Для цитирования: *Алехин И.В., Бокова О.И., Коробкин Д.И., Рогозин Е.А. К вопросу о вероятности наступления ущерба в результате атаки на информационный ресурс информационно-технических систем органов внутренних дел типа «отказ в обслуживании». Вестник Дагестанского государственного технического университета. Технические науки. 2018; 45 (4): 68-77. DOI:10.21822/2073-6185-2018-45-4-68-77*
For citation: *Alekhin I.V., Bokova O.I., Korobkin D.I., Rogozin E. A. To the question of the probability of the attackment of damage as a result of attack on the information resource of information and technical systems of internal affairs type «Refusal in Service». Herald of Daghestan State Technical University. Technical Sciences. 2018; 45 (4): 68-77. (in Russ.) DOI:10.21822/2073-6185-2018-45-4-68-77*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 519.7: 004.05
DOI:10.21822/2073-6185-2018-45-4-68-77

К ВОПРОСУ О ВЕРОЯТНОСТИ НАСТУПЛЕНИЯ УЩЕРБА В РЕЗУЛЬТАТЕ АТАКИ НА ИНФОРМАЦИОННЫЙ РЕСУРС ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

Алехин И.В.[1], Бокова О.И.[1], Коробкин Д.И.[2], Рогозин Е.А.[1]
[1] Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия,
[2] Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина,
[2]394064, г Воронеж, ул. Старых Большевиков, 54 А, Россия,
[1]e-mail: ialekhin2@mvd.ru, [1]e-mail: obokova2@mvd.ru,
[1]e-mail: aevgenirogozin@yandex.ru, [2]e-mail:516420@mail.ru

Резюме. Цель. *В целях повышения защищенности ведомственных информационно-технических систем и рациональности финансовых затрат на аппаратные решения в таких системах, целесообразно провести разработку имитационной модели информационно-технической системы органа внутренних дел (ИТС ОВД), имеющей подключение к сети Интернет, для определения вероятности наступления ущерба в результате атаки типа «отказ в обслуживании». Привести и уточнить для ИТС ОВД классификацию современных сложных ИТС, что позволит на основании открытых федеральных и ведомственных нормативных документов определить вероятные угрозы информационному ресурсу ИТС ОВД, в связи с подключением к сети Интернет. Дальнейшая разработка модели ИТС ОВД произведена в среде имитационного моделирования Anylogic, что позволяет смоделировать процесс атаки типа «отказ в обслуживании» на ведомственный ресурс и исследовать вероятность наступления ущерба. Приведены выражения из аппарата систем массового обслуживания, позволяющие произвести моделирование атаки и расчет вероятности наступления ущерба, что целесообразно применить при проектировании подобных систем в ОВД.* ***Метод.*** *Аналитическое и математическое моделирование с применением аппарата систем массового обслуживания.* ***Результат.*** *Предложена имитационная модель ИТС ОВД, позволяющая определить вероятность деструктивного воздействия на ведомственные ресурсы подобных систем.* ***Вывод.*** *Направление данного исследования актуально и требует дальнейшего развития с целью выработки методики оценки наступления ущерба в ИТС ОВД.*

Ключевые слова: *информационно-техническая система органа внутренних дел, система массового обслуживания, вероятность наступления ущерба, ресурс, Интернет, угроза, «отказ в обслуживании»*

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

TO THE QUESTION OF THE PROBABILITY OF THE ATTACKMENT OF DAMAGE AS A RESULT OF ATTACK ON THE INFORMATION RESOURCE OF INFORMATION AND TECHNICAL SYSTEMS OF INTERNAL AFFAIRS TYPE "REFUSAL IN SERVICE"

Igor V. Alekhin[1], Oksana I. Bokova[1], Dmitry I. Korobkin, Evgeny A. Rogozin[1]
[1]Voronezh Institute of the Ministry of the Interior of the Russian Federation,
[1]53 Patriotov Str.,Voronezh 394065, Russia,
[2] Military Educational and Scientific Center of the Air Force
named after N.E. Zhukovsky and Y.A. Gagarin,
[4]54A Starykh Bolshevikov Str.,Voronezh 394064, Russia
[1]e-mail: ialekhin2@mvd.ru, [1]e-mail: obokova2@mvd.ru,
[1]e-mail: aevgenirogozin@yandex.ru, [2]e-mail:516420@mail.ru

Abstract Objectives *In order to improve the security of departmental information technology systems and the rationality of the financial costs of hardware solutions in such systems, it is advisable to develop a simulation model of the information technology system of an internal affairs authority (ITS ATS) connected to the Internet to determine the likelihood of damage occurring denial of service attacks. Lead and clarify for the ITS ATS a classification of modern-time complex ITS, which will allow identifying possible threats to the ITS information resource ATS based on open federal and departmental regulatory documents in connection with Internet connection. Further development of the ATS ITS model was done in the Anylogic simulation environment, which makes it possible to simulate a denial of service attack on a departmental resource and investigate the likelihood of damage occurring. The expressions from the apparatus of queuing systems are given, which allow modeling the attack and calculating the probability of damage occurrence, which is advisable to use when designing such systems in ATS.* ***Method.*** *Analytical and mathematical modeling using the apparatus of queuing systems.* ***Result.*** *A simulation model of ITS ATS is proposed, which allows to determine the probability of a destructive impact on the departmental resources of such systems.* ***Conclusion.*** *The direction of this study is relevant and requires further development in order to develop a methodology for assessing the occurrence of damage in ITS ATS.*

Keywords: *information and technical system of the internal affairs authority, queuing system, probability of damage occurrence, resource, Internet, threat, "denial of service"*

Введение. Актуальность темы данного научного исследования определяется в рамках деятельности МВД России путём проведения анализа открытых литературных источников. Из текста статьи № 11 федерального закона «О полиции» следует, что Министерство внутренних дел Российской Федерации обязано использовать в процессе выполнения возложенных государственных функций широкий набор информационных технологий и информационных систем (ИС) с целью получения, накопления и обработки информации [1]. Тем самым, создавая большой объём дополнительных задач по обеспечению бесперебойного функционирования вверенных ИС.

Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет термин информационной системы в соответствии с ГОСТ Р 50922-2006: «Защита информации. Основные термины и определения», как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [2]. При рассмотрении вышеописанной проблематики следует дополнить определение ИС словом «технические» в связи с высокой важностью обширных распределенных технических сетей, обеспечивающих функционирование ИТС ОВД.

В настоящий момент все существующие ИТС можно разделить на четыре основные класса: корпоративные ИТС, системы оперативного управления и учета, аналитические ИТС, справочные правовые системы [3].

Постановка задачи. Анализируя вышеприведенную классификацию современных сложных ИТС можно сделать вывод о том, что ИТС ОВД является крупной корпоративной ИТС с поддержанием функционала систем оперативного управления и учета, аналитических ИТС и справочно-правовых систем. Данное обстоятельство значительно увеличивает вероятность возникновения атак со стороны злоумышленников и требует обширного комплекса мероприятий по обеспечению информационной безопасности в ИТС ОВД.

Можно выделить следующие особенности современных ИТС ОВД:

1. Комплексный подход. Современные ИТС ОВД характеризуются понятием комплексности. Это подразумевает целостный подход к автоматизации технологических процессов. Если раньше в каждом территориальном отделе была своя отдельная локальная вычислительная сеть, то сейчас в МВД России функционирует в единой ИТС. Такое построение ИТС позволяет использовать информацию одного подразделения в работе других подразделений МВД России, получать сводную информацию и повышать скорость информационных потоков внутри Министерства.
2. Оперативность. В современных условиях очень важным параметром в работе МВД становится скорость обработки и доступность информации. Поэтому современные ИТС проектируются таким образом, чтобы пользователи могли получать максимум информации, доступной на текущий момент. Особое внимание уделяется оперативности информации, то есть процессам получения самой «свежей» информации, так как от этого во многом зависит эффективность принимаемых решений (например, проведение видеоконференций и т.д.).
3. Гибкость. Наиболее распространенными способами реализации этого принципа являются модульность системы (при необходимости различные функциональные модули могут отключаться или подключаться к системе) и система настроек (т.е. присутствует возможность коррекции основных параметров).
4. Распределенность. Распределенная ИТС ОВД подразумевает многоуровневую структуру и наличие иерархии серверов.
5. Взаимосвязь с другими ИТС. МВД России работает в условиях тесного взаимодействия и интенсивного информационного обмена с другими органами государственной власти, поэтому, важное значение имеет способность ИТС ОВД взаимодействовать с ИТС других организаций. В современных ИТС предусмотрена возможность импортировать и экспортировать массивы данных в общепринятых форматах обмена данными (текстовые файлы или электронные таблицы), обеспечивая широкий спектр предоставляемых государственных услуг.
6. Доступность информации извне. В последнее время значительно увеличилась степень информационной открытости МВД России для граждан. Современная ИТС ОВД должна иметь механизмы публикации различных сервисов и данных в Интернет. Естественно, не все данные МВД России делает общедоступными, поэтому большое внимание уделяется защите ИТС от несанкционированного доступа и правильной организации уровней доступа к информации.

В ИТС ОВД также существует потенциальная опасность возникновения ущерба, связанного с использованием уязвимостей злоумышленниками, причем, потерями от реализации могут являться не только финансовый, но и репутационный ущерб.

Статья 11 Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года, указывает как направление деятельности по обеспечению информационной безопасности ОВД проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки.

Конечной целью в соответствии со статьей 27 является использование технологии «облачных вычислений» и обеспечение требуемого уровня защиты, катастрофоустойчивости и доступности информации [2].

В соответствии с требованиями приказа МВД России «Об утверждении Правил организации доступа к информационно-телекоммуникационной сети Интернет в органах внутренних дел Российской Федерации» сотрудникам для выполнения служебных задач обеспечивается подключение к сети Интернет [3]. В соответствии с данным приказом безопасность подключения обеспечивается путем использования своевременно обновляемого лицензионного программного обеспечения, а также применения антивирусных средств защиты информации. Данный перечень мер по защите информации нельзя назвать исчерпывающим и следует провести анализ угроз в соответствии со спецификой МВД России.

Как отмечено в [4], если по тем или иным причинам получение доступа к сервисам пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Поэтому важнейшим элементом информационной безопасности является доступность тех или иных сервисов ИТС.

В соответствии с исследованиями известной отечественной компании в области защиты информации Positivetechnologies за 2017 год - на государственные организации были направлены 13% всех атак. С атаками на госсектор часто связывают хакерские группировки (например, OilRig, Turla, Lazarus). В различных исследованиях можно встретить характеристику действий одной и той же группировки, но под разными названиями. В 2017 году их действующих группировок было не менее 70 [6].

Неотъемлемой составляющей обеспечения информационной безопасности в ИТС ОВД является определение вероятных рисков наступления ущерба подобных систем. По определению, данному в рекомендациях ГОСТ ISO 15408 [3], риск – это вероятность реализации угрозы информационной безопасности. В классическом представлении оценка рисков включает оценку угроз, уязвимостей и наносимого ущерба.

Неотъемлемой составляющей обеспечения информационной безопасности в ИТС ОВД является определение вероятных рисков наступления ущерба подобных систем.

По определению, данному в рекомендациях ГОСТ ISO 15408 [3], риск – это вероятность реализации угрозы информационной безопасности. В классическом представлении оценка рисков включает оценку угроз, уязвимостей и наносимого ущерба.

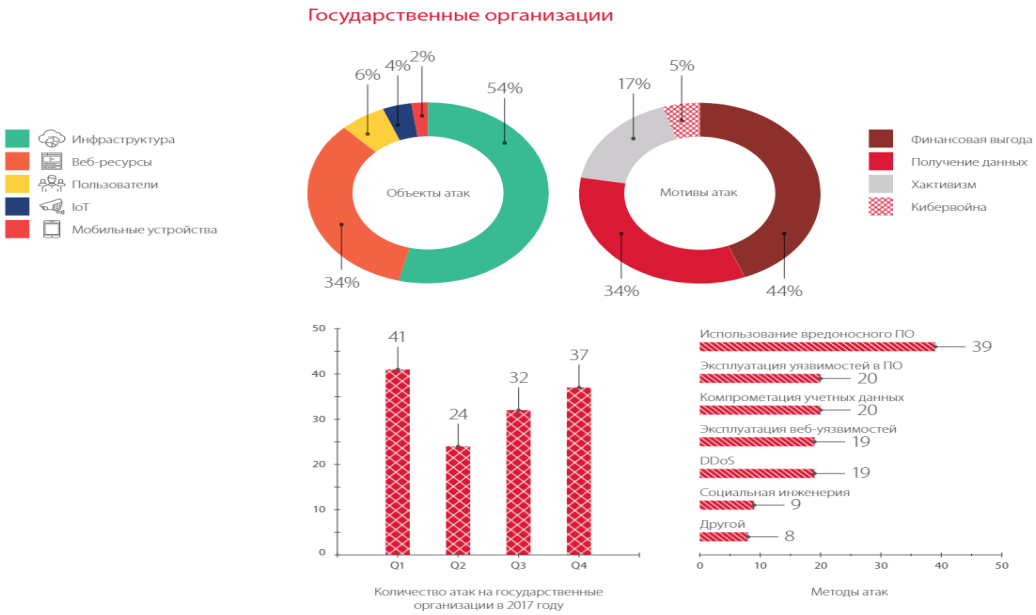

Рис. 1. Статистика по угрозам в государственном секторе
Fig. 1.Statistics on public sector threats

Как видно из рис. 1, угроза «отказ в обслуживании» (DDoS) является одной из наиболее распространенных для государственного сектора.

Анализируя список угроз ФСТЭК России [4] при нарушении доступности применимо к ИТС ОВД, предположим, что основную опасность представляют внешние нарушители со средним потенциалом, поэтому актуальными для рассмотрения являются следующие угрозы: УБИ.140: угроза приведения системы в состояние «отказ в обслуживании»; УБИ.164: угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре.

Так как величина риска является произведением величины ущерба и вероятности наступления данного ущерба, соответственно к явным рискам ИТС ОВД, имеющих подключение к сети Интернет и находящимся под Ddos-атакой, отнесем следующие:

- затрудненное подключение и передача данных, как для внешних, так и для внутренних пользователей;
- полная блокировка подключения и передачи данных;
- переход инфраструктуры ИТС ОВД в аварийное состояние, сопровождающееся продолжительными восстановительными работами.

Метод исследования. С целью разработки рекомендаций по анализу и снижению рисков наступления ущерба в случае реализации угрозы типа «отказ обслуживания» в информационно-технических системах органов внутренних дел рассмотрим структурно-функциональную модель информационно-технической системы органа внутренних дел (СФМ ИТС ОВД), предоставляющую различные сервисы, используемые сотрудниками и работниками в своей повседневной служебной деятельности.

Состав предлагаемой модели включает в себя:

- программный или аппаратный firewall: используется для контроля доступа из сети Интернет, т.к. эксплуатируется ряд сервисов, например, электронная почта, использующие данное подключение;
- сервер-балансировщик: необходим для распознавания приходящих пакетов и маршрутизации обработки запросов;
- веб-сервер: применяется для предоставления доступа к различным сервисам через браузер;
- сервер управления: предоставляет обслуживающему персоналу возможность конфигурирования и обслуживания данного сегмента ИТС ОВД;
- сервер электронной почты: применяется для отправки и получения электронной почты;
- сервер БД: используется для управления массивом, состоящим из основной и нескольких ведомых БД.

Состав и архитектура СФМ ИТС ОВД представлены на рис.2:

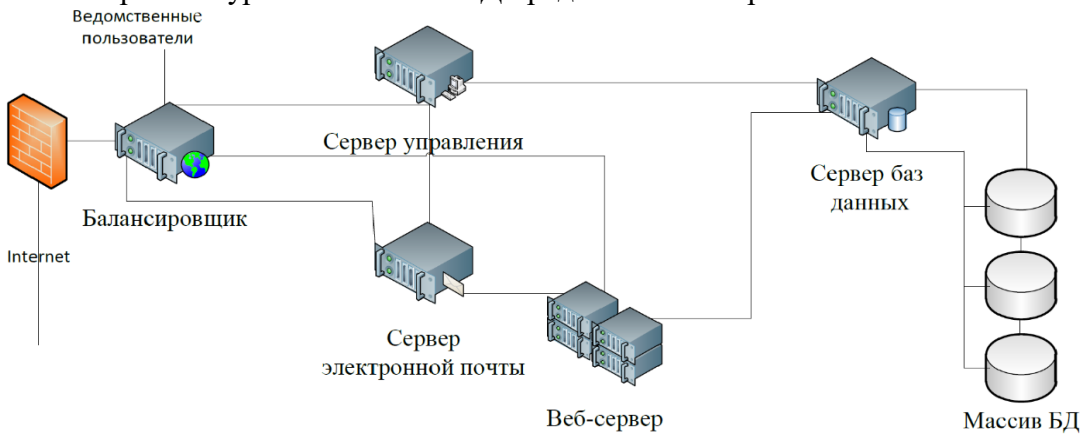

Рис. 2. Состав и архитектура ИТС ОВД
Fig. 2. Composition and architecture of ITS ATS

На рис. 3 представлена структура модели, разработанной в программном продукте AnyLogic. Данная модель отражает процесс DDOS атаки ботнет-сети на сервер.

В левой части представлена ботнет-сеть под управлением задающего узла злоумышленника (perpetrator), направляющего в ботнет-сеть запросы для последующего умножения по вы-

бранному закону распределения и отправке на сетевой адрес сервера жертвы. Преимуществом имитационного моделирования является возможность математической формализации модели с высокой степенью анализируемости протекающих внутри процессов.

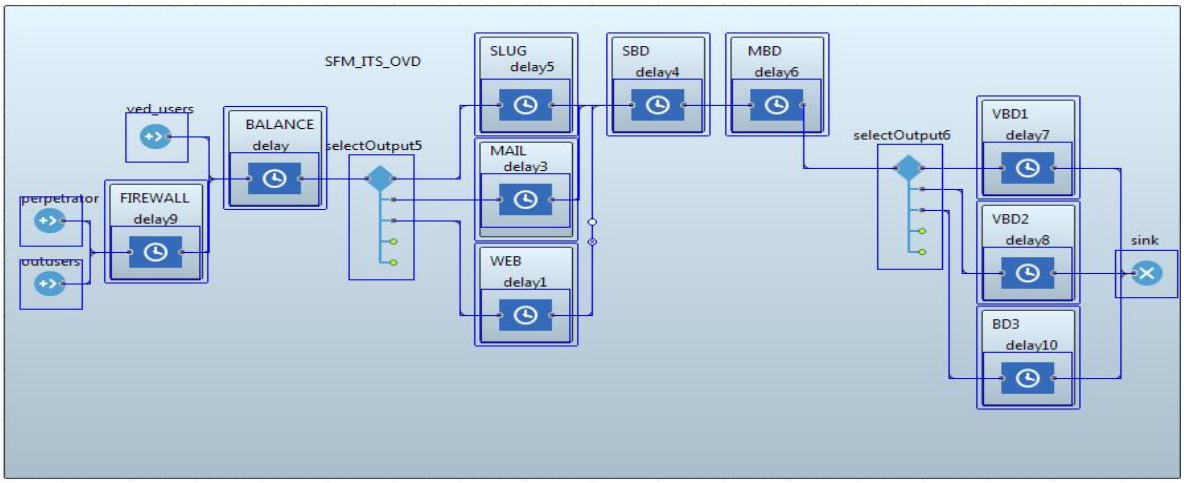

Рис. 3. Структура модели DDOS-атаки ботнет-сети на сервер
Fig. 3. Model structure of the botnet's DDOS attack on the server

Рассматриваемую модель следует определить, как типичную многоканальную систему массового обслуживания с ограниченной очередью и временем ожидания, состоящую из сети устройств, отправляющих пакеты, создаваемые в источнике perpetrator.

Следующими элементами сети является группировка серверов (обслуживающих устройств), являющихся для данного случая жертвами атаки.

Серверы в определенный момент времени могут обслуживать только одну заявку, являющуюся запросом к серверу, и, следовательно, быть в свободном или занятом состоянии. Если сервер занят, то при условии, что в буфере есть свободное место новая заявка (пакет) ставится в очередь и ждёт своего выполнения. Когда обслуживание заявки на сервере завершается, одна из заявок, находящихся в очереди, выбирается для обслуживания. Элементарная теория очередей рассматривает входные потоки, описываемые последовательностью случайных величин – интервалов времени между прибытиями $\{A_1, A_2, \ldots\}$. Наиболее применимым и удобным для расчетов является экспоненциальное распределение интервалов, соответственно, интенсивность входного потока λ в этом случае имеет распределение Пуассона [5,6].

Заметим, в связи с тем, что входные потоки от сети злоумышленника и сети легальных пользователей представлены пуассоновскими потоками, следовательно, возможно применение свойства суперпозиции двух пуассоновских процессов с интенсивностями λ_1 и λ_2. Интенсивность результирующего потока $\lambda = \lambda_1 + \lambda_2$ является также пуассоновским процессом.

Для описания широкого класса ИТС рассмотрим объединенный параметр «производительность сервера», все запросы пользователей полагаются однородными, а для определения последовательности их выполнения используется дисциплина обслуживания FCFS (FirstCome – FirstServed) – обслуживание в порядке поступления [7]. Обычно, эта дисциплина используется по умолчанию, если ничего иного не сказано.

Группировка серверов представлена элементами задержки delay, куда стекаются пакеты с запросами из ботнет-сети и сети легальных пользователей.

Элемент delay позволяет смоделировать процесс обработки запросов сервером, задавая время обработки, которое коррелируется с производительность реального сервера. Элемент delay обладает собственной очередью (буфером), позволяя представить количество мест очереди определенным типом ресурса сервера, например, оперативной памяти. Обслуживание приходящих заявок происходит по нормальному закону распределения [8], причем параметрами нормального распределения являются S_1 –математическое ожидание (оп.), S_2– среднеквадрати-

ческое отклонение (оп.) и Q – производительность сервера (оп./с.). Таким образом, время задержки определенного сервера:

$$\mu(t) = \left(\frac{1}{S_1\sqrt{2\pi}} \cdot \exp(-\frac{(t-S_2)^2}{2S_1{}^2}) \right) / Q \quad (1)$$

Отдельно стоит отметить возможность вытеснения из очереди на обработку пакетов при достижении максимального времени жизни пакета, что соответствует параметру реальных сетевых пакетов в сетях TTL и параметру Timeout при обращении на сайт в веб-браузере [9].

Нагрузка на атакуемый сервер (или интенсивность трафика на сервер):

$$\rho = \lambda / \mu. \quad (2)$$

Среднее число запросов на сервере:

$$\overline{N} = \frac{\rho}{1-\rho}. \quad (3)$$

Среднее время, которое запрос проводит во всей сети массового обслуживания (фактически, следует из теоремы Литтла):

$$\overline{\mathrm{T}} = \frac{\mathrm{N}}{\lambda} = \frac{1}{\mu - \lambda}. \quad (4)$$

В случае атак типа «отказ в обслуживании», усредненный ущерб находим в виде произведения интенсивности атаки (λ) на время наблюдения системы $\overline{u} = \lambda t$, где λ – интенсивность атаки при $\lambda(t) = \lambda \equiv const$..

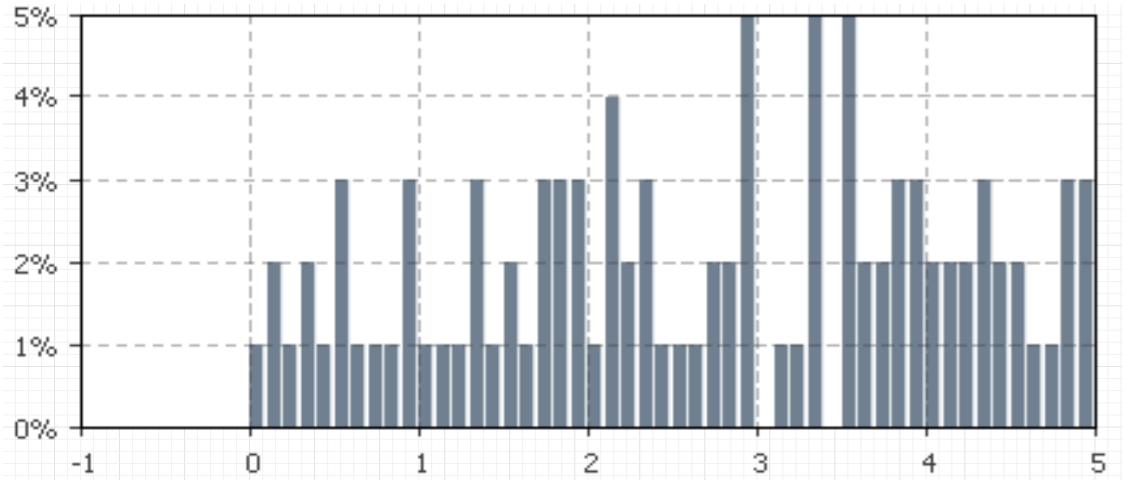

Рис. 4. Гистограмма распределения плотности вероятности обработки запросов в зависимости от времени при заданных значениях интенсивности поступления и обработки запросов

Fig. 4. Histogram of the distribution of the probability density of processing requests as a function of time for given values of the intensity of receipt and processing of requests

Параметр μ - время обработки в среде моделирования, представленный блоком delay, непосредственно зависит от производительности данного сервера (Q). В аспекте атаки «отказ в обслуживании» как правило, выполняемой однотипными сетевыми пакетами.

Результирующая диаграмма времени обработки запроса рис. 4 изображает зависимость нагрузки от времени, т.е. количество пакетов, находящихся на сервере в обработке в рассматриваемый момент времени. Данная диаграмма также отображает среднее значение нагрузки и строит кривую функции распределения.

Таким образом, оценив группировку серверов и направив в сеть исследуемый уровень потока, моделирующего процесс атаки, можно определить вероятность наступления успеха «атаки отказ в обслуживании» и деструктивного воздействия на функционирование сети в результате образования достаточно большой очереди:

$$P_{оч} = \frac{\rho^n}{n!} \cdot \frac{1-\left(\frac{\rho}{n}\right)^m}{1-\frac{\rho}{n}} p_0 \qquad (5)$$

и вероятность отказа вычисляется по следующей формуле:

$$P_{отк} = \frac{\rho^{n+m}}{n^m n!} \cdot p_0 . \qquad (6)$$

Обсуждение результатов. Вычислительный эксперимент, связанный с моделированием и получением статистических данных, характеризующих количество необработанных заявок, скопившихся в очереди, показал следующие результатысзаданными в данном эксперименте параметрами- в случае, если количество необработанных заявок в очереди стремится к 4000 происходит частичная потеря заявок, а при очереди в 8213 процесс моделирования останавливается и мы можем конкретно определить вероятностью наступившего ущерба.

Для измерения величины ущерба в количественных единицах, например, рублях, требуется разработка соответствующей методики.

Вывод. Таким образом, предложена имитационная модель с рядом математических выражений, которую целесообразно использовать при проектировании ИТС ОВД, имеющих подключение к сети Интернет на предмет её устойчивости к деструктивному воздействию типа «отказ в обслуживании». Реализация подобной атаки ведетк снижению оперативности и блокированию выполнения служебных функций сотрудниками ОВД.

Библиографический список:

1. Федеральный закон "О полиции" от 7 февраля 2011 г. N 3-ФЗ.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации».
3. Приказ МВД РФ от 14.03.2012 г. №169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года». Об утверждении Правил организации доступа к информационно-телекоммуникационной сети «Интернет» в органах внутренних дел Российской Федерации».Приказ МВД России от 24.12.2015 № 1228.
4. Зеленский В.А. Проектирование сложных систем. Учебное пособие. — Самара: Самарский государственный аэрокосмический университет, 2012. — 96 с.
5. КабановА.С. Модель оценки риска нарушения информационной безопасности / А.С.Кабанов, А.Б. Лось, В.И. Трунцев// Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. Т. 1. № 25. С. 87-91.
6. https://bdu.fstec.ru/threat.
7. Труб И. И. Объектно-ориентированное моделирование на С++ / И. И. Труб. – СПб.: Питер, 2006. –411 с.
8. Вишневский В. М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. — М.: Техносфера, 2003.— 506 с.
9. Клейнрок Л. Вычислительные системы с очередями / Л. Клейнрок: Пер. с англ. – М.: Мир, 1979. – 600с.
10. Ремезова Е. М. Имитационное моделирование в среде AnyLogic : лаб. практикум / Е. М. Ремезова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. Владимир : Изд-во ВлГУ, 2017. 87 с.
11. Syed R.A. Next generation and advanced network reliability analysis / R.A.Syed – Springer, 2018. – 311 p.
12. Стельмашонок Е.В. Возможности имитационного моделирования для исследования функционирования системы защиты информации / Е.В. Стельмашонок, В.Л. Стельмашонок // Петербургский экономический журнал. — 2017. — №4. — С. 57–68.
13. Алгоритм имитационной модели противодействия несанкционированному доступу к автоматизированной информационной системе специального назначения средствами защиты информации / С.С. Кочедыков [и др.] // Математические методы и информационные технологии управления в науке, образовании и правоохранительной сфере. — 2017. — С. 98–103.
14. Бугров Ю.Г. Повышение качества имитационной модели системы защиты информации / Ю.Г. Бугров, В.В. Мирошников, Д.В. Кочергин // Информация и безопасность. — 2008. — Т. 11. — № 1. — С. 69–73.
15. Рогозин Е.А. Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД / Е.А. Рогозин, А.Д. Попов // Вестник Воронежского института МВД России. — 2016. — № 4. — С. 122–132.

16. Синегубов С.В. Моделирование систем и сетей телекоммуникаций / С.В. Синегубов. — Воронеж: Воронеж. ин-т МВД России, 2016. — 336 с.
17. Моделирование многоуровневых систем защиты информации REDS / А.В. Володько [и др.] // Телекоммуникационные устройства и системы. — 2014. — С. 423–426.
18. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак / С.М. Климов // Известия ЮФУ. Технические науки. — 2016. — № 8 (181). — С. 27–36.

References:

1. Federal'nyy zakon "O politsii" ot 7 fevralya 2011 g. N 3-FZ. [The Federal Law "On Police" of February 7, 2011 N 3-FZ. (In Russ.)]
2. Federal'nyy zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii». [Federal Law “On Information, Information Technologies and Information Protection” (In Russ.)]
3. Prikaz MVD RF ot 14.03.2012 g. №169 «Ob utverzhdenii Kontseptsii obespecheniya informatsionnoy bezopasnosti organov vnutrennikh del Rossiyskoy Federatsii do 2020 goda». Ob utverzhdenii Pravil organizatsii dostupa k informatsionno-telekommunikatsionnoy seti «Internet» v organakh vnutrennikh del Rossiyskoy Federatsii».Prikaz MVD Rossii ot 24.12.2015 № 1228. [Order of the Ministry of Internal Affairs of the Russian Federation of March 14, 2012 No. 169 “On approval of the Concept for ensuring information security of the internal affairs bodies of the Russian Federation until 2020”. On approval of the Rules for organizing access to the information and telecommunication network “Internet” in the internal affairs bodies of the Russian Federation. ”Order of the Ministry of Internal Affairs of Russia of December 24, 2015 No. 1228. (In Russ.)]
4. Zelenskiy V.A. Proyektirovaniye slozhnykh sistem. Uchebnoye posobiye. — Samara: Samarskiy gosudarstvennyy aerokosmicheskiy universitet, 2012. — 96 s. [Zelensky V.A. Designing complex systems. Tutorial. - Samara: Samara State Aerospace University, 2012. - 96 p. (In Russ.)]
5. KabanovA.S. Model' otsenki riska narusheniya informatsionnoy bezopasnosti / A.S.Kabanov, A.B. Los', V.I. Truntsev// Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i ra-dioelektroniki. 2012. T. 1. № 25. S. 87-91. [KabanovA.S. Model for assessing the risk of breach of information security / A.S.Kabanov, A.B. Los, V.I. Truncev // Reports of Tomsk State University of Control Systems and Radio Electronics. 2012. V. 1. Number 25. P. 87-91. (In Russ.)]
6. https://bdu.fstec.ru/threat. (In Russ.)
7. Trub I. I. Ob"yektno-oriyentirovannoye modelirovaniye na S++ / I. I. Trub. – SPb.: Piter, 2006. –411 s. [Trub I. I. Object-Oriented Modeling in C ++ / I. I. Trub. - SPb .: Peter, 2006. –411 p. (In Russ.)]
8. Vishnevskiy V. M. Teoreticheskiye osnovy proyektirovaniya komp'yuternykh setey / V.M. Vish-nevskiy. — M.: Tekhnosfera, 2003.— 506 s [Vishnevsky V. M. Theoretical bases of computer networks design / V.M. Wish Nevsky. - M .: Technosphere, 2003. 506 p. (In Russ.)]
9. Kleynrok L. Vychislitel'nyye sistemy s ocheredyami / L. Kleynrok: Per. s angl. – M.: Mir, 1979. – 600s. [Kleinrock L. Computing systems with queues / L. Kleinrock: Trans. from English - M .: Mir, 1979. - 600s. (In Russ.)]
10. Remezova Ye. M. Imitatsionnoye modelirovaniye v srede AnyLogic : lab. praktikum / Ye. M. Remezova ; Vladim. gos. un-t im. A. G. i N. G. Stoletovykh. Vladimir : Izd-vo VlGU, 2017. 87 s. [Remezova EM. AnyLogic simulation modeling: lab. workshop / E.M. Remezova; We hold. state un-t them. G. G. and N. G. Stoletovs. Vladimir: VlSU Publishing House, 2017. 87 p. (In Russ.)]
11. Syed R.A. Next generation and advanced network reliability analysis / R.A.Syed - Springer, 2018. 311 p.
12. Stel'mashonok Ye.V. Vozmozhnosti imitatsionnogo modelirovaniya dlya issledovaniya funktsioniro-vaniya sistemy zashchity informatsii / Ye.V. Stel'mashonok, V.L. Stel'mashonok // Peterburgskiy ekonomicheskiy zhurnal. — 2017. — №4. — S. 57–68. [Stelmashonok E.V. Possibilities of simulation modeling for the study of the functioning of an information protection system / E.V. Stelmashonok, V.L. Stelmashonok // Petersburg Economic Journal. - 2017. - №4. - pp. 57–68. (In Russ.)]
13. Algoritm imitatsionnoy modeli protivodeystviya nesanktsionirovannomu dostupu k avtomatiziro-vannoy informatsionnoy sisteme spetsial'nogo naznacheniya sredstvami zashchity informatsii / S.S. Kochedykov [i dr.] // Matematicheskiye metody i informatsionnyye tekhnologii upravleniya v nauke, obrazovanii i pravookhranitel'noy sfere. — 2017. — S. 98–103. [Algorithm of a simulation model of countering unauthorized access to a special-purpose automated information system by means of information protection / S.S. Kochedykov [et al.] // Mathematical methods and information technology management in science, education and law enforcement. - 2017. - pp. 98–103. (In Russ.)]
14. Bugrov YU.G. Povysheniye kachestva imitatsionnoy modeli sistemy zashchity informatsii / YU.G. Bug-rov, V.V. Miroshnikov, D.V. Kochergin // Informatsiya i bezopasnost'. — 2008. — T. 11. — № 1. — S. 69–73. [Bugrov Yu.G. Improving the quality of the simulation model of information security systems / Yu.G. Bug-ditch, V.V. Miroshnikov, D.V. Kochergin // Information and Security. - 2008. - V. 11. - № 1. - P. 69–73. (In Russ.)]
15. Rogozin Ye.A. Model' funktsionirovaniya tipovoy sistemy zashchity informatsii ot nesanktsioniro-vannogo dostupa v avtomatizirovannykh informatsionnykh sistemakh OVD / Ye.A. Rogozin, A.D. Popov // Vestnik Voronezhskogo instituta MVD Rossii. — 2016. — № 4. — S. 122–132. [Rogozin E.A. Model of functioning of a typical system of information protection from unauthorized access in automated information systems of ATS / Ye.A.

Rogozin, A.D. Popov // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. - 2016. - № 4. - P. 122–132. (In Russ.)]

16. Sinegubov S.V. Modelirovaniye sistem i setey telekommunikatsiy / S.V. Sinegubov. — Voronezh: Voronezh. in-t MVD Rossii, 2016. — 336 s. [Sinegubov S.V. Simulation of telecommunication systems and networks / S.V. Sinegubov. - Voronezh: Voronezh. Institute of the Ministry of Internal Affairs of Russia, 2016. - 336 p. (In Russ.)]
17. Modelirovaniye mnogourovnevykh sistem zashchity informatsii REDS / A.V. Volod'ko [i dr.] // Tele-kommunikatsionnyye ustroystva i sistemy. — 2014. — S. 423–426. [Modeling of multi-level information security systems REDS / A.V. Volodko [et al.] // Tele-communication devices and systems. - 2014. - p. 423–426. (In Russ.)]
18. Klimov S.M. Imitatsionnyye modeli ispytaniy kriticheski vazhnykh informatsionnykh ob"yektov v usloviyakh komp'yuternykh atak / S.M. Klimov // Izvestiya YUFU. Tekhnicheskiye nauki. — 2016. — № 8 (181). — S. 27–36.[Klimov S.M. Simulation models of testing critical information objects in the conditions of computer attacks / S.M. Klimov // News SFU. Technical science. - 2016. - № 8 (181). - p. 27–36. (In Russ.)]

Сведения об авторах:

Алехин Игорь Викторович – адъюнкт кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России.

Бокова Оксана Игоревна – доктор технических наук, профессор, заместитель начальника Воронежского института МВД России по научной работе.

Коробкин Дмитрий Игоревич – кандидат технических наук, доцент, начальник научно-исследовательского отдела (информационных технологий).

Рогозин Евгений Алексеевич – доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел.

Information about the authors:

Igor V. Alekhin – Adjunct, Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Oksana I. Bokova – Dr.Sci. (Technical), Prof., Deputy Head of the Voronezh Institute of the Ministry of Internal Affairs of Russia for Scientific Work.

Dmitry I. Korobkin – Cand.Sci., Assoc. Prof., Head of the Research Department (Information Technology).

Evgeny A. Rogozin - Dr.Sci. (Technical), Prof., Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Конфликт интересов
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 05.10.2018.
Принята в печать 30.11.2018.

Conflict of interest.
The authors declare no conflict of interest.
Received 05.10.2018.
Accepted for publication 30.11.2018.