ПРИРОДА СЕТЕВЫХ АНОМАЛИЙ И ИХ ПОЛУНАТУРНОЕ МОДЕЛИРОВАНИЕ

К. Н. Мишин, Р. Р. Фаткиева

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

<vvi@iias.spb.su>

УДК 681.3.06

Мишин К. Н., Фаткиева Р. Р. **Природа сетевых аномалий и их полунатурное моделирование** // Труды СПИИРАН. Вып. 5 — СПб.: Наука, 2007.

Аннотация. *Описаны методы и способы реализации атак отказа в обслуживании с целью анализа и выделения значащих параметров порядка поведения системы. Выделение параметров порядка атак и угроз информационной безопасности на основе сформулированного фазового пространства позволит повысить эффективность систем обнаружения вторжений. В перспективе технология построения фазового пространства и выделение параметров порядка позволит прогнозировать появления атак и аномалий в сетевой среде.*— Библ. 3 назв.

UDC 681.3.06

Mishin K. N., Fatkieva R. R. **Nature and modeling of network anomalies** // SPIIRAS Proceedings. Issue 5, vol. — SPb.: Nauka, 2007.

Abstract. *Methods and ways of denial of service attacks realization for marking valuable invariants of system behavior are described. Marking invariants of attacks and information security threats based on defined phase space will let to icrease efficiency of intrusion detection systems. In the future technology of building phase space and marking invariants will let to predict attacks and anomalies appearance in network environment*. — Bibl. 3 items.

1. Введение

В настоящее время сетевая безопасность превращается в «узкое горлышко» в развитие ИТ. Профилактика известных угроз становится непосильной для сетевых и серверных узлов. С другой стороны для предупреждения атак неизвестной природы требуются новые стратегии, архитектуры и технологии [1, 2, 3].

Динамика усложнения атак и угроз информационной безопасности показывает, что структура потенциальных атак усложняется одновременно с усложнением вычислительных средств и сетей, что приводит к возможности использования уязвимостей, вызванных ошибками в процессе создания системы. Это влечет за собой экономический урон по причине временной неработоспособности той или иной информационной системы, а также возможность осуществлять различные скрытые действия по внедрению в информационные системы отслеживающих агентов-шпионов.

Согласно статистическим данным последних нескольких лет выявлено, что основной ущерб наносят так называемые информационные атаки отказа в обслуживании и распределенные атаки отказа в обслуживании, поэтому данная статья посвящена углубленному анализу и классификации существующих многочисленных атак «отказа в обслуживании», «распределенных атак отказа в обслуживании», а также выявлению природы сетевых аномалий. С этой целью проводится полунатурное моделирование существующих атак «отказа в обслуживании» на базе реального сегмента глобальной сети «Интернет». Данный

подход используется для создания метода идентификации и обнаружения атак на основе имитационного моделирования на стенде.

2. Анализ и классификация существующих сетевых аномалий

Анализ и выявление природы конкретного класса атак основывается на анализе цикла развития и воздействия информационной атаки или угрозы. Так, например, атаки отказа в обслуживании зачастую классифицируются как парализующие атаки и угрозы, которые уменьшают пропускную способность каналов передачи данных, выводят из строя различные сетевые сервисы и представляют собой угрозы, аккумулирующие аномальные явления на всех фазах динамики развития и воздействия угрозы информационной безопасности.

Данные атаки можно подразделить на следующие фазы: **probe** (сканирование узлов, 3-4 уровень модели открытых систем), **penetrate** (механизм проникновения в информационную систему), **persist** (внедрение в информационную систему, вредоносное воздействие на систему), **propagate** (транспортный механизм внедрения атаки отказа в обслуживании в систему), а также **paralyze** – парализация работы системы на неопределенное время.

Для реализации эффективного механизма раннего обнаружения атак и угроз информационной безопасности, необходимо исследовать механизмы зарождения, развития и завершения атаки. Для этого рассмотрим классификацию существующих механизмов защиты [1, 2] представленных на рис. 1.

Анализ представленных на рис. 1 методов защиты, показывает:

- неэффективность к воздействию потенциально неизвестной аномалии или атаки – так называемой атаки «нулевого дня» -«zero-day attack»;
- слабость механизма принятия решения в случае воздействия потенциальной угрозы;
- перенесение принятия решения на системы оперативного управления (администрирования);
- негибкую адаптируемость агентов посредством распространения на них заранее описанного шаблона политики безопасности со стороны станции оперативного управления;
- некорректное администрирование сложных вычислительных комплексов с точки зрения обеспечения высокого уровня информационной безопасности, а именно формирование формализованной политики информационной безопасности;
- существующие сигнатурные статистические системы обнаружения и предотвращения вторжений не эффективны из-за высокой зависимости от своевременного введения в базы данных сигнатур существующих атак на информационные системы. В процессе их эксплуатации возникает большое количество ложных положительных и отрицательных срабатываний, что приводит к резкому снижению эффективности контрмер данных систем. В существующих системах IDS/IPS недостаточно доработана система обнаружения и идентификации атак, так как не учитывается фактор интегральной оценки параметров поведения системы во время проявления потенциальной угрозы или аномалий;

Труды СПИИРАН. 2007. Вып. 5. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 5. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- в качестве критерия анализа для обнаружения потенциальных аномалий и угроз не используются интегральные оценки параметров порядка системы в целом из-за нелинейного поведения всей динамической системы (вычислительной сети), которая имеет большое число степеней свободы;
- применяемые методы имитационного моделирования не вскрывают сущности атак и аномалий, так как эти методы не позволяют оценить динамику развития потенциальной аномалии, в рамках рабочей вычислительной сети, обладающей большим количеством степеней свободы.

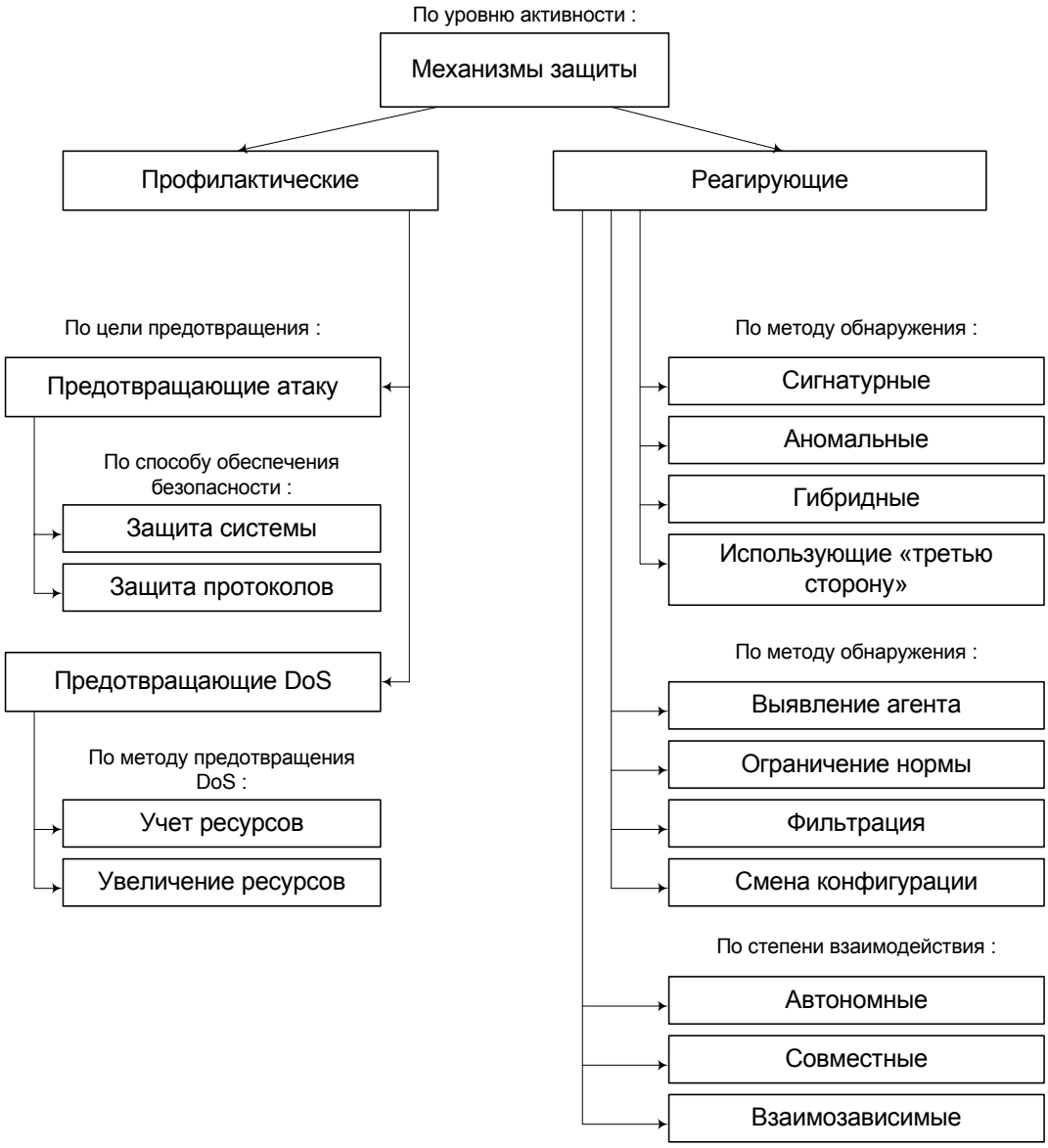

Рис. 1. Классификация существующих механизмов защиты

Труды СПИИРАН. 2007. Вып. 5. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 5. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

3. Описание стенда полунатурного моделирования

Стенд представляет собой натурную модель для исследований реализации трафика. Структурная схема стенда приводится на рис. 2

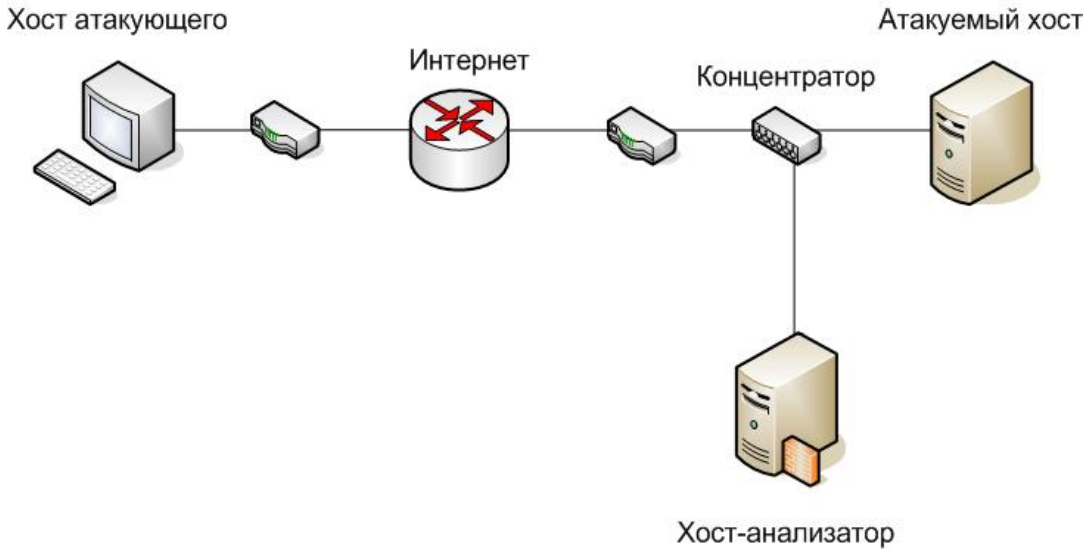

Рис. 2. Структурная схема стенда.

В ходе полунатурных исследований, «атакующий» хост производит генерирование паразитного трафика, содержащего исследуемую атаку. Трафик поступает на устройство концентратор, направляющий его далее на атакуемый хост и хост-анализатор. Оба сегмента подключены к сети Интернет через порты Fast Ethernet, в распоряжении каждого канал с пропускной способностью 100 Мбит/с. Анализатор осуществляет сканирование проходящего через него трафика атаки, формируя дамп трафика и сохраняет его в файл на жестком диске для последующей обработки. В ходе исследования поведения сетевого трафика, было собрано 5 дампов: дамп легального трафика, дамп трафика во время совершения атак SYN флуд, TCP флуд, Smurf и DoomDNS на базе следующих программных элементов и сервисов

Атакующий хост:

Операционная система: FreeBSD 6.1-RELEASE.

Используемые утилиты:

- средство аудита сети Packit 1.0;
- приложение позволяющее произвести атаку DoomDNS–Dnsflood.pl;
- утилита для тестирования производительности HTTP сервера AB – Apache server benchmarking tool.

Атакуемый хост:

Операционная система: FreeBSD 4.11-RELEASE.

Сервисы, необходимые для исследования:

- HTTP сервер Nginx 0.4.12;
- Сервер доменных имен Bind 9.3.3.

Хост-анализатор:

- Операционная система: FreeBSD 4.11-RELEASE.
- Используемые утилиты:TcpDump.

Труды СПИИРАН. 2007. Вып. 5. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 5. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

4 Определение фазового пространства

Выявление природы описанных атак, с целью их ранней идентификации требует построения соответствующего фазового пространства и выявления параметров порядка поведения системы. Для выбора параметров порядка оцениваются важные критические характеристики трафика в канале передачи. При этом следует отметить, что многие характеристики меняются во времени. Поэтому, отслеживая резкое изменение их поведения во времени, можно говорить о потенциальной аномалии или угрозе информационной безопасности. Для исследуемых типов атак перечень параметров будет различный. Выбор параметров основан на исследовании поведения всех параметров и выявлении аномальных реакций системы во время воздействия атаки. Но, несмотря на это, параметры порядка для исследуемых атак очень близки и оценить их можно с помощью табл. 1:

Таблица 1

Параметры порядка для рассматриваемых атак

Параметры порядка атаки:	**Атаки**			
	SYN flood	**Flood:**	**Smurf**	**DoomDNS**
Количество (SYN – ACK) пакетов в секунду	+	+		
Количество TCP пакетов в секунду	+	+		
Максимальное число source IP с одинаковым числом TTL в секунду	+	-	+	+
Количество различных source IP в секунду	+	-		
Количество различных source PORT в секунду				
Максимальное количество различных портов отправителя для каждого IP отправителя в секунду		+		
Количество ICMP (ECHO reply – ECHO request) в секунду			+	
Количество TCP и UDP запросов на порт назначения 53 (порт службы DNS)				
Количество UDP запросов в секунду				
Длина TCP и UDP пакета, встречающаяся максимальное число раз за секунду				

5 Результаты полунатурного моделирования

В качестве примера приведем результаты атака Smurf. Изменения количества ICMP (ECHO reply – ECHO request) в секунду представлены на рис. 3-4 и табл. 2:

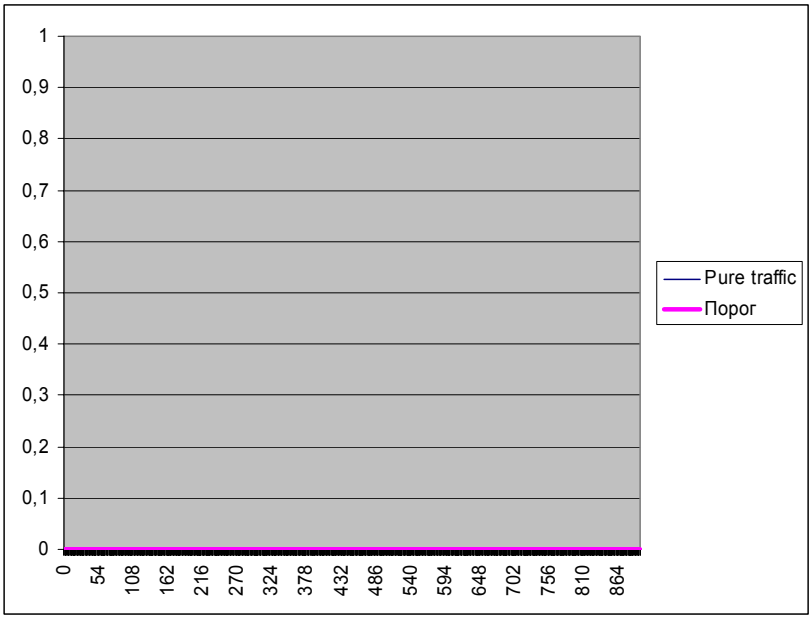

Рис. 3. Количество ICMP-пакетов при легальном трафике сети.

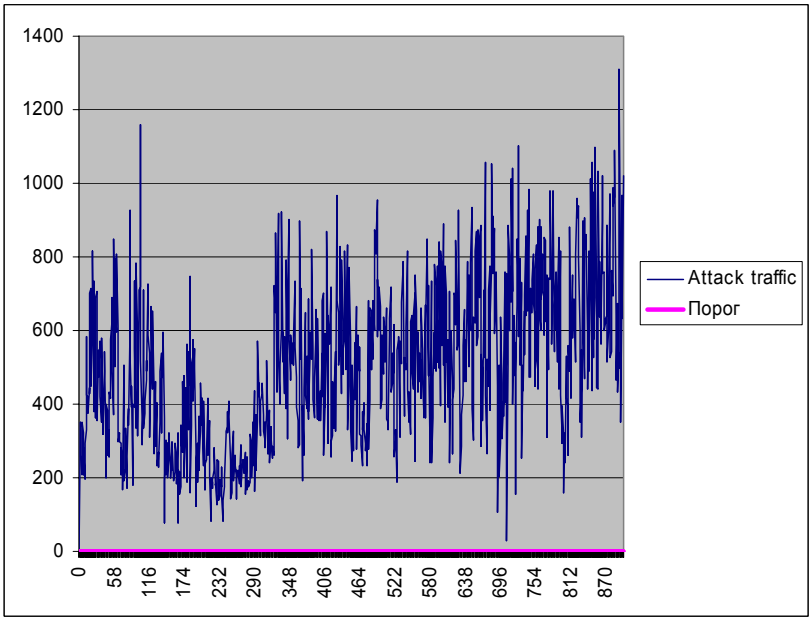

Рис. 4. Количество ICMP-пакетов при атаке.

Таблица 2

Количество ICMP-пакетов характерных для атаки Smurf

Характеристики	**Легальный трафик**	**Трафик атаки**
Пороговое значение	**0**	
Среднее арифметическое		**502,1722**
Спектральная плотность	**0**	**451955**

Труды СПИИРАН. 2007. Вып. 5. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 5. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Изменения параметра порядка — максимальное число source IP с одинаковым числом TTL в секунду представлены на рис. 5-6 и табл. 3:

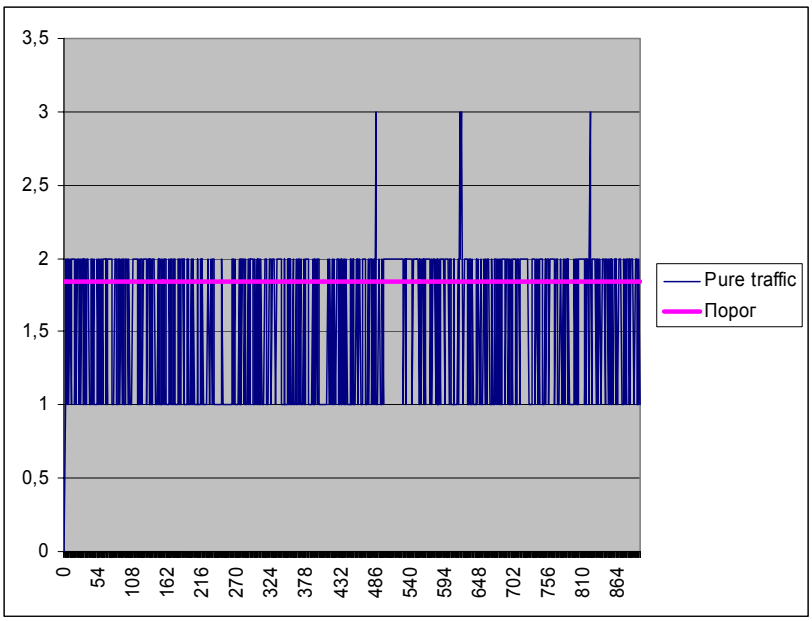

Рис. 5. Число source IP пакетов при легальном трафике сети.

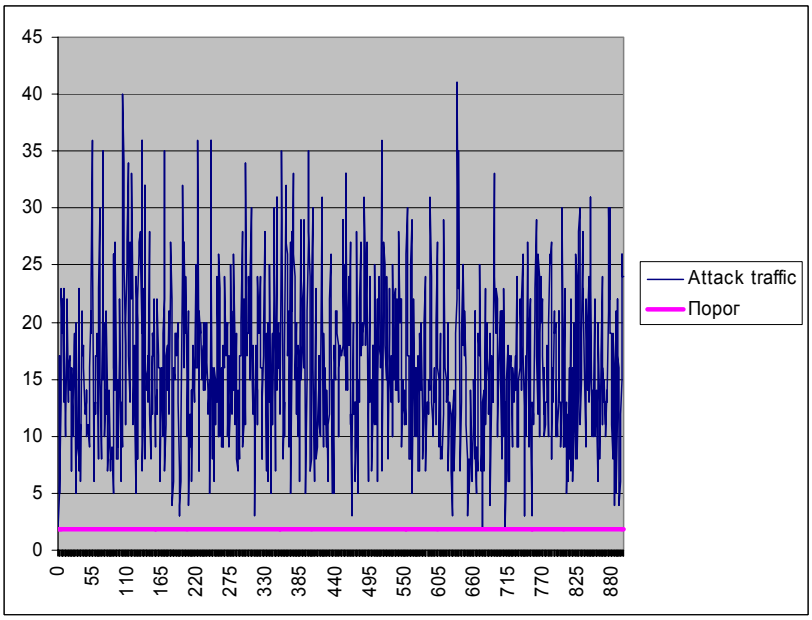

Рис. 6. Число source IP пакетов при атаке.

Таблица 3

Число source IP пакетов характерных для атаки Smurf

Характеристики	**Легальный трафик**	**Трафик атаки**
Пороговое значение	**1,845333**	
Среднее арифметическое		**16,18333**
Спектральная плотность	**1384**	**14565**

Труды СПИИРАН. 2007. Вып. 5. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 5. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

6. Заключение

На основании полученных данных и графического представления рядов, можно сделать следующие выводы:

- сравнивая пороговые и оценочные средние значения исследуемых временных рядов, можно с уверенностью судить о наличии аномалии в трафике атаки;
- по набору параметров, поведение которых было признано аномальным, можно судить о типе атаки, которая была предпринята в адрес жертвы;
- исходя из различного набора параметров, аномалии в поведении которых свойственны для исследуемых атак, можно сделать вывод о возможности определения класса применяемых атакующими хостами атаки. На основании полученной информации можно использовать различные методы реагирования, направленные на борьбу с конкретной атакой;
- для большинства параметров существует большой диапазон значений между пороговым и оценочным значением. Данный диапазон в дальнейшем может быть использован для проведения градуировки шкалы и прогнозирования возможного влияния выявленной атаки. Эта процедура очень важна для предотвращения большого числа ложных срабатываний средства детектирования атак и избежания возникновения «Dos атак второго рода».

Литература

1. *Олифер В. Г., Олифер Н. А.*, Компьютерные сети. Принципы, технологии, протоколы.СПб:.«Питер», 2001. 356 с.
2. *Котенко И. В, Степашкин М. В, Богданов В. С.* Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников. Проблемы информационной безопасности. Компьютерные системы, 2005.С. 65.
3. *Воробьев В. И., Румянцева Е. П., Фаткиева Р. Р.* Оценка эффективности инвестиций в информационную безопасность образовательных технологий // Труды РГПУ.СПб: 2007.С.47.