УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2016 Том 16 № 1 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2016 Vol. 16 No 1 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.75

ВЫБОР ВАРИАНТА ПОСТРОЕНИЯ МНОГОУРОВНЕВОГО ЗАЩИЩЕННОГО ДОСТУПА К ВНЕШНЕЙ СЕТИ

В.С. Коломойцев[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: Dek-s-kornis@yandex.ru

Информация о статье
Поступила в редакцию 25.08.15, принята к печати 07.12.15
doi:10.17586/2226-1494-2016-16-1-115-121
Язык статьи – русский

Ссылка для цитирования: Коломойцев В.С. Выбор варианта построения многоуровневого защищенного доступа к внешней сети // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 1. С. 115–121.

Аннотация

В работе исследуется выбор оптимального варианта построения схемы доступа «Прямое соединение». Данная схема служит для организации безопасного доступа к ресурсам внешней сети и состоит из нескольких групп маршрутизаторов и трех видов межсетевых экранов. Схема рассмотрена с учетом того, что в системе для различных средств защиты имеются общие зоны устранения угроз в канале. Для каждого из вариантов построения схемы доступа получены показатели среднего времени пребывания запроса в системе и вероятность безотказной работы. На основании полученных результатов было произведено сравнение вариантов построения схемы доступа между собой и с вариантом построения стандартной схемы доступа (включающей один межсетевой экран). Было выявлено, что вариант построения схемы доступа с единственной группой маршрутизаторов на всю систему обладает более высокой производительностью и надежностью, чем остальные варианты схемы «Прямое соединение».

Ключевые слова

отказоустойчивость, межсетевые экраны, сетевая организация, информационная безопасность, оптимизация, защита информации, надежность, производительность сети, схемы доступа, несанкционированный доступ.

Благодарности

Выражаю благодарность профессору В.А. Богатыреву за помощь в ходе исследования.

CHOICE OF OPTION FOR IMPLEMENTATION OF THE MULTILEVEL SECURE ACCESS TO THE EXTERNAL NETWORK

V.S. Kolomoitcev[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: Dek-s-kornis@yandex.ru

Article info
Received 25.08.15, accepted 07.12.15
doi:10.17586/2226-1494-2016-16-1-115-121
Article in Russian

For citation: Kolomoitcev V.S. Choice of option for implementation of the multilevel secure access to the external network. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 1, pp. 115–121.

Abstract

We study the optimal way for design of access scheme called "Direct Connection. This scheme provides a secure access to external network resources, and consists of several groups of routers and two kinds of firewalls. The scheme is considered in view of the fact that the system has got common areas of removing threats in the channel for different means of protection. Parameters of average residence time of request in the system and its reliability were obtained for each variant of access scheme. Based on the results, comparison of the ways of design for access scheme was carried out between themselves and with the standard access scheme (with one firewall). It was found out that design of access scheme with a single group of routers for the whole system has better performance and reliability than the other variants of "Direct Connection" access scheme.

Keywords

fault tolerance, firewalls, network organization, information security, optimization, information protection, reliability, network performance, access schemes, unauthorized access

Acknowledgements

I would like to express my gratitude to V.A. Bogatyrev for his assistance during the study.

Введение

Проблема защиты информации, использующейся в современных сложных вычислительных системах, стоит очень остро. Такие системы могут быть подключены как к корпоративным сетям, так и к сетям общего доступа, в результате чего они могут быть подвержены угрозам несанкционированного доступа (НСД), отказа узлов в обслуживании, потери информации и иным угрозам безопасности информации. Любая из вышеописанных угроз может привести к значительным экономическим и иным потерям, а значит, необходимо свести вероятность их возникновения в системе к минимуму [1–3].

Схемы организации защищенного подключения корпоративной сети к сетям общего пользования во многом определяют безопасность, надежность и производительность всей вычислительной сети в целом. Для обеспечения высоких показателей производительности, надежности и отказоустойчивости защищенного доступа к сети средства защиты могут объединяться в кластеры [4–9]. Вопросы организации узлов в кластеры рассмотрены в работах [10, 11]. Механизмы распределения запросов в кластерах известны, и их исследование выходит за рамки настоящей работы, в которой издержками на диспетчеризацию запросов будем пренебрегать.

Для достижения наиболее высокого уровня безопасности, надежности и производительности вычислительной системы вопрос применения той или иной схемы защищенного доступа должен решаться еще на этапе проектирования самой вычислительной системы. К сожалению, применимость схемы доступа в уже спроектированной вычислительной системе, в состав которой входит множество связующих и оконечных узлов, оценить затруднительно [12–16]. В результате, чтобы повысить уровень безопасности и надежности современных разнородных вычислительных систем с сохранением их производительности, необходимо использовать такие схемы безопасного доступа, которые бы минимально зависели от существующей архитектуры вычислительной системы [17, 18]. Такой схемой может стать схема безопасного доступа к ресурсам внешней (менее защищенной или неконтролируемой нами) сети «Прямое соединение».

В настоящей работе рассмотрены варианты построения схемы безопасного доступа к ресурсам внешней сети «Прямое соединение», способной посредством входящих в нее аппаратно-программных средств бороться с различными видами угроз информационной безопасности. В работе ставится задача поиска наиболее производительной конфигурации схемы доступа с сохранением приемлемого уровня надежности вычислительной системы. Будем считать, что система работает в нормальном режиме, и через канал связи, помимо полезной информации, в сеть поступает часть информации (вирусы, поврежденные пакеты и т.д.), которую требуется устранять.

Варианты объединения средств защиты в отказоустойчивые кластеры в схеме доступа «Прямое соединение», рассмотренные в работе [19], предполагают, что каждое из устройств способно бороться только с определенным для него кругом угроз. В предлагаемой работе рассмотрены системы со схемой доступа «Прямое соединение», когда для различных средств защиты имеются общие зоны устранения угроз в канале (т.е. каждое из устройств системы имеет возможность устранять часть угроз, которые способно определять и устранять другое устройство в составе схемы).

Схема «Прямое соединение»

Схема «Прямое соединение» предназначена для организации безопасного доступа узлов внутренней сети к объектам, находящимся в неподконтрольных или же в малозащищенных участках сети. Использование такой схемы предполагает минимальные изменения в архитектуре корпоративной сети, а также минимальные дополнительные финансовые затраты на ее внедрение. Структура схемы «Прямое соединение» представлена на рис. 1.

Схема доступа «Прямое соединение» имеет трехуровневую архитектуру, основанную на разных видах межсетевых экранов (МЭ) [19]. На входе во внутреннюю сеть для создания первого уровня защиты устанавливается МЭ с фильтрацией пакетов (МЭ-1), основной функциональной задачей которых является фильтрация поступающих на вход данных от нежелательных сообщений (спама) и снижение риска DDoS-атак в вычислительной системе. Зачастую имеющиеся в составе схемы маршрутизаторы могут реализовывать функционал МЭ с фильтрацией пакетов [20]. Однако ввиду того, что архитектура вычислительной системы, в которую будет внедряться схема доступа, заранее неизвестна, маршрутизатор и МЭ учитываются как разные элементы системы, где маршрутизатор (как элемент) предназначен в первую очередь для связи частей системы друг с другом, а МЭ-1 фильтрует трафик в вычислительной системе. В ином случае маршрутизаторы, используемые в схеме для связи МЭ системы между собой, могут быть объединены в единый кластер и заменены на кластер из МЭ с фильтрацией пакетов.

Через маршрутизатор к МЭ-1 подключен МЭ с адаптивной проверкой пакетов (МЭ-2), выполняющий задачу более глубокого анализа содержимого в канале [20]. Он является вторым уровнем защиты системы и выполняет тщательный поиск угроз в каждом из поступающих в сеть пакетов [19]. С учетом того, что на вход МЭ-2 будет поступать меньше данных, чем на вход МЭ-1 (так как часть данных будет

отфильтрована МЭ-1), нагрузка на данный МЭ будет меньше и, следовательно, производительность самой сети выше.

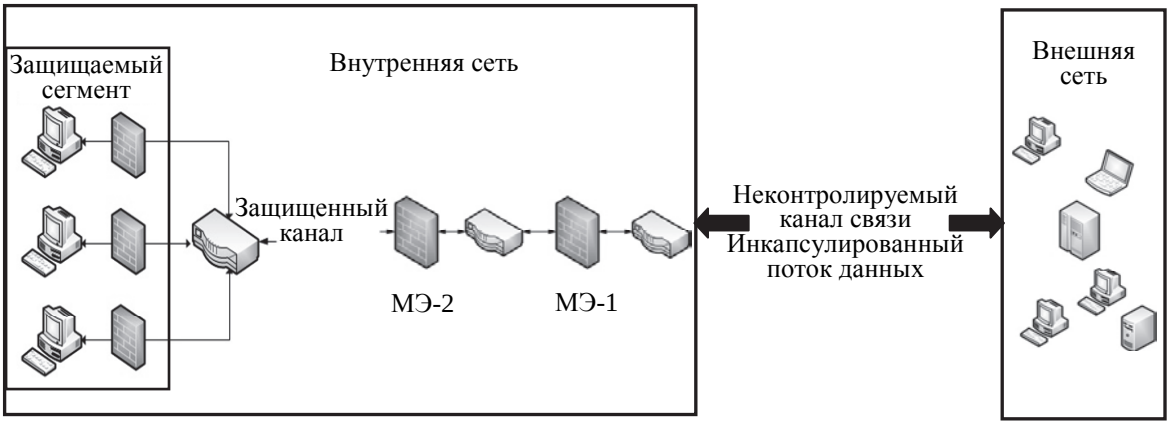

Рис. 1. Схема «Прямое соединение»

После прохождения МЭ-2 потенциально «чистые» данные поступают на адресуемый оконечный узел. На данном узле предусмотрена установка антивирусного средства (АВС) со встроенным в него МЭ (персональный МЭ), система защиты от НСД и организация защищенного хранилища (в целях хранения конфиденциальных данных, если это требуется). Указанные элементы входят в третий (персональный) уровень защиты системы [19]. В данной схеме доступа канал передачи данных должен быть защищенным, что способствует снижению, а в идеале предотвращению возможности влияния злоумышленника на данные, курсирующие в канале.

Выбор алгоритмов шифрования и средств, обеспечивающих выполнение тех или иных функций в данной схеме, осуществляется в соответствии с существующими руководящими документами.

В целях повышения общей защиты сети от DDoS-атак, потери и уничтожения данных и других аналогичных угроз критически важные узлы (как в плане сетевой архитектуры, так и в плане хранящихся на них данных) резервированы, а для данных, хранящихся на них, создаются резервные копии.

Варианты построения схемы доступа «Прямое соединение»

Для качественной и бесперебойной работы сети требуется производить резервирование узлов системы. Схема «Прямое соединение» имеет в своей сетевой архитектуре три основных составляющие (для связи оконечного узла с внешней сетью): МЭ с фильтрацией пакетов, МЭ с адаптивной проверкой пакетов и маршрутизаторы, соединяющие все элементы схемы между собой. В результате этого, в зависимости от имеющейся архитектуры вычислительной системы, схему можно построить одним из четырех способов (рис. 2):

- DC-3 – три группы маршрутизаторов для соединения всех устройств системы между собой и связи с узлами из внешней сети;
- DC-2-1 – две группы маршрутизаторов; первая группа – для соединения обеих групп МЭ и требуемых оконечных узлов, вторая – для соединения группы МЭ-1 с ресурсами из внешней сети;
- DC-2-2 – две группы маршрутизаторов; одна группа – для соединения обеих групп МЭ и связи с узлами из внешней сети, другая группа – для соединения группы МЭ-2 и оконечных узлов;
- DC-1 – одна группа маршрутизаторов для соединения с внешней сетью, соединения групп МЭ между собой и соединения с оконечными узлами.

Рассматриваемые варианты сравним со стандартной схемой доступа (STD), которая представляет собой соединение группы, содержащей n маршрутизаторов, и группы из m МЭ для обеспечения безопасного доступа к ресурсам внешней сети оконечными узлами. Стандартная схема доступа изображена на рис. 3.

Оценка надежности и среднего времени пребывания запроса в системе

Для получения минимального среднего времени пребывания запроса в системе (СВПЗС) и вычисления вероятности безотказной работы системы требуется произвести поиск кратности резервирования узлов при ограничении стоимости реализации системы C [21–23].

Ввиду того, что в настоящее время вопросы стоимости памяти или ее переполнения уже не являются критическими, каждое устройство (маршрутизатор, МЭ и т.д.) можно представить как узел сети системы массового обслуживания типа M/M/1 с бесконечной очередью, для которой среднее время пребывания запросов в системе определяется как

$$T = \frac{1/\mu}{1-\rho} = \frac{\nu}{1-\lambda/\mu} = \frac{\nu}{1-\lambda\cdot\nu},$$

где μ – интенсивность обслуживания; $\rho = \lambda/\mu$ – коэффициент использования канала; $\nu = 1/\mu$ – среднее время обслуживания запроса в узле; λ – интенсивность потока запросов. При распределении потока запросов на обслуживание в *n*-узлов интенсивность потока запросов, поступающих в каждый узел, делится на *n*. В результате среднее время пребывания запросов в системе для каждого из узлов будет равно

$$T = \frac{\nu}{1-\frac{\lambda\cdot\nu}{n}}.$$

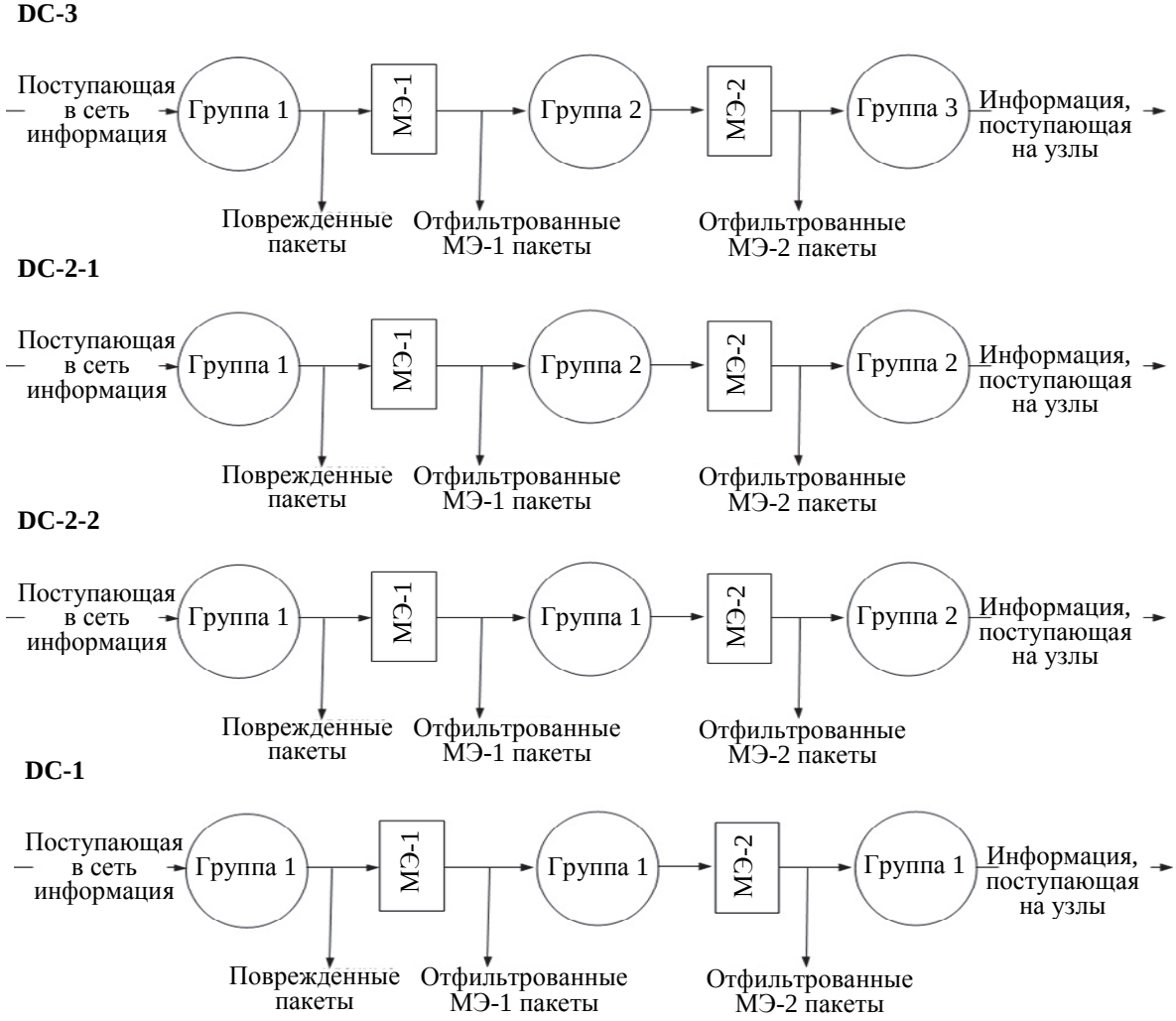

Рис. 2. Варианты сетевой архитектуры схемы «Прямое соединение»

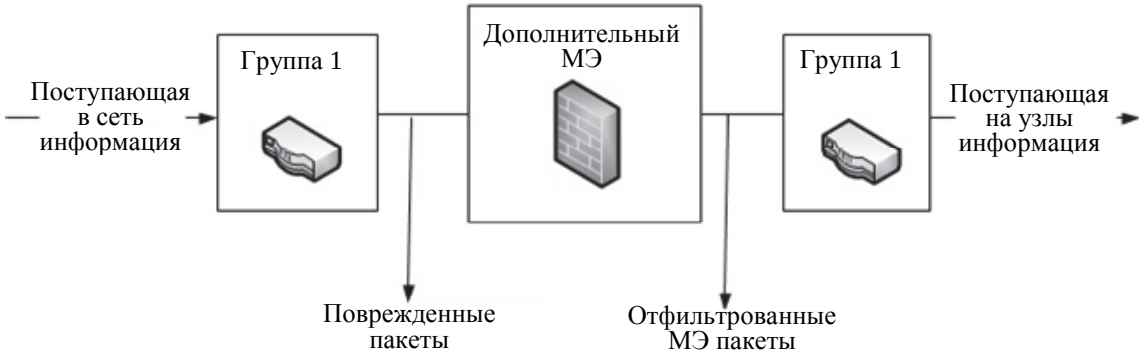

Рис. 3. Стандартная схема доступа

При прохождении запросов через несколько узлов СВПЗС определяется как сумма времен пребывания в узлах, которые последовательно задействованы в его обслуживании. Таким образом, для системы, состоящей из набора узлов, общее среднее время пребывания запросов в системе, будет определяться как $T_{\text{общ}} = \sum_i T_i$.

После прохождения маршрутизатора входной поток фильтруется, т.е. интенсивность входного потока на МЭ с фильтрацией пакетов будет ниже, чем на маршрутизаторе. То же будет происходить с входным потоком, поступающим на МЭ с адаптивной проверкой пакетов – после прохождения МЭ определенная доля входного потока (вредоносные данные) будет отфильтрована, и на МЭ с адаптивной проверкой пакетов поступит меньший входной поток.

В результате для STD, DC-1, DC-2-1, DC-2-2 и DC-3 СВПЗС и затраты на их реализацию равны

$$T_{STD} = \frac{\nu_0}{1-R/n_{01}} + \frac{\nu_1}{1-d_1 \cdot F_1} + \frac{\nu_0}{1-d_2 \cdot R/n_{01}},$$

$$T_{DC-1} = \frac{\nu_0}{1-R/n_{01}} + \frac{\nu_1}{1-d_1 \cdot F_1} + \frac{\nu_0}{1-d_2 \cdot R/n_{01}} + \frac{\nu_2}{1-d_3 \cdot F_2} + \frac{\nu_0}{1-d_4 \cdot R/n_{01}},$$

$$T_{DC-2-1} = \frac{\nu_0}{1-R/n_{01}} + \frac{\nu_1}{1-d_1 \cdot F_1} + \frac{\nu_0}{1-d_2 \cdot R/n_{02}} + \frac{\nu_2}{1-d_3 \cdot F_2} + \frac{\nu_0}{1-d_4 \cdot R/n_{02}},$$

$$T_{DC-2-2} = \frac{\nu_0}{1-R/n_{01}} + \frac{\nu_1}{1-d_1 \cdot F_1} + \frac{\nu_0}{1-d_2 \cdot R/n_{01}} + \frac{\nu_2}{1-d_3 \cdot F_2} + \frac{\nu_0}{1-d_4 \cdot R/n_{02}},$$

$$T_{DC-3} = \frac{\nu_0}{1-R/n_{01}} + \frac{\nu_1}{1-d_1 \cdot F_1} + \frac{\nu_0}{1-d_2 \cdot R/n_{02}} + \frac{\nu_2}{1-d_3 \cdot F_2} + \frac{\nu_0}{1-d_4 \cdot R/n_{03}},$$

$$C_{STD} = c_0 \cdot n_{01} + c_1 \cdot n_1, \quad C_{DC-1,DC-2-1,DC-2-2,DC-3} = c_0 \cdot \sum_i n_{0i} + c_1 \cdot n_1 + c_2 \cdot n_2,$$

где ν_0, ν_1, ν_2 – среднее время обслуживания в маршрутизаторах, МЭ-1, МЭ-2; d_1, d_2, d_3, d_4 – доля входного потока, оставшаяся после прохождения через каждое из устройств (маршрутизатор, МЭ-1, МЭ-2); n_{0i}, n_1, n_2 – число маршрутизаторов в каждой из групп, МЭ-1, МЭ-2; c_0, c_1, c_2 – стоимости маршрутизаторов, МЭ-1 и МЭ-2 соответственно. При этом $R = \lambda \cdot \nu_0$; $F_1 = \lambda \cdot \nu_1 / n_1$; $F_2 = \lambda \cdot \nu_2 / n_2$, а λ – интенсивность входного потока запросов; $d_1 = (1 - A_0 \cdot p_0)$; $d_2 = 1 - (p_1 \cdot (A_1 - l_{10}) + p_0 \cdot (A_0 - l_{10}) + l_{10} \cdot (1 - \overline{p}_0 \cdot \overline{p}_1))$; $d_3 = 1 - (p_1 \cdot (A_1 - l_{10}) + (A_0 - l_{10}) \cdot (1 - \overline{p}_0^2) + l_{10} \cdot (1 - \overline{p}_0^2 \cdot \overline{p}_1))$; $d_4 = 1 - (p_1 \cdot M_{e1} + (1 - \overline{p}_0^2) \cdot R_{emp} + p_2 \cdot M_{e2} + (l_{10} - l_{00}) \cdot (1 - \overline{p}_0^2 \cdot \overline{p}_1) + (l_{20} - l_{00}) \cdot (1 - \overline{p}_0^2 \cdot \overline{p}_2) + (l_{21} - l_{00}) \cdot (1 - \overline{p}_1 \cdot \overline{p}_2) + l_{00} \cdot (1 - \overline{p}_0^2 \cdot \overline{p}_1 \cdot \overline{p}_2))$, где $R_{emp} = (A_0 - l_{20} - l_{10} + l_{00})$; $M_{e1} = (A_1 - l_{21} - l_{10} + l_{00})$; $M_{e2} = A_2 - l_{21} - l_{20} + l_{00}$, а A_0, A_1, A_2 – доли ошибок (угроз) во входном потоке, обнаруживаемых маршрутизатором с вероятностью p_0, МЭ с фильтрацией пакетов – с вероятностью p_1 и МЭ с адаптивной проверкой пакетов – с вероятностью p_2; l_{00} – величина перекрытия обнаружения ошибок маршрутизатора, МЭ-1 и МЭ-2, l_{10} – маршрутизатора и МЭ-1, l_{20} – маршрутизатора и МЭ-2, l_{21} – МЭ-1 и МЭ-2 соответственно.

При оценке надежности считаем, что отказы различных узлов независимы, а поток отказов распределен по экспоненциальному закону (как это принято при расчетах надежности). Влияние злонамеренных воздействий, направленных на снижение надежности, а также на безопасность системы (см., например, [24]), в настоящей работе не рассматривается.

Надежность рассматриваемых схем равна $P_{STD} = P_{01} \cdot P_{m1}$, $P_{DC-1} = P_{01} \cdot P_{m1} \cdot P_{m2}$, $P_{DC-2-1,DC-2-2} = P_{01} \cdot P_{m1} \cdot P_{02} \cdot P_{m2}$, где P_{m1}, P_{m2}, P_{0i} – вероятность безотказной работы групп МЭ-1, МЭ-2 и маршрутизаторов соответственно. Причем $P_{m1} = (1 - (1 - r_1)^{n_1})$, $P_{m2} = (1 - (1 - r_2)^{n_2})$, а при условии, что маршрутизаторы в каждой из групп являются одинаковыми, $P_{0i} = (1 - (1 - r_0)^{n_{0i}})$, где $r_j = e^{-\lambda_j t}$, а λ_0, λ_1, λ_2 – интенсивность отказов маршрутизаторов, МЭ-1 и МЭ-2; n_{0i} – количество маршрутизаторов в i-ой группе; n_1 – количество МЭ-1; n_2 – количество МЭ-2; t – время работы устройства. Зная кратность узлов каждого из элементов схемы, которая требуется для получения минимального СВПЗС при известных значениях входного потока, можно вычислить вероятность безотказной работы системы.

Приведем результаты расчета при следующих исходных данных: A_0=0,07; A_1=0,15; A_2=0,26; p_0=0,85; p_1=0,9; p_2=0,9; l_{00}=0,04; l_{10}=0,04; l_{20}=0,06; l_{21}=0,12; ν_0=0,025 с; ν_1=0,04; ν_2=0,075 с; c_0=10 у.е.; c_1=20 у.е.; c_2=35 у.е.; для МЭ-1 r_{m1}=0,9, для МЭ-2 r_{m2}=0,9, для групп маршрутизаторов r_{0i}=0,9 и ограничении средств на построение системы C=500 у.е. Зависимость СВПЗС от интенсивности входного потока, представлена на рис. 4, а, а вероятности безотказной работы при соответствующих конфигурациях системы – на рис. 4, б.

Как видно из рисунков, лучшими показателями по задержкам обслуживания и надежности обладает вариант стандартной схемы доступа (STD). Однако такая схема не обеспечивает высокий уровень безопасности и защиты узлов подзащитной сети [17, 18]. С другой стороны, вариант построения схемы доступа «Прямое соединение» (которая способна обеспечить требуемый уровень безопасности), использующий одну группу маршрутизаторов на всю систему, обладает сравнительно тем же уровнем надежности, что и стандартная схема, и лучшим среди остальных вариантов схемы показателем СВПЗС. Если в имеющейся вычислительной системе используются две группы маршрутизаторов для соединения элементов системы между собой, то, несмотря на то, что оба варианта схемы обладают примерно равными показателями СВПЗС, вариант DC-2-1 будет более приемлем, так как он способен обеспечить более высокий уровень надежности системы, чем вариант схемы DC-2-2.

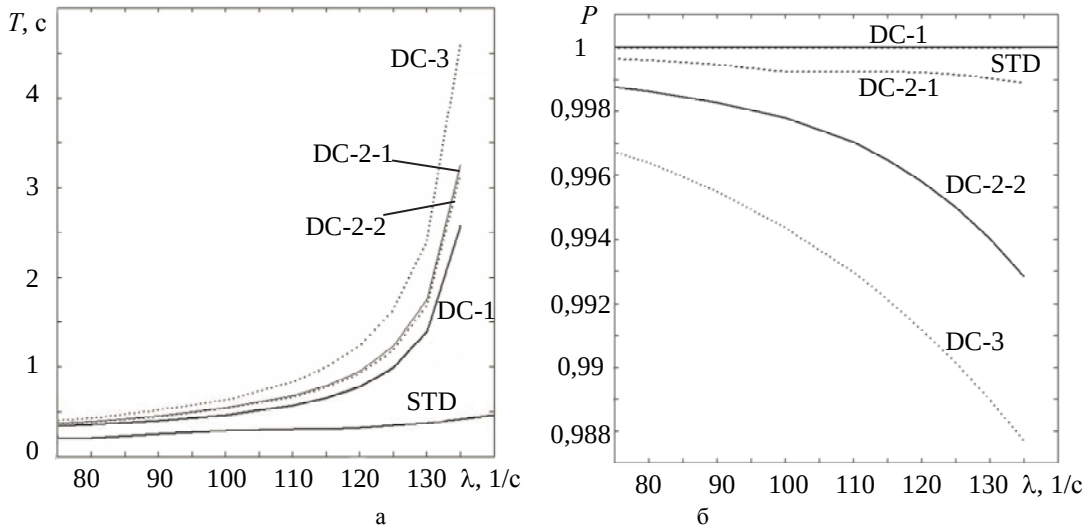

Рис. 4. Среднее время пребывания запросов в схемах защищенного доступа (а); надежность вариантов схем защищенного доступа (б)

Заключение

В работе проанализированы возможности различных вариантов построения схемы «Прямое соединение», позволяющей организовать многоуровневое защищенное подключение оконечного узла внутренней сети к ресурсам, расположенным во внешней сети. Рассмотренные варианты, помимо взаимного сравнения, также были сравнены с вариантом построения стандартной схемы обеспечения безопасного доступа к ресурсам внешней сети.

Показано, что эффективнее применять вариант построения схемы «Прямое соединение» с использованием одной группы маршрутизаторов на всю систему (DC-1). Данный вариант имеет наименьшие значения минимального среднего времени пребывания запроса и обладает более высоким уровнем надежности, чем другие варианты построения схемы. Показано, что второй (DC-2-1) и третий (DC-2-2) варианты построения схемы являются практически идентичными друг другу по показателю минимального среднего времени пребывания запросов в системе, но при этом в плане надежности их разница увеличивается с ростом нагрузки в канале.

Таким образом, при внедрении схемы «Прямое соединение» эффективнее всего использовать вариант ее построения с использованием общего пула маршрутизаторов для всей системы, причем эффективность возрастает с ростом загрузки системы.

References

1. Gatchin Yu.A., Zhariniv I.O., Korobeynikov A.G. mathematical Estimation models of information security system infrastructure at the enterprise. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2012, no. 2(78), pp. 92–95. (In Russian)
2. Aliev T.I. Design of systems with priorities. *Journal of Instrument Engineering*, 2014, vol. 57, no. 4, pp. 30–35. (In Russian)
3. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Intervals optimization of systems information security inspection. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 5(93), pp. 119–125. (In Russian)
4. Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T.A., Mead N.R. *Survivable network systems: an emerging discipline. Technical Report CMU/SEI-97-TR-013*. Pittsburgh, 1997.

5. Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T.A., Mead N.R. Survivability: protecting your critical systems. *IEEE Internet Computing*, 1999, vol. 3, no. 6, pp. 55–63. doi: 10.1109/4236.807008
6. Bogatyrev V.A., Bogatyrev A.V., Golubev I.Yu., Bogatyrev S.V. Queries distribution optimization between clusters of fault-tolerant computing system. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 3(85), pp. 77–82.
7. Bogatyrev V.A., Bogatyrev A.V. Functional reliability of a real-time redundant computational process in cluster architecture systems. *Automatic Control and Computer Sciences*, 2015, vol. 49, no. 1, pp. 46–56. doi: 10.3103/S0146411615010022
8. Bogatyrev V.A. Exchange of duplicated computing complexes in fault-tolerant systems. *Automatic Control and Computer Sciences*, 2011, vol. 45, no. 5, pp. 268–276. doi: 10.3103/S014641161105004X
9. Bogatyrev V.A., Bogatyrev S.V., Golubev I.Y. Optimization and the process of task distribution between computer system clusters. *Automatic Control and Computer Sciences*, 2012, vol. 46, no. 3, pp. 103–111. doi: 10.3103/S0146411612030029
10. Savel'ev S. Modern corporate information secure system. *Storage News*, 2008, no. 3 (36), pp. 10–14. (In Russian)
11. Romanov M. The fault-tolerant safety. *Storage News*, 2007, no. 2 (31), pp. 20–24. (In Russian)
12. Eremenko A.V., Levitskaya E.A., Sulavko A.E., Samotuga A.E. Differentiation of access to information based on hidden monitoring of users of computer systems: continuous identification. *SibADI Journal*, 2014, no. 6 (40), pp. 92–102.
13. Peisert S., Talbot E., Bishop M. Turtles all the way down: a clean-slate, ground-up, first-principles approach to secure systems. *Proc. 2012 New Security Paradigms Workshop, NSPW'12*. Bertinoro, Italy, 2012, pp. 15–26.
14. Whitmore J.J. A method for designing secure solutions. *IBM Systems Journal*, 2001, vol. 40, no. 3, pp. 747–768. doi: 10.1147/sj.403.0747
15. Goncharov E.I. Setting up data exchange between personal data information systems of different class. *Bezopasnost Informatsionnykh* Tekhnology, 2011, no. 2, pp. 75–78.
16. Rome J.A. *Enclaves and Collaborative Domains*. Oak Ridge, 2003. Available at: http://web.ornl.gov/~webworks/cppr/y2001/pres/117259.pdf (accessed 18.11.2015).
17. Kolomoitsev V.S. A comparative analysis of approaches to secure connection of the corporate network nodes to shared network. *Kibernetika i Programmirovanie*, 2015, no. 2, pp. 46–58. (In Russian) doi: 10.7256/2306-4196.2015.2.14349
18. Shlyapkin A.V. Methods and tools countering attacks on computer networks. *Informatsionnye Sistemy i Tekhnologii: Upravlenie i Bezopasnost'*, 2014, no. 3, pp. 325–330.
19. Kolomoitsev V.S., Bogatyrev V.A. Evaluating the effectiveness and justification of choice of the structural organization of the system of multi-level secure access to extranet resources. *Informatsiya i Kosmos*, 2015, no.3, pp. 71–79. (In Russian)
20. Kolomoitsev V.S. Analysis of opportunities of firewall types. *Materialy Konferentsii Informatsionnaya Bezopasnost' Regionov Rossii IBRR-2015* [Proc. Information Security of Russian Regions 2015]. St. Petersburg, 2015, pp. 218–219.
21. Bogatyrev V.A. Reliability of accommodation of functional resources in uniform computer networks. *Elektronnoe Modelirovanie*, 1997, no. 3, pp. 21–29. (In Russian)
22. Bogatyrev V.A. On the distribution of functional resources in the failover multicomputer systems. *Pribory i Sistemy. Upravlenie, Kontrol', Diagnostika*, 2001, no. 12, pp. 1–5. (In Russian)
23. Bogatyrev V.A., Bogatyrev S.V. Association reservation servers in clasters highly reliable computer system. *Informatsionnye Tekhnologii*, 2009, no. 6, pp. 41–47.
24. Shcheglov K.A., Shcheglov A.Yu. The reservation methods capabilities to enhance integral information and operational security level of modern informational systems. *Informatsionnye Tekhnologii*, 2015, vol. 21, no. 7, pp. 521–527.

Коломойцев Владимир Сергеевич – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Dek-s-kornis@yandex.ru

Vladimir S. Kolomoitcev – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, Dek-s-kornis@yandex.ru