МЕТОДЫ И СРЕДСТВА ОЦЕНИВАНИЯ КАЧЕСТВА РЕАЛИЗАЦИИ ФУНКЦИОНАЛЬНЫХ И ЭКСПЛУАТАЦИОННО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДУПРЕЖДЕНИЯ ВТОРЖЕНИЙ НОВОГО ПОКОЛЕНИЯ

Гаценко О.Ю.[1], Мирзабаев А.Н.[2] , Самонов А.В.[3]

В статье представлены предложения по совершенствованию и развитию научно–методического, алгоритмического и программного обеспечения процессов обоснования и проверки качества реализации требований к функциональным и эксплуатационно–техническим характеристикам (ФЭТХ) систем обнаружения и предупреждения вторжений нового поколения (СОПВ–НП), обладающих более совершенными возможностями для противодействия современным методам и средствам реализации киберугроз. Опираясь на базовые положения, принципы и методы, разработанные в рамках таких научно–практических дисциплин как исследование операций, системотехника, системная и программная инженерия, определено, что наиболее полно и объективно качество СОПВ–НП проявляется в процессе ее использования по назначению и выражается в форме оценки эффективности ее функционирования, которая отражает степень достижения стоящих перед ней целей с учетом затрат ресурсов и времени. В связи с этим был сделан вывод о том, что основным способом получения близких к реальным значениям оценок показателей эффективности функционирования СОПВ–НП является их тестирование на испытательном стенде, достаточно полно и точно моделирующем предполагаемые условия применения системы. В качестве основных показателей качества реализации ФЭТХ СОПВ–НП предложено использовать следующие метрики: обобщенную функциональную полноту и корректность решения целевых задач, производительность системы в заданных режимах ее функционирования, надежность и устойчивость в условиях реализации против СОПВ специальных воздействий, способность противодействовать техникам и методам обмана и обфускации, обобщенную стоимость владения. Для обеспечения реализации данного подхода на практике разработаны методы, алгоритмы и программное обеспечение получения и оценивания значений показателей качества СОПВ–НП. Достоверность и практическая значимость разработанных методов и средств подтверждена посредством их успешного апробирования для тестирования ряда современных СОПВ–НП.

***Ключевые слова**: компьютерные атаки, киберугрозы, уязвимости, функциональные и эксплуатационные характеристики, система обнаружения вторжений, методы и средства тестирования, техники обмана и обфускации*

DOI: 10.21681/2311-3456-2018-2-24-32

Введение

В настоящее время наблюдается тенденция увеличения числа и серьезности компьютерных инцидентов, связанных с воздействием компьютерных атак на объекты критической информационной инфраструктуры (КИИ) государства через глобальные информационные сети, магистральное цифровое коммуникационное оборудование и внешние беспроводные устройства. Для реализации киберугроз злоумышленники используют изощренные методы и средства проникновения и внедрения вредоносного кода, скрытые каналы управления и воздействия, специальные приемы и техники обмана и обфускации. Это обуславливает необходимость опережающего развития и совершенствования методов и средств противодействия этим угрозам, их комплексирования, интеграции и обеспечения более высокого уровня управляемости и интеллектуальности. Одним из наиболее перспективных направлений решения данной задачи является создание и использование систем обнаружения и противодействия киберугрозам, интегрирующих в себе функции сразу нескольких средств защиты и способных противо-

1 Гаценко Олег Юрьевич, доктор технических наук, старший научный сотрудник, АО НИИ ПС, Санкт-Петербург, Россия, E-mail: gatcenko@mail.ru

2 Мирзабаев Алишер.Нигматджонович, Военно-космическая академия им. А.Ф. Можайского, Санкт-Петербург, Россия, E-mail: ali_mir73@mail.ru

3 Самонов Александр Валерьянович, кандидат технических наук, доцент, Военно-космическая академия им. А.Ф. Можайского, Санкт-Петербург, Россия, E-mail: a.samonov@mail.ru

стоять современным техникам обфускации и обмана, получившим название систем обнаружения и предотвращения вторжений нового поколения (СОПВ-НП).

Основными проблемными вопросами, которые необходимо решить при создании новых или выборе из числа существующих систем, являются задача обоснования состава и структуры требований к функциональным и эксплуатационно-техническим характеристикам (ФЭТХ) СОПВ и задача оценивания качества их реализации. Как показал проведенный анализ, имеющееся в распоряжении исследователей и разработчиков научно-методическое, алгоритмическое и программное обеспечение решения данных задач не в полной мере отвечает современным вызовам и потребностям. Основными направлениями его развития и совершенствования, с нашей точки зрения, являются:

1) обоснование систематизированного комплекса требований к ФЭТХ СОПВ-НП, максимально полно и точно учитывающего особенности среды и условия их применения;

2) разработка методов и средств измерения, расчета и оценивания качества реализации ФЭТХ СОПВ-НП на испытательном стенде.

В статье представлены результаты исследований и работ, направленных на решение указанных выше задач.

1. Основные этапы методики оценивания качества реализации ФЭТХ СОПВ-НП

Теоретическая и методологическая основа создания и исследования сложных программно-технических систем, к которым относятся СОПВ-НП, разрабатывается в рамках таких научно-практических дисциплин как исследование операций [1, 2], системотехника, системная и программная инженерии [3-5]. В соответствии с базовыми положениями и принципами этих дисциплин объективно качество СОПВ-НП проявляется в процессе ее использования по назначению и выражается в форме оценки эффективности ее функционирования, которая отражает степень достижения стоящих перед ней целей с учетом затрат ресурсов и времени. Оценивание и анализ эффективности функционирования СОПВ-НП представляет собой триединую задачу:

– оценивания эффективности выполнения целевой функции;

– анализа эффективности выполнения целевой функции;

– оптимального синтеза средства, обеспечивающего требуемую эффективность выполнения функции.

Первые две задачи объединяются под названием прямой задачи, предназначенной для оценивания возможностей существующих систем и принятия решения по выбору наиболее пригодной или оптимальной. Обратная задача решается при проектировании новой системы для обоснования требований к ее составу, структуре, функциональным и эксплуатационным характеристикам. Основными этапами решения этих задач являются [2]:

1. Анализ и декомпозиция целевого предназначения (функций) системы.

2. Выбор показателей эффективности выполнения целевых функций.

3. Обоснование критерия оценивания эффективности выполнения целевых функций.

4. Разработка математических (имитационных) моделей выполнения системой целевых функций.

5. Вычисление показателей эффективности выполнения целевых функций.

6. Оценивание эффективности выполнения целевых функций и принятие решения.

7. Исследование влияния ЭТХ системы на эффективность выполнения целевых функций и принятие решения.

Эффективность обладает определенной интенсивностью своего проявления, которая называется показателем эффективности (ПЭ). ПЭ системы – это количественная характеристика результата ее функционирования в течение определенного периода времени при заданных характеристиках ее состояния и определенных внешних воздействиях. Для принятия решения о степени достижения цели, необходимо обосновать критерий эффективности, т.е. правило, позволяющее сопоставлять СОПВ, характеризующихся различной степенью достижения цели, и осуществлять направленный выбор наиболее пригодных или оптимальных из них. Основным способом получения значений показателей эффективности функционирования СОПВ-НП является проведение тестовых испытаний в условиях максимально приближенных к реальным. При выборе и обосновании показателей и критериев эффективности выполнения целевых функций необходимо максимально полно и точно учитывать предполагаемые условия эксплуатации СОПВ. Математические модели и средства моделирования должны позволять описывать и оценивать влияние ЭТХ системы на эффективность выполняемых ею операций, а также разрабатывать и выполнять тестовые сценарии. Обоснованный выбор наиболее адекватных и эффективных решений и средств осуществляется посредством сравнения полученных в ходе испытаний результатов

(значений ФЭТХ СОВ) с заданными требованиями.

На рисунке 1 представлена схема, иллюстрирующая последовательность и содержание основных этапов методики подготовки и проведения испытаний СОПВ-НП с целью получения реальных оценок эффективности ее функционирования в заданных условиях применения. Основными из них являются:

1. Обоснование состава и структуры требований к ФЭТХ СОПВ-НП на основе анализа модели угроз и условий ее применения, а также требований и рекомендаций соответствующих нормативно-методических документов (НМД).

2. Разработка «Программы и методик проведения испытаний СОПВ-НП» для разработанного перечня требований к ФЭТХ СОПВ-НП.

3. Подготовка испытательного стенда для проведения тестовых испытаний СОПВ-НП в соответствии с утвержденными «Программой и методиками испытаний СОПВ-НП».

4. Разработка наборов тестовых данных для проведения испытаний СОПВ-НП.

5. Проведение испытаний в соответствии с «Программой и методиками испытаний СОПВ-НП».

6. Анализ полученных результатов, оценивание качества СОПВ-НП, принятие решений.

2. Обоснование состава и структуры комплекса требований к функциональным и эксплуатационно-техническим характеристикам СОПВ-НП

Целевым предназначением СОВ в соответствии с требованиями НМД ФСТЭК является реализация трех основных операций: сбор данных о событиях ИБ из различных источников, обнаружение и реагирование на попытки информационно-технических воздействий (ИТВ) в отношении защищаемых ресурсов в реальном режиме времени[4]. Для оценивания эффективности решения этих задач с помощью СОПВ в настоящее время используются показатели полноты, точности и оперативности. При решении указанных выше задач СОПВ-НП должны обеспечивать [6-9]:

- высокую производительность и оперативность обнаружения и предупреждения атак;

- высокую надежность и стабильность при высоких нагрузках и атаках, направленных на СОПВ;

- обнаружение и противодействие известным техникам обмана и обхода средств защиты;

- иметь приемлемую общую стоимость владения.

Формирование полного и адекватного условиям эксплуатации комплекса требований к представленным выше ФЭТХ СОПВ осуществляется на основе анализа следующих документов:

1) технического задания (ТЗ) и задания по безопасности (ЗБ) для СОПВ;

2) конструкторской и эксплуатационной документации (КЭД) на СОПВ;

3) требований к СОПВ, изложенных в соответствующих НМД.

Наиболее важной информацией, характеризующей условия применения СОПВ, являются:

- данные о сетевой инфраструктуре и топологии защищаемой информационной системы (ИС);

- данные о составе и характеристиках технических и программных средств, установленных на объектах защищаемой ИС;

- данные о критических элементах защищаемой ИС и выполняемых ими функциях;

- положения и требования политики безопасности, принятой в защищаемой ИС.

В результате анализа этих данных определяется перечень объектов (маршрутизаторов, коммутаторов, серверов приложений и баз данных, рабочих мест, средств защиты и т.д.), которые должна защищать СОПВ. Для каждого объекта из этого перечня определяется список уязвимостей аппаратного и программного обеспечения и формируется перечень атак, которые могут быть реализованы. Особое внимание следует уделить критичным элементам ИС и наиболее опасным атакующим воздействиям. В результате проведенного анализа формируются следующие списки и массивы информационных объектов:

$W = \{w_1, w_2, \dots, w_n\}$ - состав объектов защищаемой ИС;

$V = \{V_{w1}, V_{w2}, \dots, V_{wn}\}$ – перечень уязвимостей ИС, где

$V_{wi} = \{v_{wi}^1, v_{wi}^2, \dots, v_{wi}^k\}$ – описания уязвимостей по каждому *wi* элементу ИС;

$E = E_{v_{w1}}, E_{v_{w2}}, E_{v_{wn}}$ - описания атак (exploits), которые могут быть реализованы в отношении элементов ИС - *W*, в т.ч. с использованием уязвимостей ее элементов - V_{wi}.

Для разработки указанных выше списков и массивов используются специализированные базы данных, содержащие описание уязвимостей и атак.[5] Полученные списки атак, направленных на конкретные элементы ИС, должны быть отранжи-

4 Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. N 638. http://fstec.ru/

5 http://capec.mitre.org, http://www.cvedetails.com/, http://www.bdu.fstec.ru/, https://www.exploit-db.com/, https://nvd.nist.gov

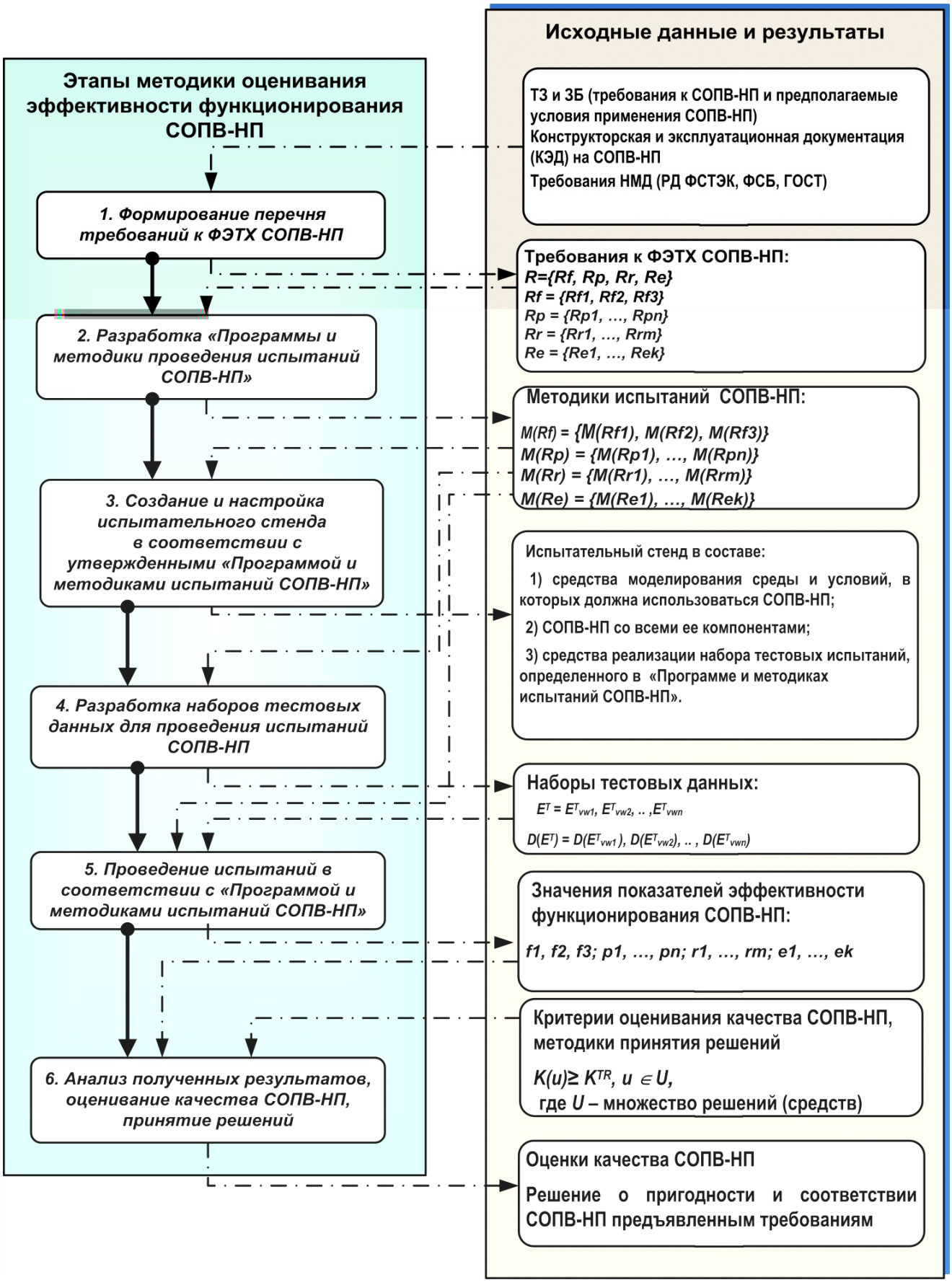

***Рис. 1**. Этапы методики оценивания эффективности функционирования СОПВ-НП*

рованы по убыванию уровня критичности создаваемой угрозы для определения приоритетности и последовательности проводимых испытаний.

3. Рекомендации по подготовке тестовых наборов и проведению испытаний СОПВ-НП

Основным способом получения оценок качества реализации функциональных и эксплуатационно-технических характеристик СОПВ-НП является проведение комплекса испытаний в соответствии с программой и методиками: $M(Rf)$, $M(Rp)$, $M(Rr)$, $M(Re)$ на основе специально разработанных тестовых наборов: $D(E^T) = D(E^T_{vw1}), D(E^T_{vw2}), .., D(E^T_{vwn})$, моделирующих определенные ситуации и условия применения системы. Основными факторами, характеризующими эти ситуации и условия, являются топология, способы функционирования и технические характеристики защищаемых ресурсов, а также модели потенциальных нарушителей. На основе учета этих факторов формируются соответствующие тестовые наборы, которые различаются по следующим параметрам [6 -9]:

1) составу и структуре сетевого трафика с точки зрения типов и соотношения анализируемых протоколов;

2) составу и структуре сетевого трафика с точки зрения количества и типов атакующих воздействий;

3) скорости поступления данных, измеряемой в пакетах в секунду - pps (packet per second) и/или в мегабитах в секунду - mbs (megabit per second);

4) количеству соединений определенного типа, устанавливаемых в секунду;

5) количеству одновременно поддерживаемых соединений (всего и определенных типов по отдельности).

Кроме того, тестовые наборы должны включать примеры использования следующих техник и методов обмана и обхода СОПВ-НП [10 - 12]:

1) фрагментация IP пакетов (IP Packet Fragmentation);

2) сегментация потока TCP пакетов (Stream Segmentation);

3) фрагментация RPC пакетов (RPC Fragmentation);

4) обфускация URL адресов (URL obfuscation);

5) обфускация HTML документов (HTML Obfuscation);

6) сжатие и архивирование HTTP трафика (HTTP Compression);

7) кодирование полезной нагрузки (Payload Encoding)

8) фальсификация FTP/Telnet (FTP/Telnet Evasion);

9) мутация полезной нагрузки (наполнение случайными данными) (Payload Padding).

Для формирования тестовых наборов можно использовать такие средства как HPING3, IDSwakeup, TCPReplay, TRex.

Тестирование СОПВ-НП предлагается проводить в следующем порядке [6, 13 -15]:

1) испытания системы для определения предельных скоростей захвата и корректной обработки сетевого трафика, не содержащего атак;

2) тестирование при обычных рабочих нагрузках на сетевом трафике, который содержит атаки определенных типов;

3) тестирование системы на предельных нагрузках на сетевом трафике, который содержит атаки определенных типов в определенном количестве.

На рисунке 2 представлена схема проведения испытаний первого типа, в ходе которых оцениваются полнота Фп и точность Фт реализации функциональных возможностей СОПВ-НП, обеспечивающих корректную идентификацию и обработку сетевых протоколов, потоков и приложений, а также измеряется ее максимальная пропускная способность V_{max}. В качестве исходных данных при реализации серии испытаний СОПВ-НП с помощью соответствующих тестовых наборов используются следующие параметры:

V_{max} – максимальное значение скорости сетевого трафика, с которого начинаются испытания;

ΔV_{mp} – точность, с которой необходимо рассчитать оценку пропускной способности;

K_{mp} – требуемое значение коэффициента, характеризующего процент потерь при захвате и обработке трафика.

Если при тестировании потери превышают максимально допустимое значение, т.е. если $S/(V_{max}*t) < K_{mp}$, где S – объем обработанного трафика, а $V_{max}*t$ – объем поступившего за время t, то скорость подачи трафика уменьшается на величину равную половине ΔV. Если потерь нет, то скорость увеличивается на половину текущего значения ΔV. Испытания завершаются тогда, когда выполняются два условия $S/(Vmax*t) \geq Kmp$ и $\Delta V \leq Vmp$. В результате проведенных испытаний получаем оценки значений показателей качества, характеризующих полноту $Фп$, точность $Фт$ и производительность V_p СОПВ-НП.

Для проведения испытаний второго и третьего типов, т.е. тестирования СОПВ-НП на сетевом трафике, который содержит атаки, необходимо определить перечень наиболее актуальных и представляющих реальную угрозу для защищаемых ресурсов способов реализации сетевых

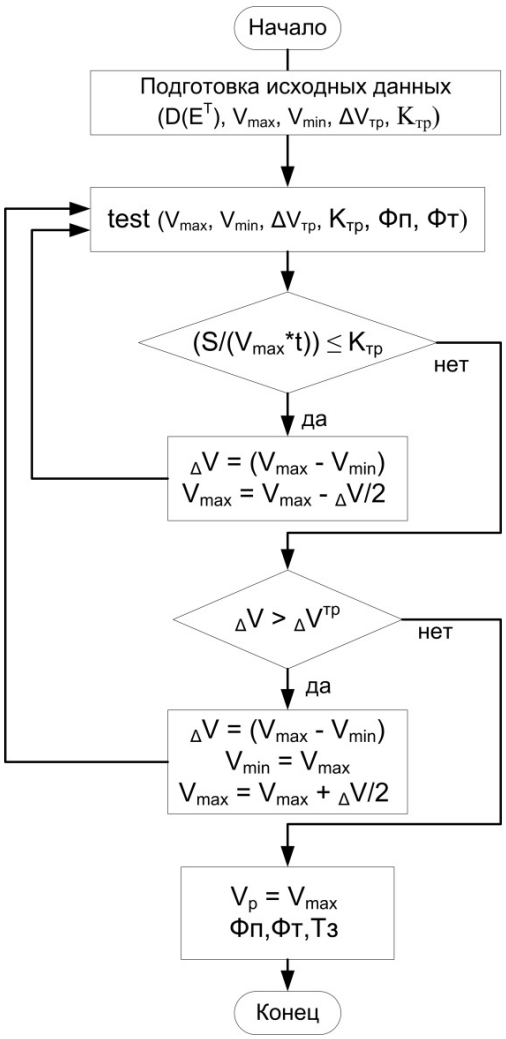

***Рис. 2**. Схема алгоритма тестирования и расчета показателей качества СОПВ-НП*

атак. Данная задача решается на основе анализа особенностей топологии и технических характеристик защищаемых ресурсов, использования актуальных баз данных угроз, уязвимостей и способов реализации атак, а также с помощью таких средств моделирования ИТВ как Scapy Framework [16], Metasploit Framework [17], pytbull [18], TRex [19], NSL-KDD, ADFA-LD, UNSW-NB15 [20 - 22] и др.

В качестве показателей качества реализации функциональных возможностей СОПВ-НП предлагается использовать комплексный показатель Ф=<Фп, Фт, Фо>, состоящий из трех метрик. Первая метрика Фп характеризует полноту системы, вторая Фт - точность (корректность), третья Фо является обобщенной оценкой полноты и точности. Расчет этих показателей может быть осуществлен на основе следующих исходных данных:

1) Ntp - количество атак, обнаруженных правильно (true positive);

2) Nfp - число ложных срабатываний (false positive);

3) Nfn - число пропусков атак, присутствовавших в тестовом трафике (false negative);

4) Ntn - число «правильных» пропусков (true negative).

Показатель *Фп* рассчитывается по следующей формуле: $Фп = Ntp /(Ntp + Nfn)$. Показатель *Фт* соответствует доле правильно обнаруженных атак среди всех обнаруженных и рассчитывается по формуле: $C = Ntp /(Ntp + Nfp)$. Показатель эффективности *Фо* учитывает значения всех четырех метрик, полученных в ходе испытаний, и рассчитывается по следующей формуле: $Фо=(Ntp + Ntn)/(Ntp + Ntn + Nfp + Nfn)$.

Описанная выше методика была апробирована для тестирования трех СОПВ: Snort 3.0, Suricata 3.2.1 и Bro 2.5.1. В таблице 1 представлены полученные в ходе испытаний оценки трех показателей: Фо – обобщенной полноты и точности, V_n - пропускной способности (в mbs) и $T_З$ – временной задержки (ms).

Как видно из таблицы, с увеличением количества атак в тестовых наборах значения данных показателей существенно снижаются, что в ряде случаев приводит к пропуску атак. Наилучшие результаты продемонстрировала СОПВ Suricata 3.2.1.

Таблица 1.
Результаты тестирования СОПВ

Тестовый набор	Результаты тестирования СОВ по трем показателям: Фо, Vп, Тз								
	Snort 3.0			Suricata 3.2.1			Bro IDS 2.5.1		
	Фо	*Vп*	*Тз*	*Фо*	*Vп*	*Тз*	*Фо*	*Vп*	*Тз*
TCP без атак	-	1013	268	-	1446	158	-	1825	717
TCP с 5% атак	0,92	990	269	0,92	1310	169	0,85	1830	861
TCP с 10% атак	0,85	937	304	0,86	782	315	0,81	1340	1001
TCP с 15% атак	0,81	759	460	0,84	498	452	0,78	1210	1062

Выводы

В настоящей статье предложен подход к оцениванию качества реализации ФЭТХ СОПВ-НП. Установлено, что основными показателями качества реализации СОПВ-НП являются: обобщенная функциональная полнота и корректность обнаружения и предотвращения атак, производительность в заданных режимах работы системы, надежность и устойчивость в условиях реализации против СОПВ специальных ИТВ, способность противодействовать техникам и методам обмана и обфускации, обобщенная стоимость владения. Определено, что основным способом получения близких к реальным значениям оценок показателей эффективности функционирования СОПВ-НП является тестирование систем на испытательном стенде, достаточно полно и точно моделирующем предполагаемые условия применения системы. Для обеспечения реализации данного подхода на практике разработаны методы и алгоритмы получения и оценивания значений показателей качества СОПВ-НП. Достоверность и практическая значимость разработанных методов и средств подтверждена посредством их успешного использования для тестирования ряда современных систем.

***Рецензент**: Езерский Владимир Васильевич, доктор технических наук, профессор, заместитель генерального директора по науке и развитию, АО НИИ ПС, E-mail office@nii-ps.ru.*

Литература

1. Вентцель Е.С. Исследование операций: задачи, принципы, методология: учебное пособие / 5-е изд., стер. — М.: КНОРУС, 2013. — 192 с.
2. Петухов, Г.Б. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем/ Г. Б. Петухов, В. И. Якунин. – М.: АСТ, 2006. – 504 с.
3. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
4. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264-270.
5. Кондратьев А.А., Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. Методологическое обеспечение интеллектуальных систем защиты от сетевых атак// Современные проблемы науки и образования. – 2014. – № 2.; URL: http://www.science-education.ru/ru/article/view?id=12875 (дата обращения: 26.04.2018).
6. Test Methodology. Next Generation Intrusion Prevention System (NGIPS) v3.0 (NGFW) 17.03.2017. https://research.nsslabs.com/reports/free-120/files/NSSLabsNextGeneratio (дата обращения: 26.04.2018).
7. ASD-Approved Protection Profile. Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS). Ver. 1.0. https://www.asd.gov.au/infosec/epl/profiles.htm (дата обращения: 26.04.2018).
8. IPS performance tests show products must slow down for safety http://www.networkworld.com/article/2306671/network-security/ips-performance-tests-show-products-must-slow-down-for-safety.html (дата обращения: 24.04.2018).
9. А.Г. Богораз, О.Ю. Пескова. Сравнительный анализ методик оценки межсетевых экранов Южный федеральный университет. https://cyberleninka.ru/article/n/metodika-testirovaniya-i-otsenki-mezhsetevyh-ekranov (дата обращения: 26.04.2018).
10. SANS Institute InfoSec Reading Room. Phillip Bosco. Intrusion Detection and Prevention Systems Cheat Sheet: Choosing the Best Solution, Common Misconfigurations, Evasion Techniques, and Recommendations. January 20, 2016.
11. SANS Institute InfoSec Reading Room. Author: Pierce Gibbs. Intrusion Detection Evasion Techniques and Case Studies. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-evasion-techniques-case-studies-37527 (дата обращения: 26.04.2018).
12. NSS Labs Evasions Test Methodology v1.0. https://www.nsslabs.com/research-advisory/library/industry/methodologies/advanced-endpoint-protection-test-methodology-v1-0/advanced-endpoint-test-methodology-advanced-endpoint-v1-0/ (дата обращения: 26.04.2018).
13. Nickerson C. и др. The Penetration Testing Execution Standard / Chris Nickerson, Dave Kennedy, Chris John Riley, Eric Smith, Iftach Ian Amit, Andrew Rabie, Stefan Friedli, Justin Searle, Brandon Knight, Chris Gates, Joe McCray, Carlos Perez, John Strand, Steve Tornio, Nick Percoco, Dave Shackelford, Val Smith, Robin Wood, Wim Remes, Rick Hayes. 30.04.2012 [Электронный ресурс]. // Penetration Testing Execution Standarts [сайт]. URL: http://www.pentest-standard.org/index.php/ PTES_Technical_Guidelines (дата обращения 16.02.2018).
14. Rathore B. и др. ISSAF — Information System Security Assesment Framework / Rathore B., Brunner M., Dilaj M., Herreragh O., Brunati P., Subramaniam R., Raman S., Chavan U. 30.04.2006. 1264 p. URL: http://www.oissg.org/ issaf02/issaf0.1-5.pdf (дата обращения 16.03.2018).
15. Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. W. Haidera, J. Hua,,1, J. Slaya, B.P. Turnbulla, Y. Xieb. Journal of Network and Computer Applications. journal homepage: www.elsevier.com/locate/jnca/ (дата обращения: 26.04.2018).
16. http://scapy.readthedocs.io/en/latest (дата обращения: 26.04.2018).
17. https://www.metasploit.com (дата обращения: 26.04.2018).
18. http://pytbull.sourceforge.net/index.php (дата обращения: 26.04.2018).
19. https://libraries.io/github/napatech/trex-core (дата обращения: 26.04.2018).

20. Data Mining and Intrusion Detection Systems. International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016. www.ijacsa.thesai.org (дата обращения: 26.04.2018).
21. https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys (дата обращения: 26.04.2018).
22. Manu Bijone, «A Survey on Secure Network: Intrusion Detection & Prevention Approaches.» American Journal of Information Systems, vol. 4, no. 3 2016. http://pubs.sciepub.com/ajis/4/3/2 (дата обращения: 26.04.2018).

METHODS AND MEANS OF EVALUATING THE QUALITY OF IMPLEMENTATION FUNCTIONAL AND PERFORMANCE CHARACTERISTICS OF NEXT GENERATION INTRUSION DETECTION AND PREVENTION SYSTEMS

Gacenko O[6]., Mirzabaev A.[7], Samonov A.[8]

The article presents the proposals for the improvement and development of scientific–methodological, algorithmic and software support of the processes of justification and quality control of the implementation of the requirements for functional and operational characteristics of the next generation intrusion detection and prevention systems (NGIPS), which have more advanced capabilities to counter modern methods and means of implementation of cyber threats. Based on the foundation provisions, principles and methods developed in the framework of scientific and practical disciplines such as operations research, systems engineering, system and software engineering, it is determined that the most complete and objective quality of NGIPS manifests itself in the process of its use for the intended purpose and is expressed in the form of an assessment of the effectiveness of its functioning, which reflects the degree of achievement of its objectives, taking into account the costs of resources and time. In this regard, it was concluded that the main way to obtain close to real values estimates of performance indicators NGIPS is testing systems on the test bench, sufficiently fully and accurately simulates the intended conditions of use of the system. As the main indicators of quality of implementation of NGIPS it is offered to use: the generalized functional completeness and correctness of detection and prevention of attacks, performance of the system in the given modes of its functioning, reliability and stability in the conditions of realization against NGIPS of special influences, ability to counteract technicians and methods of deception and obfuscation and the total cost of ownership. To ensure the implementation of this approach in practice, methods and algorithms for obtaining and evaluating the values of quality indicators NGIPS. The reliability and practical significance of the developed methods and tools is confirmed by means of their successful approbation for testing of a number of modern IPS.

***Keywords**: computer attacks, cyber threats, vulnerabilities, functional and operational characteristics, intrusion detection and prevention system, methods and means of testing, deception and obfuscation techniques*

References

1. Ventcel' E.S. Issledovanie operacij: zadachi, principy, metodologiya: uchebnoe posobie / 5-e izd., ster. — M.: KNORUS, 2013. — 192 s.
2. Petuhov, G.B. Metodologicheskie osnovy vneshnego proektirovaniya celenapravlennyh processov i celeustremlennyh sistem/ G. B. Petuhov, V. I. YAkunin. – M.: AST, 2006. – 504 s.
3. Markov A.S., Cirlov V.L., Barabanov A.V. Metody ocenki nesootvetstviya sredstv zashchity informacii. M.: Radio i svyaz', 2012. 192 s.
4. Barabanov A.V., Markov A.S., Cirlov V.L. Ocenka sootvetstviya sredstv zashchity informacii «Obshchim kriteriyam» // Informacionnye tekhnologii. 2015. T. 21. № 4. S. 264-270.
5. Kondrat'ev A.A., Talalaev A.A., Tishchenko I.P., Fralenko V.P., Hachumov V.M. Metodologicheskoe obespechenie intellektual'nyh sistem zashchity ot setevyh atak// Sovremennye problemy nauki i obrazovaniya. – 2014. – № 2.; URL: http://www.science-education.ru/ru/article/view?id=12875 (data obrashcheniya: 26.04.2018).
6. Test Methodology. Next Generation Intrusion Prevention System (NGIPS) v3.0 (NGFW) 17.03.2017. https://research.nsslabs.com/reports/free-120/files/NSSLabsNextGeneratio.

6 Oleg Gacenko, Dr.Sc, AO NII PS, Saint-Petersburg, Russia. E-mail: gatsen@mail.ru
7 Alisher Mirzabaev, Military space Academy A.F. Mozhaisky, Saint-Petersburg, Russia. E-mail: ali_mir73@mail.ru
8 Alexander Samonov, Ph.D, Military space Academy A.F. Mozhaisky, Saint-Petersburg, Russia. E-mail: a.samonov@mail.ru

7. ASD-Approved Protection Profile. Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS). Ver. 1.0. https://www.asd.gov.au/infosec/epl/profiles.htm
8. IPS performance tests show products must slow down for safety http://www.networkworld.com/article/2306671/network-security/ips-performance-tests-show-products-must-slow-down-for-safety.html
9. A.G. Bogoraz, O.YU. Peskova. Sravnitel'nyj analiz metodik ocenki mezhsetevyh ehkranov YUzhnyj federal'nyj universitet. https://cyberleninka.ru/article/n/metodika-testirovaniya-i-otsenki-mezhsetevyh-ekranov (data obrashcheniya: 26.04.2018).
10. SANS Institute InfoSec Reading Room. Phillip Bosco. Intrusion Detection and Prevention Systems Cheat Sheet: Choosing the Best Solution, Common Misconfigurations, Evasion Techniques, and Recommendations. January 20, 2016.
11. SANS Institute InfoSec Reading Room. Author: Pierce Gibbs. Intrusion Detection Evasion Techniques and Case Studies. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-evasion-techniques-case-studies-37527
12. NSS Labs Evasions Test Methodology v1.0. https://www.nsslabs.com/research-advisory/library/industry/methodologies/advanced-endpoint-protection-test-methodology-v1-0/advanced-endpoint-test-methodology-advanced-endpoint-v1-0/ (data obrashcheniya: 26.04.2018)
13. Nickerson C. и др. The Penetration Testing Execution Standard / Chris Nickerson, Dave Kennedy, Chris John Riley, Eric Smith, Iftach Ian Amit, Andrew Rabie, Stefan Friedli, Justin Searle, Brandon Knight, Chris Gates, Joe McCray, Carlos Perez, John Strand, Steve Tornio, Nick Percoco, Dave Shackelford, Val Smith, Robin Wood, Wim Remes, Rick Hayes. 30.04.2012 [Электронный ресурс]. // Penetration Testing Execution Standarts [сайт]. URL: http://www.pentest-standard.org/index.php/ PTES_Technical_Guidelines (data obrashcheniya 16.02.2018).
14. Rathore B. и др. ISSAF — Information System Security Assesment Framework / Rathore B., Brunner M., Dilaj M., Herreragh O., Brunati P., Subramaniam R., Raman S., Chavan U. 30.04.2006. 1264 p. URL: http://www.oissg.org/ issaf02/issaf0.1-5.pdf (data obrashcheniya 16.03.2018).
15. Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. W. Haidera, J. Hua,,1, J. Slaya, B.P. Turnbulla, Y. Xieb. Journal of Network and Computer Applications. journal homepage: www.elsevier.com/locate/jnca/ data obrashcheniya: 26.04.2018)
16. http://scapy.readthedocs.io/en/latest (data obrashcheniya: 26.04.2018)
17. https://www.metasploit.com (data obrashcheniya: 26.04.2018)
18. http://pytbull.sourceforge.net/index.php (data obrashcheniya: 26.04.2018)
19. https://libraries.io/github/napatech/trex-core (data obrashcheniya: 26.04.2018)
20. Data Mining and Intrusion Detection Systems. International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016. www.ijacsa.thesai.org (data obrashcheniya: 26.04.2018)
21. https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys (data obrashcheniya: 26.04.2018)
22. Manu Bijone, «A Survey on Secure Network: Intrusion Detection & Prevention Approaches.» American Journal of Information Systems, vol. 4, no. 3 2016. http://pubs.sciepub.com/ajis/4/3/2 (data obrashcheniya: 26.04.2018)