УДК 004.056.5

ОПТИМАЛЬНЫЙ ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПОДСИСТЕМЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

Зангиев Т. Т.,

кандидат технических наук, доцент,

Кубанский государственный технологический университет,

Краснодар, Россия

Евстратов Е. Е.,

студент,

Кубанский государственный технологический университет,

Краснодар, Россия

Аннотация

В связи с высокими требованиями к устойчивости функционирования сетей и их информационной безопасностью актуальной проблемой является выбор на рынке программно-аппаратных продуктов, средств защиты информации от различного ряда угроз, возникающих в вычислительной сети предприятия. Для решения задачи оптимального выбора были проанализированы существующие методы многокритериального выбора, разработана и верифицирована комплексная методика, базирующаяся на структурировании функции качества и имитационного моделирования локально-вычислительной сети, разработан программный модуль оптимального выбора.

Ключевые слова: принятие решений, методы многокритериального выбора, метод структурирования функции качества, имитационное моделирование локальных вычислительных сетей.

OPTIMUM CHOICE OF INFORMATION SECURITY MEANS FOR NETWORK SECURITY SUBSYSTEMS

Zangiev T.T.,
Candidate of Technical Sciences, Assistant Professor,
Kuban State Technological University,
Krasnodar, Russia
Evstratov E.E.,
Student,
Kuban State Technological University,
Krasnodar, Russia

Annotation
Due to the high requirements for the stability of the functioning of networks and their information security, an urgent problem is the choice of information security from a variety of threats that arise in the local area network on the market. During this study, to solve the optimal choice problem, the authors analyzed the existing methods of multi-criteria selection, developed and tested a comprehensive methodology based on the method of quality function deployment and local area network simulation, developed an optimal choice software module based on the methodology.
Keywords: decision making, multi-criteria selection methods, quality function deployment, local area network simulation.

При выборе средств защиты информации нередко случаются ситуации, когда выделенные на защиту информации материальные ресурсы не используются должным образом, ввиду чего не окупаются. В связи с этим всегда остается актуальной задача оптимального выбора средств защиты информации.

На принятие решения определяющее воздействие оказывают результаты анализа их последствий, но зачастую сложно точно рассчитать и оценить последствия для подавляющего большинства решений. Далеко не всегда удается учесть все факторы, влияющие на результат принятого решения.

Несмотря на то, что рынок программно-аппаратных продуктов предлагает много средств защиты информации, сложно разобраться, чем они отличаются друг от друга, и какими принципами следует руководствоваться при их выборе. В рамках данной работы для решения задачи оптимального выбора предлагается разработать методику, базирующуюся на методе структурирования функций качества и имитационного моделирования локально-вычислительной сети.

Оптимальность выбора определяется совокупностью критериев, по которым оценивается каждая из альтернатив. Критерии формирует субъект выбора, или лицо, принимающее решение. Также он устанавливает для себя большую ценность одних критериев и, наоборот, меньшую ценность других. Чаще всего лицо, принимающее решение, не обладает соответствующими профессиональными навыками, позволяющими оценить альтернативы по каждому критерию, и поэтому для данной работы привлекаются эксперты, имеющие необходимые компетенции и знания в соответствующих областях [1].

В процессе оптимального выбора средств защиты информации подсистемы сетевой безопасности, исходя из того, что любой набор критериев опосредованно связан с особенностями локальной вычислительной сети конкретного информационного объекта, возникает необходимость совмещения общих методик многокритериального выбора и методик, способных оценить результаты принятого решения с учетом специфики локальных вычислительных сетей конкретных объектов – имитационного моделирования поведения устройств в контексте модели вычислительной сети.

Объектом исследования является подсистема сетевой безопасности.

Целью работы является разработка комплексной методики оптимального выбора средств защиты информации для подсистемы сетевой безопасности.

В ходе исследования были проанализированы следующие методы многокритериального выбора:

– сведение задачи к однокритериальной (условная максимизация, линейная свёртка, максиминная свёртка)

– метод анализа иерархий [2];

– методы нечеткого математического программирования [3];

– метод структурирования (развертывания) функции качества [4].

Исходя из выявленных преимуществ и недостатков, в качестве математического аппарата разработанной комплексной методики выбора средств защиты информации был выбран метод структурирования функции качества ввиду его адаптивности и простоты реализации.

Методика структурирования функции качества является одной из наиболее эффективных методик в области планирования качества. В контексте задачи оптимального выбора альтернативы из некоторого набора она сводится к переводу неформально сформулированных предпочтений лица, принимающего решение, в набор конкретных характеристик-критериев оценки средств защиты информации.

Данная методика очень уместна в ситуациях, когда на предприятии лицо, принимающее решение имеет опосредованное отношение и незначительные познания в области выбора средств защиты информации и не может сформулировать конкретные предпочтения по критериям оценки средств. В то же время, перед специалистом отдела информационной безопасности предприятия стоит задача анализа и выбора альтернатив по конкретному набору критериев и соответствующих экспертных оценок каждой из альтернатив, при этом требуется учитывать пожелания и предпочтения лица, принимающего решение, несущего различные виды ответственности, вплоть до уголовной, за неверный выбор в виде

реализации угроз информационной безопасности и последующей компрометации информации.

Методику структурирования функции качества в адаптированном под требования задачи выбора виде можно разделить на следующие этапы:

1. Выяснение и уточнение списка потребностей организации. Задача специалиста состоит в том, чтобы с помощью различных методов преобразовать предпочтения лица, принимающего решение, в характеристики средств защиты информации. К примеру, «эффективность» может быть развернуто в «оперативность реагирования», а «стоимость» – в «стоимость закупки» и «стоимость эксплуатации».

2. Ранжирование потребностей – проставление каждой потребности индекса значимости. Требования, выносимые средству, бывают противоречивы, поэтому нужно иметь чёткое представление, удовлетворение каких потребностей приоритетнее.

3. Определение технических характеристик альтернатив. На данном этапе формируется список критериев и соответствующих оценок каждой альтернативы.

4. Определение корреляции между потребностями и критериями. В результате выполнения предыдущих этапов был получен ранжированный список потребностей, сформулированный в удобном для лица, принимающего решение, виде, и список критериев, удобный для проведения сравнения специалистом. Необходимо ответить на вопрос, как каждая потребность зависит от каждого критерия. Зачастую, достаточно таких трех понятий, как «сильная связь», «слабая связь» и «не связаны». В результате формируется таблица из критериев и потребностей с их индексами значимости, где значение каждого парного пересечения определяется произведением индекса значимости потребности и уровнем её связи с критерием.

5. Вычисление итогового значения. После выполнения предыдущих этапов остается лишь вычислить итоговый результат по каждой из альтернатив в виде суммы произведений оценки альтернативы по критерию и оценки корреляции потребностей с критерием.

Таким образом, учитывая определенные цели, стратегию компании и оценку критичности влияющих факторов, можно отдать предпочтение наиболее подходящей альтернативе. Также стоит упомянуть, что ввиду несложности математических вычислений, данная методика позволяет практически без последствий увеличивать число альтернатив и критериев ввиду линейного роста требований к вычислительным мощностям.

Исходя из того, что любой набор критериев опосредованно связан с особенностями локальной вычислительной сети конкретного информационного объекта, возникает необходимость имитационного моделирования устройства в ней. Моделирование позволяет более точно оценить эффективность и интеграционные способности устройства с учетом специфик сети объекта.

Разработанная комплексная методика оптимального выбора средств защиты информации для подсистемы сетевой защиты базируется на двух составляющих:

– основах метода структурирования функции качества;

– методе имитационного моделирования локальной вычислительной сети конкретного объекта.

Опишем пункты алгоритма разработанной методики в контексте выбора универсального шлюза безопасности в качестве средства защиты информации подсистемы сетевой безопасности.

1. Определение и уточнение списка потребностей. В качестве потребностей были выбраны следующие:

– «Простота установки»;

– «Простота использования»;

– «Импортозамещение»;
– «Оперативность и эффективность реагирования»;
– «Стоимость закупки и эксплуатации».

Потребность «Импортозамещение» позволит оценить, можно ли использовать решение в рамках государственных инициатив по поддержке отечественного производителя и борьбе с санкциями, что бывает необходимо при проектировании комплексных систем защиты информации на государственных информационных системах и критических информационных инфраструктурах.

2. Следующим этапом является проставление каждой потребности индивидуального индекса значимости. Ввиду того, что требования, выносимые выбираемому устройству, бывают противоречивы, поэтому нужно иметь чёткое представление, удовлетворение каких потребностей приоритетнее.

Индексы значимости для каждой потребности представляет собой десятичную дробь из интервала от нуля до единицы и зависят от количества потребностей.

Присвоим каждой потребности индексы значимости:

– «Простота установки» – 1;
– «Простота использования» – 0,8;
– «Импортозамещение» – 0,6;
– «Оперативность и эффективность реагирования» – 0,4;
– «Стоимость закупки и эксплуатации» – 0,2.

3. Определение списка критериев и соответствующих оценок каждой альтернативы. Для универсальных шлюзов безопасности, были выделены следующие критерии [2, 3]:

– «Российский производитель»;
– «Сертификат ФСТЭК»;
– «Архитектура решений»;

– «Функции межсетевого экранирования»;
– «Создание виртуальных частных сетей VPN»;
– «Поддержка сетевых сервисов»;
– «Функции прокси-сервера»;
– «Основные функции безопасности NGFW»;
– «IDS/IPS»;
– «Контроль приложений»;
– «Защита от DDoS»;
– «Антивирусная защита»;
– «Антибот-защита»;
– «Защита почтового трафика (безопасность почты, антиспам)»;
– «Веб-фильтрация»;
– «Обнаружение утечек информации (DLP)»;
– «Проактивная защита Threat Intelligence»;
– «Песочница (Sandbox)»;
– «Дополнительные функции NGFW»;
– «Аутентификация»;
– «Высокая доступность и кластеризация»;
– «Возможности централизованного управления»;
– «Мониторинг работы и система отчетности»;
– «Возможности интеграции»;
– «Техническая поддержка»;
– «Стоимость».

Каждая из сравниваемых альтернатив была оценена по каждому из критериев числовым значением от нуля до единицы следующим образом:

– Большая часть информации была в виде списка характеристик, поэтому проводился сравнительный анализ и ранжирование альтернатив по каждому из подкритериев. В ином случае, показатели суммировались и нормировались.

– Исходя из ранжирования каждой альтернативе по каждому критерию была проставлена соответствующая оценка.

4. Определение корреляции между потребностями и критериями.

В результате выполнения предыдущих этапов был получен ранжированный список потребностей и список критериев. На данном этапе необходимо оценить, насколько удовлетворение каждой потребности зависит от каждого критерия. Уровень зависимости представляет собой

– 1 – сильная связь;

– 0,5 – слабая связь;

– 0 – связь отсутствует.

Результат оценки корреляции критериев и потребностей представлен в таблице 1.

Таблица 1 – Корреляция критериев и потребностей

Критерии	Простота установки	Простота использования	Импортозамещение	Оперативность и эффективность реагирования	Стоимость закупки и эксплуатации
Российский производитель	0	0,5	1	0	0,5
Сертификат ФСТЭК	0	0	1	0	0
Архитектура решений	1	1	0	0,5	0,5
Функции межсетевого экранирования	0	0	0	1	0
Создание виртуальных частных сетей VPN	0	0	0	1	0
Поддержка сетевых сервисов	0	0	0	1	0,5
Функции прокси-сервера	0	0	0	1	0
Основные функции безопасности NGFW	0	0	0	1	0
IDS/IPS	0	0	0	1	0
Контроль приложений	0	0	0	1	0
Защита от DDoS	0	0	0	1	0
Антивирусная защита	0	0	0	1	0
Антибот-защита	0	0	0	1	0
Защита почтового трафика (безопасность почты, антиспам)	0	0	0	1	0
Веб-фильтрация	0	0	0	1	0
Обнаружение утечек информации (DLP)	0	0	0	1	0
Проактивная защита Threat Intelligence	0	0	0	1	0
Песочница (Sandbox)	0	0,5	0	1	0
Дополнительные функции NGFW	0	0	0	1	0
Аутентификация	0	0	0	1	0
Высокая доступность и кластеризация	0,5	1	0	1	0,5
Возможности централизованного управления	0	1	0	0,5	0
Мониторинг работы и система отчетности	0	1	0	0	0
Возможности интеграции	0,5	0,5	0	0,5	0,5
Техническая поддержка	0	1	0	0	0,5
Стоимость	0	0	0	0	1

5. Вычисление итогового значения каждой из альтернатив. Итоговый рейтинг каждой альтернативы вычисляется в виде суммы произведений оценки альтернативы по критерию и оценки корреляции потребностей с критерием, умноженный на уровень значимости потребности: $R = \sum_{i=1}^{n} C_i * (\sum_{j=1}^{m} P_{ij} * K_j)$, где R – итоговый рейтинг альтернативы, C_i – оценка альтернативы по i-тому критерию, P_{ij} – уровень зависимости j-той потребности от i-того критерия и K_j – индекс значимости j-той потребности.

Итоговая оценка альтернатив, перечисленных в таблицах приложения Б при вышеописанных значениях индекса значимости и корреляции приведена в таблице 2.

Таблица 2 – Итоговая оценка альтернатив

Наименование альтернативы	Оценка
Cisco	12.576
Check point	14.394
Fortinet	15.335
Huawei	13.495
Palo Alto Networks	13.536
Juniper Networks SRX	14.68
Zyxel ATP	10.086
Ideco UTM	8.401
Traffic Imspector Next Generation	8.888
Интернет Контроль Сервер (ИКС)	9.062
Diamond VPN/FW	10.655
Код Безопасности	10.017
Usergate	13.137

В результате выполнения всех предыдущих действий, можно выделить 3 явных лидера альтернатив: Fortinet, Juniper Networks SRX, Check point.

6. Моделирование альтернатив. Для конкретизации выбора одной из альтернатив необходимо провести имитационное моделирование каждого из

устройств-лидеров в виртуальном стенде, собранном по структуре локальной вычислительной сети объекта. Ввиду того, что каждое устройство крупных компаний-производителей выпускается в виртуальной версии, помимо программно-аппаратной, и вендоры предоставляют пробную версию – образ операционной системы устройства, действующую определенный период времени, образ устройства можно загрузить в среду моделирования (к примеру, виртуальную лабораторию GNS3 или EVE-NG) и провести тесты в рамках модели сети конкретного объекта.

В целях автоматизации выбора средств защиты информации было разработан модуль программы оптимального выбора на высокоуровневом языке программирования C# в среде Microsoft Visual Studio 2017. Разработка реализует описанный выше метод оптимального выбора средств защиты информации по методу структурирования функции качества. В качестве исходных данных программа принимает таблицы оценок альтернатив и корреляции в формате *.csv.

Общий интерфейс программы после загрузки исходных данных представлен на рисунке 1.

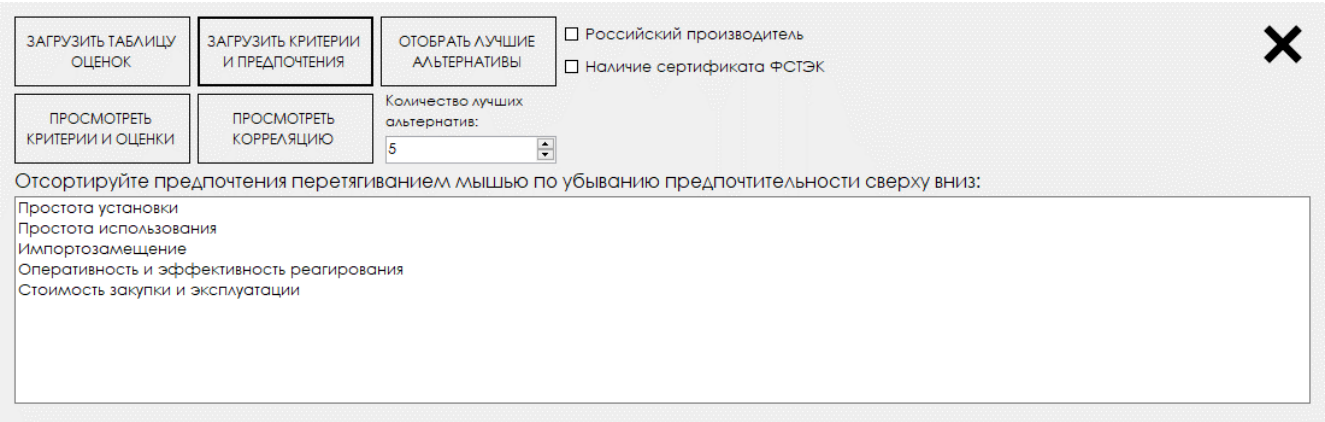

Рис.1 – Вид основной формы приложения после загрузки исходных данных *[составлено авторами]

После загрузки исходных таблиц необходимо ранжировать предпочтения по убыванию важности сверху вниз. Ввиду реализованной технологии Drag’n’Drop это удобнее делать перетаскиванием мышью, чем проставлением

индексов значимости каждому предпочтению. При необходимости следует указать условия наличия сертификата ФСТЭК, российского производства и выбрать количество искомых лучших альтернатив. После нажатия на кнопку «Отобрать лучшие альтернативы» открывается форма просмотра результатов. Вид формы при различных условиях представлен на рисунках 2, 3, 4.

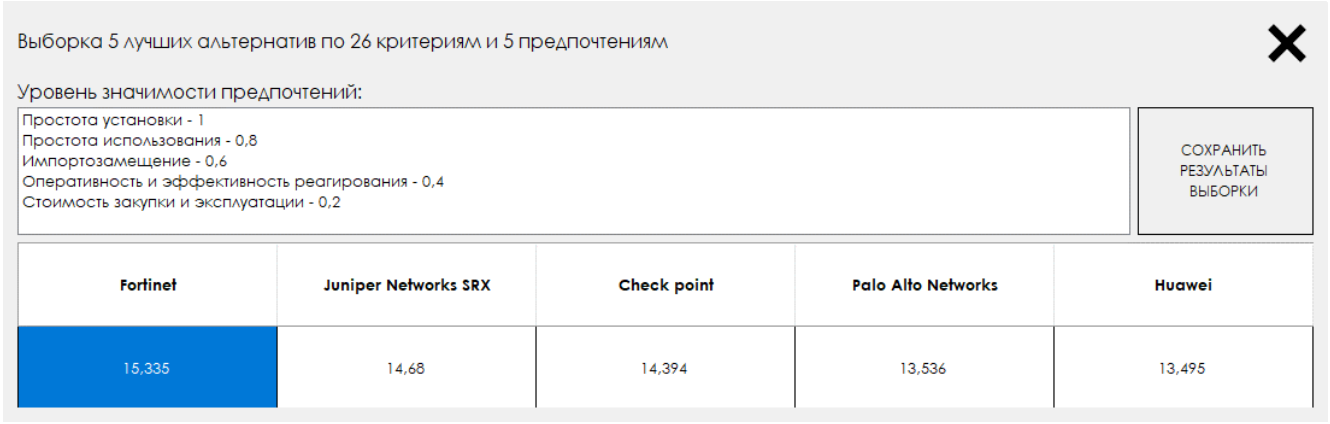

Рис.2 – Форма просмотра результатов *[составлено авторами]

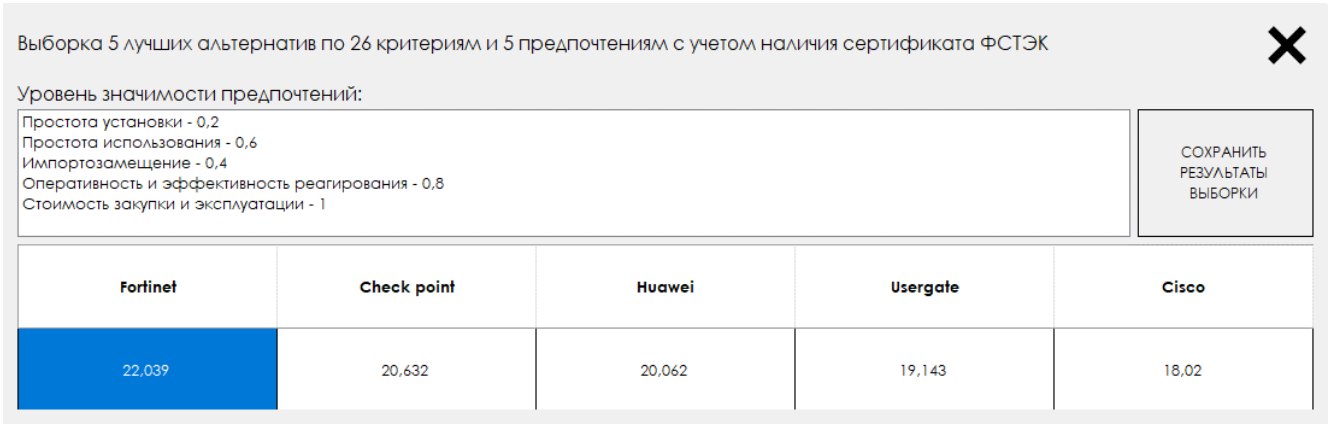

Рис.3 – Форма просмотра результатов *[составлено авторами]

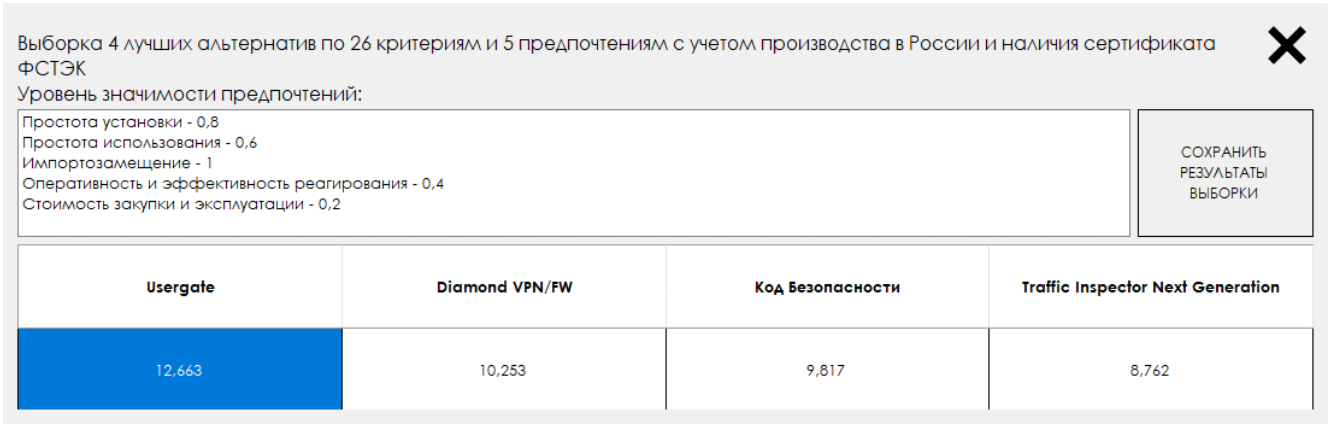

Рис.4 – Форма просмотра результатов *[составлено авторами]

На форме просмотра результатов также имеется кнопка «Сохранить результаты выборки», при нажатии на которую формируется отчет о произведенном выборе альтернатив с последующим сохранением в текстовый файл формата *.txt. Вид отчета в диалоговом окне предварительного просмотра представлен на рисунке 5.

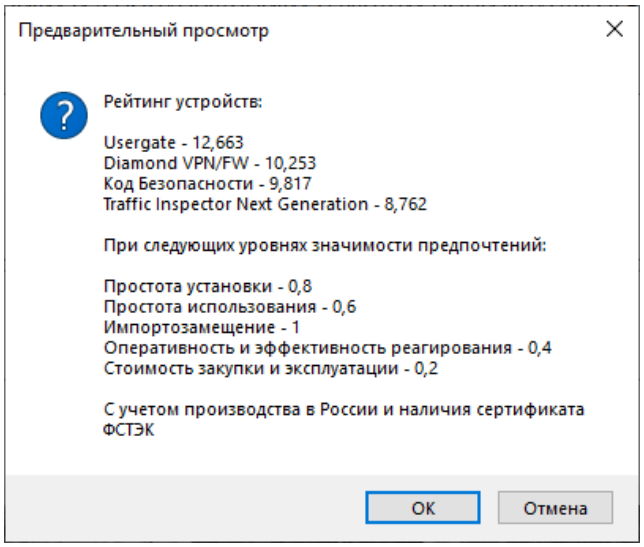

Рис.5 – Отчет в диалоговом окне предварительного просмотра *[составлено авторами]

Помимо этого, в виртуальной лаборатории GNS3 был собран и протестирован виртуальный тестовый полигон с одним из вариантов топологии на основе

структуры локальной вычислительной сети информационного объекта для проверки эффективности и интеграционных свойств универсального шлюза безопасности Fortinet FortiGate (Рис.6).

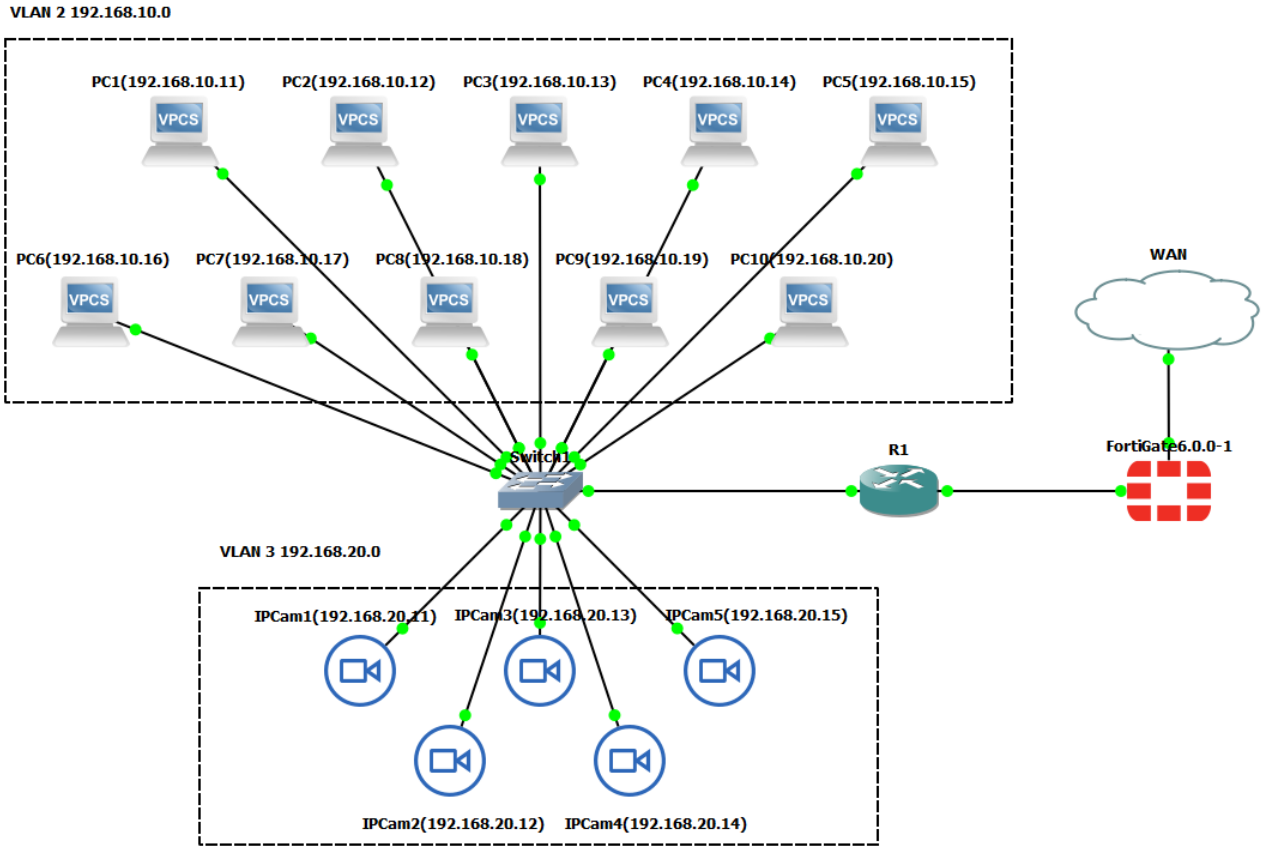

Рис.6 – Виртуальный тестовый полигон в среде GNS3 *[составлено авторами]

Таким образом, была разработана и верифицирована комплексная методика оптимального выбора средств защиты информации для подсистемы сетевой безопасности с учетом особенностей локальной вычислительной сети конкретного информационного объекта на основе метода структурирования функции качества и имитационного моделирования. Разработанная на основе методики программа позволяет эффективно и точно оценить и ранжировать набор средств защиты информации и вывести полученные данные в отчет, а собранный виртуальный стенд – оценить эффективность принятых решений в контексте локальной вычислительной сети конкретного информационного объекта.

Библиографический список:

1. Т.Т. Зангиев, А.В. Романенко. Оптимальный выбор средств защиты информации при нечетких исходных данных // Химия, физика, биология, математика: теоретические и прикладные исследования: Сб. ст. по материалам XI-XII Международной научно-практической конференции «Химия, физика, биология, математика: теоретические и прикладные исследования». – № 5-6(6). – М., Изд. «Интернаука», 2018.

2. А.Г. Тутыгин, В.Б. Коробов Преимущества и недостатки метода анализа иерархий // Известия РГПУ им. А.И. Герцена. – 2010. - №122.

3. Толмачёв С.Г. Принятие проектных решений на основе нечеткого отношения предпочтения // Информационно-управляющие системы. – 2014. - №5 (72).

4. Сапунова Т.А., Рудакова А.И., Тыщенко О.А. Развертывание функции качества (QFD) как метода структурирования пожеланий и нужд потребителя // Вектор экономики. – 2019. - №4. – URL: http://www.vectoreconomy.ru/images/publications/2019/4/economicsmanagement/Sapunova_Rudakova_Tyshchenko.pdf

5. Сравнение универсальных шлюзов безопасности USG (NGFW). Часть 1. [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/compare/USG-NGFW, свободный (дата обращения: 1.05.20)

6. Сравнение универсальных шлюзов безопасности USG (NGFW). Часть 2. [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/compare/USG-NGFW-part2, свободный (дата обращения: 1.05.20)

Оригинальность 86%