Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети

Estimation of efficiency and rationale for the selection of the structural organization of the system of multi-level secure access to external network resources

Коломойцев / Kolomoitcev V.
Владимир Сергеевич
(Dek-s-kornis@yandex.ru)
ФГАОУ ВПО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (НИУ ИТМО), аспирант.
г. Санкт-Петербург

Богатырев / Bogatyrev V.
Владимир Анатольевич
(Vladimir.bogatyrev@gmail.com)
доктор технических наук, профессор, почетный работник науки и техники РФ.
НИУ ИТМО, профессор.
г. Санкт-Петербург

Ключевые слова: информационная безопасность – information security; несанкционированный доступ – unauthorized access; межсетевой экран – firewall; сетевая организация – network organization; отказоустойчивость – fault tolerance; защита информации – information protection; надежность – reliability.

В работе предложена оценка эффективности и проведено обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети. Проведены оптимизация и сравнительный анализ схем доступа «Прямое соединение» и «Общая схема» при организации защищенного подключения оконечного узла внутренней сети к ресурсам, расположенным во внешней сети.

The study proposes estimation of efficiency and rationale for the selection of the structural organization of the system of multi-level protected access to external network resources. Optimization and comparative analysis of the access shemes 'Direct connection' and 'Common scheme' are performed during organization of protected connection of the internal network endpoint node to resources located in external network.

Введение

В современных сложных вычислительных системах, подключенных как к корпоративным сетям, так и к сетям общего пользования, остро стоит проблема защищенности информации. Несанкционированный доступ, отказ узла в обслуживании, потеря информации, а также нарушение режима секретности в компьютерной системе может привести к значительным экономическим и иным потерям [1–5].

Угроза безопасности вычислительной системы может исходить как извне – в результате удаленных сетевых атаках, так и изнутри подзащитной сети – с помощью различных закладочных программных или аппаратных средств. Для решения проблем защиты информации могут быть применены меры и использованы средства обеспечения информационной безопасности, расположенные на различных уровнях сети.

Принципы организации защищенного подключения корпоративной сети к сетям общего пользования являются одними из важнейших элементов обеспечения информационной защищенности, существенно влияющими на безопасность и надежность работы в сети. Эффективные методы обеспечения безопасности, как правило, требуют значительных материальных затрат на их реализацию.

В данной работе исследуются возможности схем по организации защищенного доступа к ресурсам внешней сети, учитывающей требования, изложенные в руководящих документах по информационной безопасности. Исследование направлено на выбор рациональных вариантов системы защиты при обеспечении ее высокой надежности и минимизации среднего времени пребывания в ней запросов при различных видах ограничений на ее реализацию [6–8].

Объект и задачи исследования

Рассматриваемая схема ориентирована на повышение степени защищенности устройств сети и безопасности доступа к слабо защищенным и/или неподконтрольным участкам сети. Схема позволяет снизить риск DDoS-атак, повысить защиту устройств от вредоносного программного обеспечения, устранить возможности несанкционированного доступа к узлу сети и угрозы прослушивания канала передачи данных [9].

Исследуемая схема базируются на общей сетевой схеме доступа узла к внешней сети: узел «Внутренней (локальной) сети» – маршрутизатор – устройства «Внешней сети (Интернет)». Такой подход позволяет минимизировать степень возможной реорганизации уже имеющейся корпоративной сети. Данная общая схема доступа изображена на рис. 1.

В общей схеме доступа оконечного узла корпоративной сети к узлам внешней сети защита этого узла основана на встроенных в него средствах, включающих средства антивирусной защиты и стандартный межсетевой экран (МЭ). На входе в сеть при общей схеме доступа устанавливается маршрутизатор.

Применяемые в данной схеме меры приводят к тому, что практически вся работа по ликвидации угроз из внешней сети ложится на оконечный узел. Для снижения нагрузки на оконечный узел после маршрутизатора может быть установлен дополнительный МЭ с глубокой проверкой поступающих пакетов.

Для критически важных систем указанных средств защиты недостаточно. В связи с этим требуется использовать схему обеспечения комплексной информационной безопасности. В роли такой схемы может выступить, схема «Прямое соединение» [9].

Таким образом, далее предлагается рассмотреть возможности общей схемы доступа с дополнительным МЭ и схемы «Прямое соединение» в различных ее физических интерпретациях с точки зрения их надежности и минимального среднего времени пребывания запроса в системе.

Базовый вариант схемы доступа «Прямое соединение»

Использование схемы «Прямого соединения» предполагает минимальные изменения в архитектуре корпоративной сети, а также минимальные дополнительные финансовые затраты на ее создание. Структура схемы «Прямое соединение» представлена на рис. 2.

В данной схеме на входе во внутреннюю сеть (сразу после маршрутизатора) устанавливается МЭ с фильтрацией пакетов (МЭ-1) для фильтрации поступающих на вход данных от нежелательных сообщений (спама) и снижения риска DDoS-атак. Чаще всего указанный выше маршрутизатор может нести на себе функционал МЭ с фильтрацией пакетов, однако представляется эффективнее использовать раздельно маршрутизатор и МЭ. После маршрутизатора требуется установить МЭ с адаптивной проверкой пакетов (МЭ-2) для более глубокого анализа содержимого пакета [1]. С учетом того, что на вход МЭ-2 будет поступать меньше данных, чем на вход МЭ-1, нагрузка на данный МЭ будет меньше и, следовательно, производительность самой сети выше.

После прохождения МЭ-2 потенциально «чистые» данные должны поступить на адресуемый оконечный узел. На данном узле предусматривается установка антивирусного средства (АВС) со встроенным в него МЭ, система защиты от несанкционированного доступа (НСД) и организация защищенного хранилища. 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

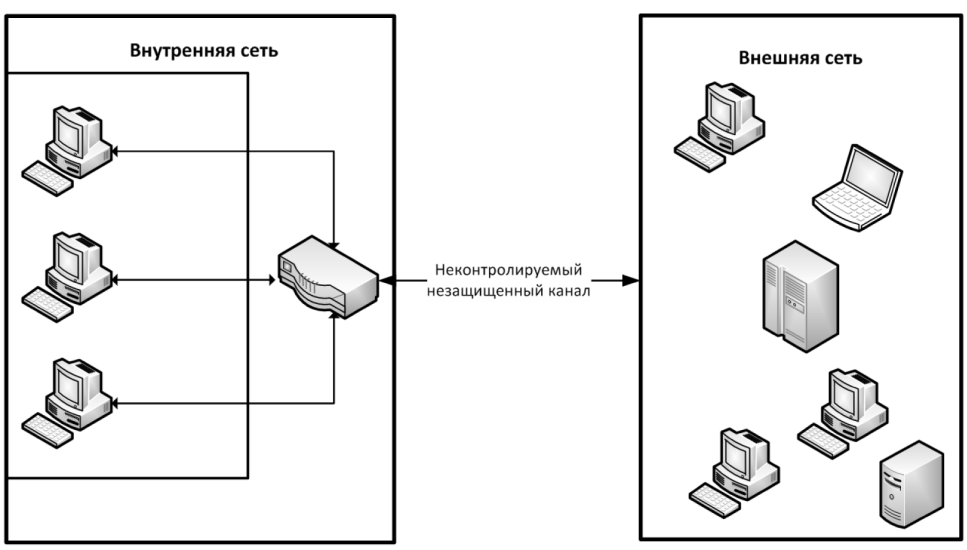

Рис. 1. Общая схема доступа узла во внешнюю сеть

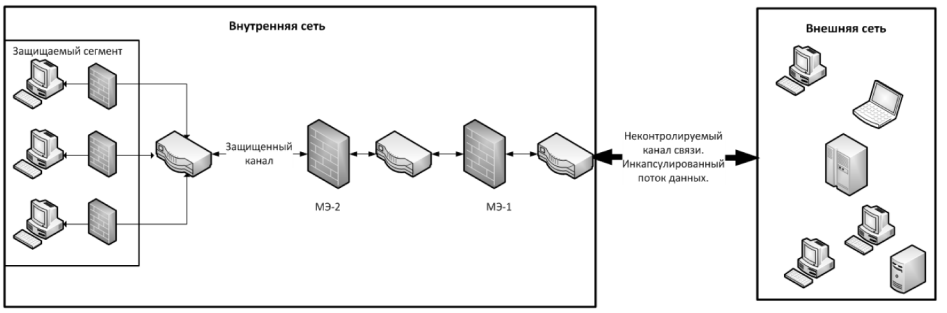

Рис. 2. Схема «Прямое соединение»

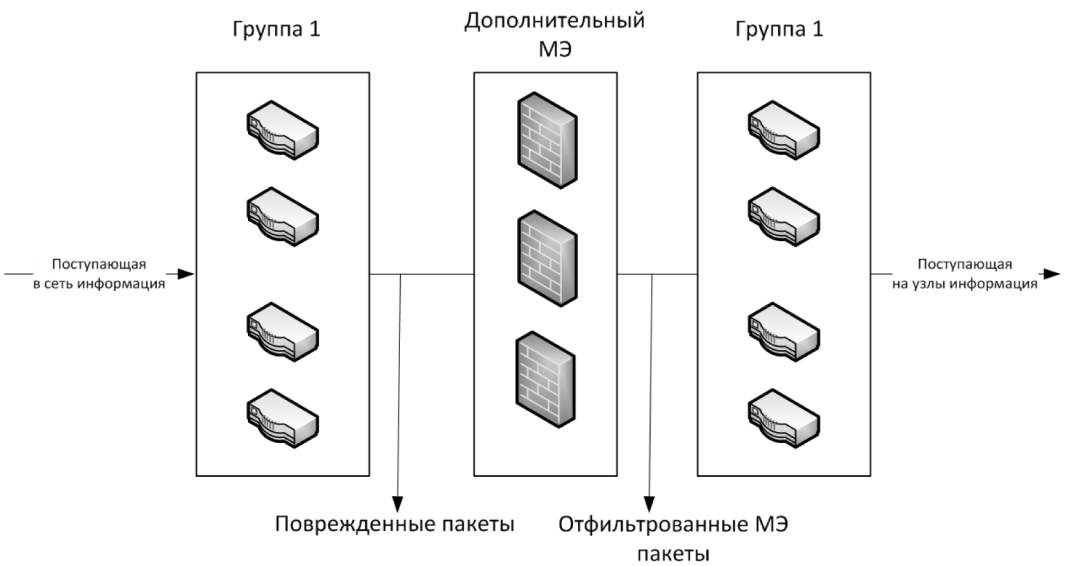

Рис. 3. Общая схема подключения

них данных) резервированы, а для данных, хранящихся на них, создаются резервные копии.

Сетевая инфраструктура «Общей схемы» доступа и варианты ее построения для 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: МЭ с фильтрацией пакетов, МЭ с адаптивной проверкой пакетов и маршрутизаторы, соединяющие все элементы схемы между собой. В рассматриваемой схеме возможны четыре варианта к построению схемы: с помощью трех, двух или одной групп маршрутизаторов на всю систему.

Сетевая инфраструктура «Общей схемы» представлена на рис. 3.

Возможные варианты построения сетевой инфраструктуры схемы «Прямое соединение» представлены на рис. 4.

Оценка надежности и среднего времени пребывания запроса в системе

При оптимизации представленных вариантов доступа по схеме «Прямое соединение» и «Общей схемы» требуется найти кратность резервирования узлов в каждой из групп, при котором достигается минимум среднего времени пребывания запросов в

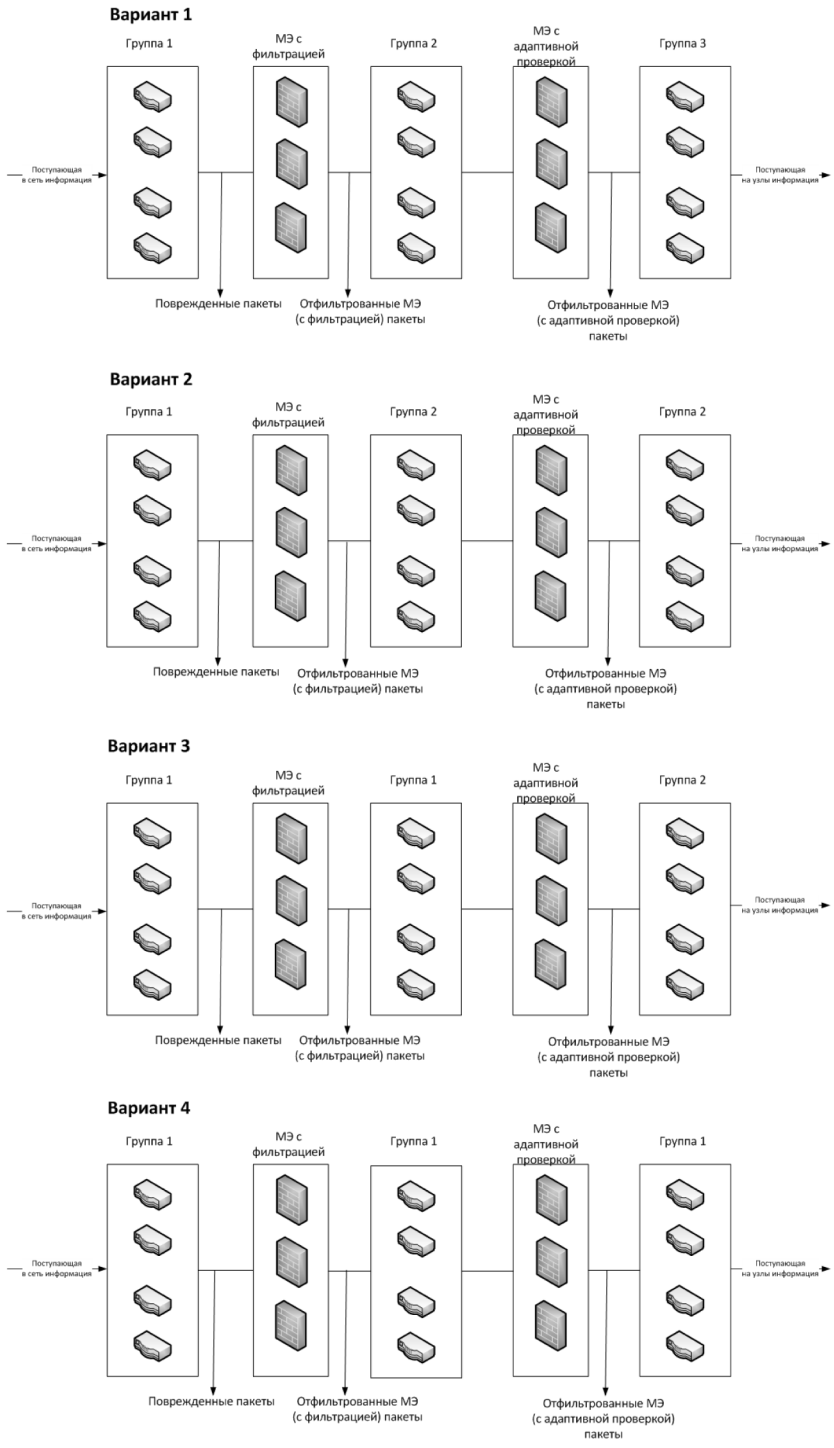

Рис. 4. Варианты сетевой архитектуры схемы «Прямое подключение»

системе (далее – СВПЗС) при ограничении стоимости реализации системы [10–13].

В рамках данного исследования будем предполагать, что каждый из МЭ и маршрутизаторы устраняют и находят только свою часть угроз (ошибок) во входящем потоке.

Каждый узел сети представим системой массового обслуживания типа M/M/1 с бесконечной очередью, для которой среднее время пребывания запросов в системе определяется как [14, с. 25]

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

где μ – интенсивность обслуживания, а $\rho = \lambda/\mu$ – 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 находиться как:

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

При прохождении запросов через несколько узлов среднее время пребывания в системе 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:

$$T_{общ} = \sum_i T_i .$$

После прохождения маршрутизатора входной поток фильтруется и, тем самым, интенсивность входного потока на МЭ с фильтрацией пакетов будет ниже, чем на маршрутизаторе. Аналогично будет происходить со входным поступающим потоком на МЭ с адаптивной проверкой пакетов – после прохождения МЭ определенная доля входного потока будет отфильтрована и на МЭ с адаптивной проверкой пакетов будет поступать меньший входной поток.

Таким образом, для «Общей схемы» и всех четырех вариантов схемы «Прямое соединение» СВПЗС определяются как:

$$T_0(\lambda) = \frac{\nu_0}{1-\frac{\lambda\cdot\nu_0}{n_{01}}} + \frac{\nu_2}{1-\lambda\cdot(1-A_0\cdot\rho_0)\cdot\frac{\nu_2}{n_2}} + \frac{\nu_0}{1-\lambda\cdot(1-A_2\cdot\rho_2)\cdot(1-A_0\cdot\rho_0)\cdot\frac{\nu_0}{n_{01}}},$$

$$T_1(\lambda) = \frac{\nu_0}{1-\frac{\lambda\cdot\nu_0}{n_{01}}} + \frac{\nu_1}{1-\lambda\cdot(1-A_0\cdot\rho_0)\cdot\frac{\nu_1}{n_1}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_0}{n_{02}}} + \frac{\nu_2}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_2}{n_2}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t2}\cdot\frac{\nu_0}{n_{03}}},$$

$$T_2(\lambda) = \frac{\nu_0}{1-\frac{\lambda\cdot\nu_0}{n_{01}}} + \frac{\nu_1}{1-\lambda\cdot(1-A_0\cdot\rho_0)\cdot\frac{\nu_1}{n_1}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_0}{n_{02}}} + \frac{\nu_2}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_2}{n_2}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t2}\cdot\frac{\nu_0}{n_{02}}},$$

$$T_3(\lambda) = \frac{\nu_0}{1-\frac{\lambda\cdot\nu_0}{n_{01}}} + \frac{\nu_1}{1-\lambda\cdot(1-A_0\cdot\rho_0)\cdot\frac{\nu_1}{n_1}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_0}{n_{01}}} + \frac{\nu_2}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_2}{n_2}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t2}\cdot\frac{\nu_0}{n_{02}}},$$

$$T_4(\lambda) = \frac{\nu_0}{1-\frac{\lambda\cdot\nu_0}{n_{01}}} + \frac{\nu_1}{1-\lambda\cdot(1-A_0\cdot\rho_0)\cdot\frac{\nu_1}{n_1}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_0}{n_{01}}} + \frac{\nu_2}{1-\lambda\cdot\alpha_{t1}\cdot\frac{\nu_2}{n_2}} + \frac{\nu_0}{1-\lambda\cdot\alpha_{t2}\cdot\frac{\nu_0}{n_{01}}},$$

причем $\alpha_{t1} = (1-A_0\cdot\rho_0)\cdot(1-A_1\cdot\rho_1)$, а $\alpha_{t2} = \alpha_{t1}\cdot(1-A_2\cdot\rho_2)$, где $(1-A_i\cdot\rho_i)$ – доля отфильтрованного входного потока ранее расположенным узлом.

При этом ν_0, ν_1, ν_2 – среднее время обслуживания запроса в маршрутизаторах, МЭ с фильтрацией пакетов и МЭ с адаптивной проверкой пакетов; λ – интенсивность потока запросов; A_0, A_1, A_2 – соответственно 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_0; n_{0i} – число маршрутизаторов в i-ой группе; n_1 – число МЭ с фильтрацией пакетов; n_2 – число МЭ с адаптивной проверкой пакетов.

Затраты на реализацию рассматриваемых вариантов системы защиты:

$$C_0 = c_0\cdot n_{01} + c_2\cdot n_2,$$

$$C_{1-4} = c_0\cdot\sum_i n_{0i} + c_1\cdot n_1 + c_2\cdot n_2,$$

где стоимости маршрутизаторов – c_0, МЭ с фильтрацией пакетов – c_1, МЭ с адаптивной проверкой пакетов – c_2.

Оптимизация системы защиты включает поиск распределения числа узлов каждого типа, обеспечивающего минимум среднего времени пребывания запросов в системе, вычисляемого по формулам $T_0(\lambda) - T_4(\lambda)$, при условии ограничения стоимости реализации системы $C_0 \le C, C_1 \le C, ..., C_4 \le C$ и соблюдения условий стационарности режима обслуживания [15–19].

Предлагаемые модели позволяют провести обоснование (выбор) решений по построению системы защиты в зависимости от параметров входного потока и характеристик сети. Для иллюстрации такого обоснования приведем пример расчета при: ν_0=0.025 с, ν_1=0.04 с, ν_2=0.075с, c_0=10 у.е., c_1=25 у.е., c_2=50 у.е., C=550 у.е., p_0=0.95, p_1= p_2=0.899, A_0=0.05, A_1=0.1, A_2=0.25 (значения параметров выбраны произвольным образом).

Результаты расчетов среднего времени пребывания запросов в системе по формулам $T_0(\lambda) - T_4(\lambda)$ для числа узлов каждого типа, определенных в результате оптимизации, в зависимости от интенсивности входного потока λ представлены на рис. 5.

Кривые здесь и далее, имеют следующее соответствие: Кривая 1 – данные «Общей схемы»; кривые 2–5 – варианты построения схемы «Прямое соединение».

Надежность построенных схем равна: $P_0 = P_{01}\cdot P_{m2}$, $P_1 = P_{01}\cdot P_{m1}\cdot P_{02}\cdot P_{m2}\cdot P_{03}$, $P_{2-3} = P_{01}\cdot P_{m1}\cdot P_{02}\cdot P_{m2}$,

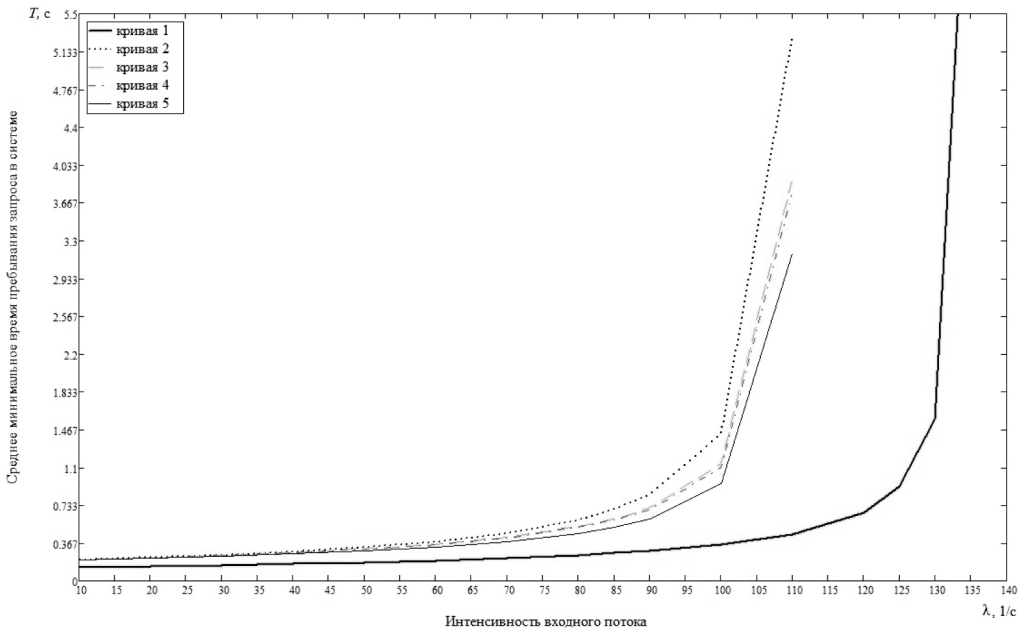

Рис. 5. Минимальные средние времена пребывания запросов в системе

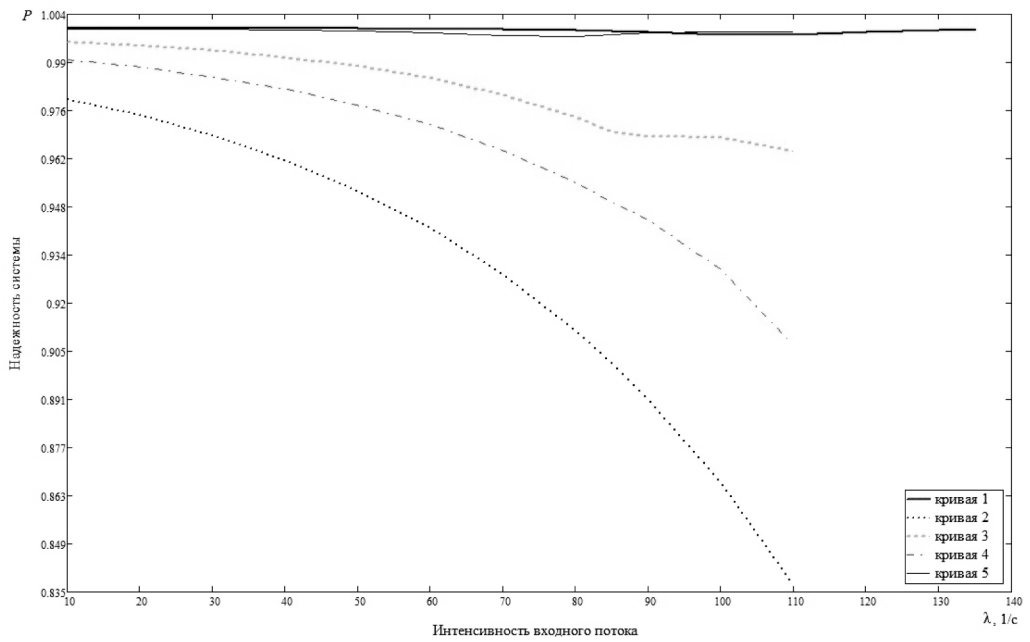

Рис. 6. Надежность схем доступа с учетом минимального среднего времени пребывания запросов в системе

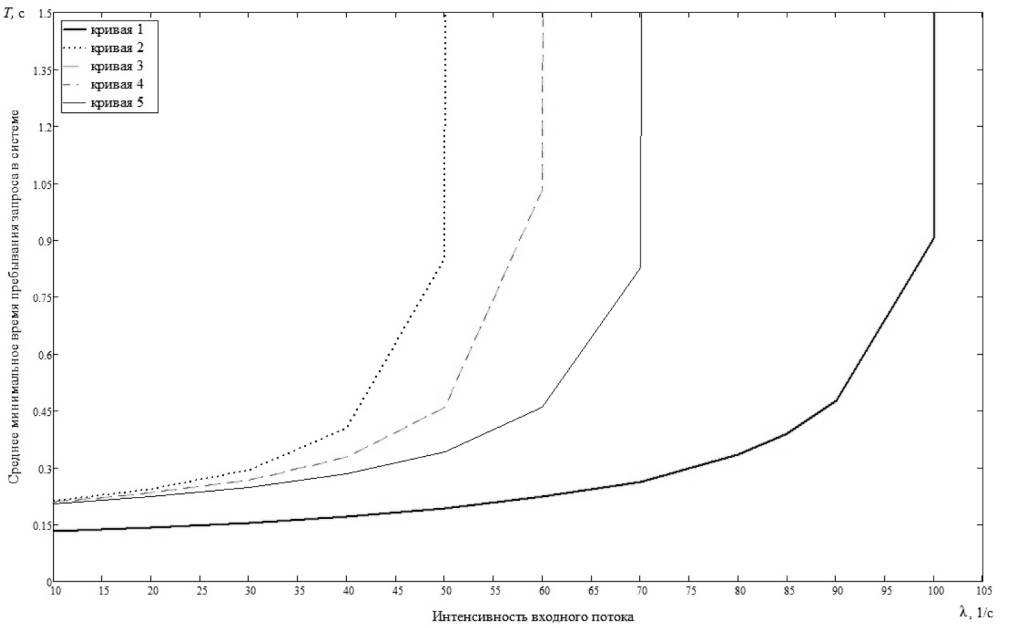

Рис. 7. Минимальные средние времена пребывания запросов в системе при максимально возможной надежности

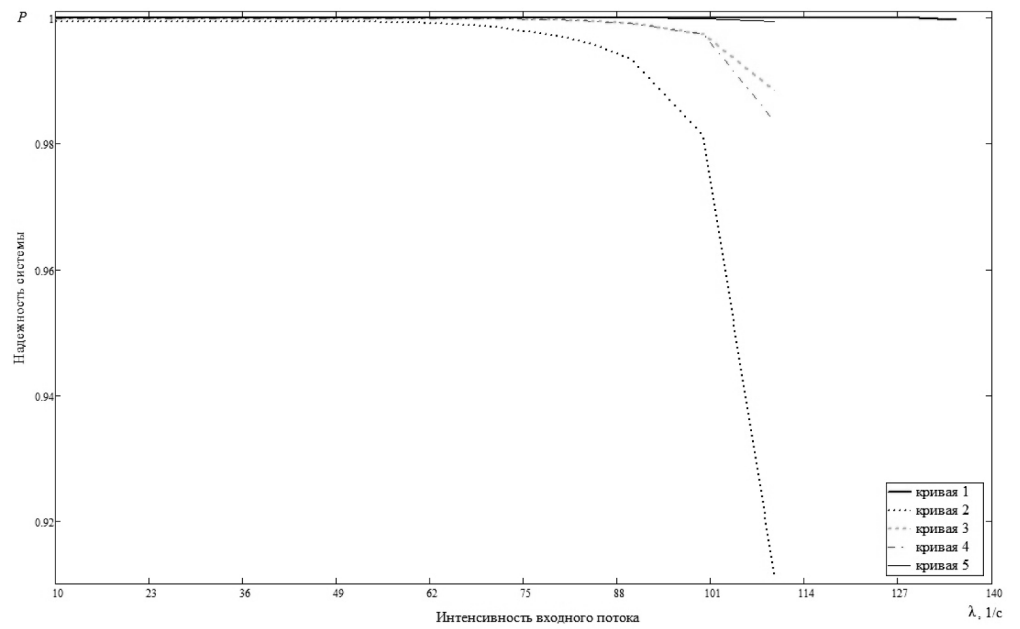

Рис. 8. Надежность схем доступа с учетом входного потока запросов

$P_4 = P_{01} \cdot P_{m1} \cdot P_{m2}$, 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 с фильтрацией пакетов и МЭ с адаптивной проверкой пакетов, n_{0_i} – число маршрутизаторов в i-ой группе; n_1 – число МЭ с фильтрацией пакетов; n_2 – число МЭ с адаптивной проверкой пакетов.

Результаты расчетов надежности, в зависимости от интенсивности входного потока λ, для значений числа узлов каждого типа, определенных в результате минимизации среднего времени пребывания запросов в системе по формулам $T_0(\lambda) - T_4(\lambda)$ при r_0=0.7, r_1=0.8, r_2=0.9, представлены на рис. 6.

Для случаев, когда требуется построить наиболее надежную «Общую схему» и варианты схемы «Прямое соединение», результаты при тех же заданных начальных параметрах, представлены на рис. 7 и рис. 8.

Как видно из графиков, «Общая схема», является более надежной и имеет меньшее минимальное СВПЗС. Также она способна работать при бóльших значениях интенсивности входного потока, чем схема «Прямое соединение». Однако, как уже говорилось ранее, она обеспечивает меньший уровень защиты оконечных узлов системы и приводит к высокой нагрузке на оконечные узлы. С другой стороны, схема «Прямое соединение», которая позволяет достигнуть более высокого уровня защищенности оконечных узлов и снизить на них нагрузку, имеет хуже показатели в плане минимального СВПЗС, чем «Общая схема», и в определенных вариантах ее построения имеет хуже показатели надежности.

Так, исходя из рис. 5 и рис. 7, лучшими результатами по минимальному СВПЗС, обладает четвертый вариант построения схемы «Прямое соединение», а худшим – первый вариант. Из рисунков видно, что варианты два и три, обладают практически идентичными значениями по минимальному СВПЗС. Из рис. 6 и рис. 8 при соответствующих значениях интенсивности входного потока видно, что второй вариант построения схемы «Прямое соединение», является более надежным, чем третий вариант ее построения. В случае, когда требуется построить наиболее надежную схему по данным двум вариантам, следует учитывать, что разница в надежности между ними начинает сильно проявляться лишь на высоких значениях интенсивностии входного потока, тогда как в случае, когда требуется достигнуть наименьшего минимального СВПЗС, разница между данными вариантами является существенной даже при малых значения плотности входного потока.

Из рис. 6 и рис. 8 видно, что четвертый вариант построения схемы «Прямое соединение» обладает практически равными значениями надежности, что и «Общая схема». Исходя из этого можно сделать вывод, что применение четвертого варианта построения схемы «Прямое соединение» позволяет достигнуть требуемого высокого уровня защищенности оконечных узлов системы с некоторыми вынужденными потерями (связанными с увеличением количества соединенных последовательно вычислительных узлов) по СВПЗС, сохраняя при этом высокий уровень надежности всей системы.

Заключение

В статье произведен анализ возможностей схемы доступа «Прямое соединение», а также произведено сравнение данной схемы с «Общей схемой» организации защищенного подключения оконечного узла внутренней сети к ресурсам, расположенным во внешней сети. В ходе исследования были выявлены достоинства и недостатки схемы «Прямое соединение» в зависимости от варианта ее построения.

Показано, что схема «Прямое соединение» обладает в одном из вариантов своего построения (с использованием одной группы маршрутизаторов на всю схему доступа) практически равной надежностью, что и «Общая схема» организации защищенного доступа во внешнюю сеть. При этом в результате того, что схема «Прямое соединение» имеет большее количество узлов и связей, для создания более безопасного доступа оконечных узлов во внешнюю сеть она обладает худшими значениями среднего времени пребывания запросов в системе, по сравнению с «Общей схемой».

Таким образом, применение схемы «Прямое соединение» позволит увеличить защищенность системы, с сохранением ее надежности, без внесения существенных архитектурных изменений сети организации. Однако при этом, приведет к увеличению среднего времени пребывания запросов в системе, тем выше, чем меньше финансовые возможности организации.

Литература

1. Kenneth, I. A History and Survey of Network Firewalls / I. Kenneth, F. Stephanie. – University of New Mexico, 2002. – 42 p.

2. Гатчин, Ю. А. Математические модели оценки инфраструктуры системы защиты информации на предприятии / Ю.А. Гатчин, И.О. Жаринов, А.Г. Коробейников // Научно-технический вестник ИТМО. – 2012. – № 2 (78). – С. 92–95.

3. Алгоритм классификации информации для решения задачи фильтрации нежелательных сообщений / А.Г. Коробейников [и др.] // Программные системы и вычислительные методы. – 2012. – № 1. – С. 89–95.

4. Алиев, Т. И. Проектирование систем с приоритетами / Т.И. Алиев // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57. – № 4. – С. 30–35.

5. Богатырев, В. А. Оптимизация интервалов проверки информационной безопасности систем / В.А. Богатырев, А.В. Богатырев, С.В. Богатырев // Научно-технический вестник ИТМО. – 2014. – № 5 (93). – С. 119–125.

6. Оптимизация распределения запросов между кластерами отказоустойчивой вычислительной системы / В.А. Богатырев [и др.] // Научно-технический вестник ИТМО. – 2013. – № 3. – С. 77–82.

7. Оптимизация вычислительных систем с объединением межсетевых экранов в отказоустойчивые кластеры / В.А. Богатырев [и др.] // Научно-технический вестник ИТМО. – 2011. – № 6 (76). – С. 140–142.

8. Богатырев, В. А. Оценка и выбор отказоустойчивых конфигураций межсетевых экранов / В.А. Богатырев, С.Б. Фокин, М.В. Попова // Научно-технический вестник ИТМО. – 2011. – № 3 (73). – С. 139–140.

9. Коломойцев, В. С. Сравнительный анализ подходов к организации безопасного подключения узлов корпоративной сети к сети общего доступа / В.С. Коломойцев // Кибернетика и программирование. – 2015. – № 2. – С. 46–58.

10. Богатырев, В. А. Критерии оптимальности многоуровневых отказоустойчивых компьютерных систем / В.А. Богатырев, С.В. Богатырев // Научно-технический вестник ИТМО. – 2009. – № 5 (63). – С. 92–97.

11. Bogatyrev, V. Functional Reliability of a Real-Time Redundant Computational Process in Cluster Architecture Systems / V. Bogatyrev, A. Bogatyrev // Automatic Control and Computer Sciences. – 2015. – Vol. 49. – No. 1. – P. 46–56. DOI 10.3103/S0146411615010022.

12. Богатырев, В. А. Оптимизация древовидной сети с резервированием коммутационных узлов и связей / В.А. Богатырев, С.В. Богатырев, А.В. Богатырев // Телекоммуникации. – 2013. – № 2. – С. 42–48.

13. Богатырев, В. А. Комбинаторно-вероятностная оценка надежности и отказоустойчивости кластерных систем / В.А. Богатырев // Приборы и системы. Управление, контроль, диагностика. – 2006. – № 6. – С. 21–26.

14. Клейнрок, Л. Вычислительные системы с очередями / Л. Клейнрок ; пер. с англ. под ред. Б.С. Цыбакова. – М.: Мир, 1979. – 600 с.

15. Богатырев, В. А. Оптимальное резервирование системы разнородных серверов / В.А. Богатырев // Приборы и системы. Управление, контроль, диагностика. – 2007. – № 12. – С. 30–36.

16. Bogatyrev, V. Optimization and the Process of Task Distribution between Computer System Clusters / V. Bogatyrev, I. Golubev, S. Bogatyrev //Automatic Control and Computer Sciences. – 2012. – No. 3. – P. 103–111.

17. Bogatyrev, V. Fault tolerance of clusters configurations with direct connection of storage devices / V. Bogatyrev // Automatic Control and Computer Sciences. – 2011. – Vol. 45. – No. 6. – P. 330–337.

18. Богатырев, В. А. Оценка надежности выполнения кластерами запросов реального времени / В.А. Богатырев, А.В. Богатырев, С.В. Богатырев // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57. – № 4. – С. 46–48.

19. Богатырев, А. В. Перераспределение запросов между вычислительными кластерами при их деградации / А.В. Богатырев, В.А. Богатырев, С.В. Богатырев // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57. – № 9. – С. 54–58.