных пользователей. Такая максимальная производительность достигается за счет многоядерного процессора нового поколения, технологии Fastpath, а также новой операционной системы [11].

A6 – Dionis DPS-7000 от ООО «Фактор-ТС» – российский программно-аппаратный комплекс, выполняющий различные функции и позволяющий решать задачи разной степени сложности: от предоставления безопасного доступа в Интернет сотрудникам компании до объединения множества филиалов организации в единую защищенную сеть. Его преимуществами выступают высокий уровень производительности и надежность ядра сети организации. Отличительной особенностью данного решения является наличие действующих сертификатов соответствия не только ФСТЭК России, но и ФСБ России [12].

A7 – Ideco EX от ООО «Айдеко» – передовая отечественная модель, разработанная специально для крупных корпораций с количеством пользователей больше 3000. Как и другие представленные на российском рынке аналоги, данная платформа защищает сеть компании от внутренних и внешних угроз, обеспечивает анализ и фильтрацию трафика, позволяет наращивать ресурсы вычислительной системы, а также выполняет иные функции безопасности. Данное средство защиты также сертифицировано ФСТЭК России [13].

Подбор критериев

Следующий этап исследования посвящен выявлению присущих всем отобранным UTM/NGFW-решениям характеристик, которые являются наиболее важными с точки зрения производительности и информационной безопасности.

K1 – полнота программного функционала. Это один из наиболее существенных параметров при сравнении вышеупомянутых альтернатив. Так как межсетевые экраны нового поколения характеризуются разнообразными свойствами, среди них были выделены десять наиболее сопоставимых опций, являющихся ключевыми для данных решений. Все альтернативы были проанализированы на предмет наличия («1») или отсутствия («0») отобранных функций, после чего был рассчитан процент ненулевых характеристик относительно общего их числа – это и есть искомое значение K1 по каждой из альтернатив. Наглядно данное сравнение UTM/NGFW-решений представлено в табл. 2.

Таблица 2

Сравнение альтернатив по программным характеристикам

Характеристика	A1	A2	A3	A4	A5	A6	A7
Контроль пакетов и фильтрация трафика	1	1	1	1	1	1	1
VPN	1	0	0	1	1	1	1
Антивирус	0	1	1	1	1	1	1
Глубокая инспекция пакетов	1	1	1	1	0	0	0
Система обнаружения и предотвращения вторжений	1	1	1	1	1	1	1
Контент-фильтрация	1	1	1	1	1	0	1
Контроль приложений	1	1	1	1	1	0	1
Инспектирование SSL трафика	1	1	1	1	1	1	1
Отказоустойчивость	1	1	1	1	0	1	1
Двухфакторная аутентификация	0	1	0	1	1	0	1
Полнота программного функционала, %	80	90	80	100	80	60	90

Остальные критерии характеризуют производительность и масштабируемость межсетевых экранов нового поколения.

K2 – производительность в режиме межсетевого экрана. Данный параметр определяет скорость и эффективность обработки сетевого трафика и потому является достаточно важным при выборе UTM/NGFW-решения.

K3 – производительность в комбинированном режиме. Это очень важный критерий, так как от его величины зависит возможность совмещения высоких сетевых нагрузок с обеспечением достаточного уровня безопасности.

K4 – максимальное рекомендуемое количество пользователей. Данный критерий имеет немаловажное значение для крупных компаний, так как в случае увеличения числа их сотрудников требуется масштабируемость такого сетевого решения.

K5 – удельная производительность при максимальной нагрузке в комбинированном режиме. Данный критерий получается как частное от деления K3 на K4 и вводится для определения достаточности заявленной наибольшей производительности при максимальной нагрузке на сеть.

Набор данных

Для дальнейшего анализа необходимо свести воедино как значения критерия K1, рассчитанные в предыдущем разделе, так и значения других критериев, взятые из паспортов программно-аппаратных комплексов соответствующих производителей. Полученный набор данных отражен в табл. 3.

Данные значения будут использованы в

Таблица 3

Значения альтернатив по критериям

	К1, %	К2, Гбит/с	К3, Гбит/с	К4, чел.	К5, Мбит/с
А1	80	50	8	3 000	2,67
А2	90	60	8	10 000	0,8
А3	80	45	1,531	6 000	0,26
А4	100	25	1,2	1 500	0,8
А5	80	15	4	4000	1
А6	60	90	8	2000	4
А7	90	42	5	3000	1,67

следующем разделе для проведения непосредственно сравнительного анализа.

Сравнение методом анализа иерархий

В проведенных ранее исследованиях [14] уже был проведен анализ межсетевых экранов нового поколения методом простой ранжировки по нескольким критериям, однако в данной статье для целей сравнения использовался метод анализа иерархий.

В рамках этого метода прежде всего нужно проранжировать отобранные критерии в соответствии с субъективной оценкой их важности [15]. В результате критерии К1-К5 были упорядочены так, как показано в табл. 4, после чего с учетом этих значений был получен вектор приоритетов для критериев ($\overline{a}$).

Следующим этапом данного метода является ранжирование альтернатив по выбран-

Таблица 4

Ранжирование критериев

Критерий	К1	К2	К3	К4	К5
Ранг	4	2	1	5	3
$\overline{a}$	0,10551249	0,2713178	0,3875969	0,0590009	0,17657192

ным критериям на основании числовых параметров, приведенных в таблице 3. Результат представлен в таблице 5.

Приведенные выше данные позволяют получить векторы приоритетов для альтернатив ($\overline{b_i}$) по каждому из пяти критериев, что в дальнейшем даст возможность перейти уже к заключительному этапу исследования, по результатам которого будет выявлено наиболее оптимальное решение.

Результаты исследования

Все полученные на предыдущем этапе анализа значения векторов приоритетов $\overline{a}$, $\overline{b_1}$, $\overline{b_2}$, $\overline{b_3}$, $\overline{b_4}$ и $\overline{b_5}$ сводятся в итоговую таблицу, на основании которой определяются искомые приоритеты альтернатив, что наглядно показано в таблице 6.

Данные итоговой таблицы позволяют окончательно проранжировать выбранные для анализа решения следующим образом:

1. Dionis DPS-7000 (А6);
2. UserGate F8000 (А2);
3. Континент 4 IPC-R3000 (А1);
4. Ideco EX (А7);
5. ViPNet xFirewall 5 xF5000 Q2 (А3);
6. Zyxel USG FLEX 700H (А5);

Таблица 5

Ранжирование альтернатив по критериям

	К1	К2	К3	К4	К5
А1	4	3	1	4	2
А2	2	2	1	1	5
А3	4	4	6	2	7
А4	1	6	7	7	5
А5	4	7	5	3	4
А6	7	1	1	6	1
А7	2	5	4	4	3

Таблица 6

Итоговая таблица

$\bar{a}$	0,10551249	0,2713178	0,3875969	0,0590009	0,17657192	Приоритеты
A1	0,09316335	0,1744857	0,2507642	0,1129243	0,23452822	0,20244015
A2	0,20594004	0,2369332	0,2507642	0,3023758	0,07188385	0,213742
A3	0,09316335	0,12214	0,0434658	0,2295816	0,02775659	0,07826242
A4	0,28243205	0,0490397	0,0251958	0,0281044	0,07188385	0,06722213
A5	0,09316335	0,0285737	0,071217	0,16612	0,11535738	0,07535605
A6	0,02619781	0,3085642	0,2507642	0,0479695	0,30889083	0,2410503
A7	0,20594004	0,0802634	0,1078286	0,1129243	0,16969928	0,12192694

7. Traffic Inspector Next Generation L1500+-AQ (A4).

Таким образом, на основе полученных методом анализа иерархий результатов модель программно-аппаратного межсетевого экрана нового поколения Dionis DPS-7000 является наиболее оптимальным выбором с точки зрения функциональной полноты и аппаратной производительности.

Однако стоит отметить, что представленный в данном исследовании перечень критериев не является исчерпывающим и не учитывает цели внедрения того или иного средства защиты информации. В случае, если целью является защита коммерческой тайны, имеет смысл рассмотреть в качестве одного из критериев критерий стоимости, присвоив ему ранг в соответствии со степенью важности данного критерия для конкретной организации. В тех же случаях, когда речь идет о защите персональных данных, сведений, составляющих государственную тайну, и иной информации, обрабатываемой в информационных или автоматизированных системах определенного уровня защищенности, необходимо в обязательном порядке включить в перечень критериев критерий наличия сертификата ФСТЭК России или ФСБ России, подтверждающим соответствие средств защиты информации предъявляемым к ним требованиям, и присвоить ему наивысший ранг.

Кроме того, необходимо принять во внимание субъективность результатов данного метода принятия решений, несмотря на его структурированность и системность. Это обусловлено особенностью самого метода анализа иерархий, в основе которого лежит отбор и последующее ранжирование необходимых критериев, по которым будет производиться оценка рассматриваемых альтернатив. В большинстве же случаев выбираемые параметры и присваиваемые им ранги зависят исключительно от предпочтений того, кто принимает решение, и потому не существует однозначного способа подбора и упорядочения критериев по степени их важности.

Заключение

Проведенное исследование показывает необходимость в многоступенчатой методике подбора межсетевого экрана нового поколения. Для начала следует определиться с необходимой реализацией данного средства защиты, которое может быть представлено как в виде специализированного программного обеспечения, так и в виде программно-аппаратного комплекса, а также принять решение о том, какая информация подлежит защите. На основании этого должны быть отобраны те критерии, по которым будет вестись сравнение, при этом в случае программно-аппаратных комплексов важно учитывать не только характеристики аппаратной платформы, но и некоторые программные критерии, как, например, полнота программного функционала. На заключительном этапе стоит воспользоваться методом анализа иерархий, который при всей своей зависимости от ранжирования критериев позволяет в случае правильной расстановки приоритетов сделать оптимальный выбор.

Литература

1. Барыбина А.З. Моделирование угроз информационной безопасности сценарным подходом. // Естественно-гуманитарные исследования, 2022. № 4 (42). С. 35–44.

2. Малий Ю.В., Прокушев Я.Е. Концептуальная модель выбора средств программно-аппаратной защиты. // Computational nanotechnology, 2020. № 1. С. 63–71. DOI: 10.33693/2313-223X-2020-7-1-63-71.

3. Орехов А.В., Орехов А.А. Автоматическое обнаружение аномалий сетевого трафика при DDoS-

атаках. // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления, 2023. Том 19. № 2. С. 251–263. DOI: 10.21638/11701/spbu10.2023.210.

4. Баранов А.В., Корепанов П.М., Кузнецов Е.Е. Обеспечение информационной безопасности научного суперкомпьютерного центра. // Программные продукты и системы, 2023. Том 36. № 4. С. 615–631. DOI: 10.15827/0236-235X.142.615-631.

5. Бирюков А.С. Защита информации в компьютерной сети предприятия. // Молодой ученый, 2020. № 15 (305). С. 81–84.

6. Код Безопасности. Континент 4. Доступно по: https://www.securitycode.ru/products/kontinent-4/?tab=models (дата обращения: 04.03.2024).

7. UserGate. UserGate. Доступно по: https://www.usergate.com/ru/products/usergate-f (дата обращения: 04.03.2024).

8. ИнфоТэКС. ViPNet xFirewall 5. Доступно по: https://infotecs.ru/products/vipnet-xfirewall-5/ (дата обращения: 04.03.2024).

9. Родионычева Е.Д., Голубев А.С. Оценка стоимости приобретения программно-аппаратного комплекса для обеспечения информационной безопасности информационных систем в сфере здравоохранения. // Известия высших учебных заведений. Серия «Экономика, финансы и управление производством» [Ивэкофин], 2021. № 3 (49). С. 124-129. DOI: 10.6060/ivecofin.2021493.558.

10. Смарт-Софт. Traffic Inspector Next Generation. Доступно по: https://www.smart-soft.ru/ (дата обращения: 04.03.2024).

11. Zyxel. Zyxel. Доступно по: https://www.zyxel.com/ru/ru/products/next-gen-firewall/usg-flex-firewall-usg-flex-700h/license-and-spec (дата обращения: 04.03.2024).

12. Фактор-ТС. Dionis. Доступно по: https://dps.factor-ts.ru/produkciya/utm-dionis-dps/dionis-dps-5000-6000-7000-series/#anchor2 (дата обращения: 04.03.2024).

13. Ideco. Ideco. Доступно по: https://ideco.ru/apparatnye-resheniya#!/tproduct/596522077-1685701471282 (дата обращения: 04.03.2024).

14. Шаханова М.В., Четверик М.А., Шаханова В.С. Сравнение различных характеристик отечественных файрволов. // Международный журнал информационных технологий и энергоэффективности, 2024. Том 9. № 1 (39). С. 90–95.

15. Саати Т.Л. Принятие решений: Метод анализа иерархий // Пер. с англ. Вачнадзе Р.Г. // – М.: Радио и связь; 1993. – 314 с.

References

1. Barybina A.Z. Modelirovaniye ugroz informatsionnoy bezopas-nosti stsenarnym podkhodom. // Yestestvenno-gumanitarnyye issledovaniya, 2022. № 4 (42). S. 35–44.

2. Maliy YU.V., Prokushev YA.Ye. Kontseptual'naya model' vybora sredstv programmno-apparatnoy zashchity. // Computational nanotechnology, 2020. № 1. S. 63–71. DOI: 10.33693/2313-223X-2020-7-1-63-71.

3. Orekhov A.V., Orekhov A.A. Avtomaticheskoye obnaruzheniye anoma-liy setevogo trafika pri DDoS-atakakh. // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaya matematika. Informatika. Protsessy upravleniya, 2023. Tom 19. № 2. S. 251–263. DOI: 10.21638/11701/spbu10.2023.210.

4. Baranov A.V., Korepanov P.M., Kuznetsov Ye.Ye. Obespecheniye in-formatsionnoy bezopasnosti nauchnogo superkomp'yuternogo tsentra. // Programmnyye produkty i sistemy, 2023. Tom 36. № 4. S. 615–631. DOI: 10.15827/0236-235X.142.615-631.

5. Biryukov A.S. Zashchita informatsii v komp'yuternoy seti pred-priyatiya. // Molodoy uchenyy, 2020. № 15 (305). S. 81–84.

6. Kod Bezopasnosti. Kontinent 4. Dostupno po: https://www.securitycode.ru/products/kontinent-4/?tab=models (data ob-rashcheniya: 04.03.2024).

7. UserGate. UserGate. Available at: https://www.usergate.com/ru/products/usergate-f (accessed 04.03.2024).

8. InfoTeKS. ViPNet xFirewall 5 [Infotecs. ViPNet xFirewall 5]. Available at: https://infotecs.ru/products/vipnet-xfirewall-5/ (accessed 04.03.2024).

9. Rodionycheva Ye.D., Golubev A.S. Otsenka stoimosti priobreteniya programmno-apparatnogo kompleksa dlya obespecheniya informatsionnoy bezopasnosti informatsionnykh sistem v sfere zdravookhraneniya. // Iz-vestiya vysshikh uchebnykh zavedeniy. Seriya «Ekonomika, finansy i upravleniye proizvodstvom» [Ivekofin], 2021. № 3 (49). S. 124-129. DOI: 10.6060/ivecofin.2021493.558.

10. Smart-Soft. Traffic Inspector Next Generation. Available at: https://www.smart-soft.ru/ (accessed 04.03.2024).

11. Zyxel. Zyxel. Available at: https://www.zyxel.com/ru/ru/products/next-gen-firewall/usg-flex-firewall-usg-flex-700h/license-and-spec (accessed 04.03.2024).

12. Faktor-TS. Dionis. Available at: https://dps.factor-ts.ru/produkciya/utm-dionis-dps/dionis-dps-5000-6000-7000-series/#anchor2 (accessed 04.03.2024).

13. Ideco. Ideco. Available at: https://ideco.ru/apparatnye-resheniya#!/tproduct/596522077-1685701471282 (accessed 04.03.2024).

14. Shakhanova M.V., Chetverik M.A., Shakhanova V.S. Sravneniye raz-lichnykh kharakteristik otechestvennykh fayrvolov. // Mezhdunarodnyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti, 2024. Tom 9. № 1 (39). S. 90–95.

15. Saati T.L. Prinyatiye resheniy: Metod analiza iyerarkhiy // Per. s angl. Vachnadze R.G. // – M.: Radio i svyaz'; 1993. – 314 s

КАРЕЛОВА Оксана Леонидовна, доктор физико-математических наук, доцент, профессор кафедры «Международная информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный лингвистический университет». 119034, г. Москва, ул. Остоженка, 38, стр. 1.; Профессор кафедры «Прикладные информационные технологии» федерального государственного бюджетного образовательного учреждения высшего образования «Президентская академия». 119571, г. Москва, проспект Вернадского, 82, стр. 1. E-mail: okarelova@yandex.ru

KARELOVA Oksana Leonidovna, Doctor of Physical and Mathematical Sciences, Associate Professor, Professor at the Department of International Information Security of the Federal State Budgetary Educational Institution of Higher Education «Moscow State Linguistic University». 119034, Moscow, Ostozhenka str., 38, bld. 1.; Professor at the Department of Applied Information Technologies of the Federal State Budgetary Educational Institution of Higher Education «Presidential Academy». 119571, Moscow, Vernadskogo ave., 82, bld. 1. E-mail: okarelova@yandex.ru

ЛИСИН Георгий Андреевич, обучающийся 4-го курса направления подготовки «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный лингвистический университет». 119034, г. Москва, ул. Остоженка, 38, стр. 1. E-mail: gal060303@gmail.com

LISIN Georgiy Andreevich, student of the 4th year of the training course «Information Security» of the Federal State Budgetary Educational Institution of Higher Education «Moscow State Linguistic University». 119034, Moscow, Ostozhenka str., 38, bld. 1. E-mail: gal060303@gmail.com