МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

DOI: 10.25586/RNU.V9187.19.01.P.003 УДК 519.8

В.А. Минаев, И.Д. Королев, О.В. Петрова, И.О. Овчаренко

МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ МНОГОКАНАЛЬНЫХ АВТОМАТИЗИРОВАННЫХ КОМПЛЕКСОВ ОТ DDoS-АТАК

Рассматривается распространенный вид компьютерных атак – DDoS-атаки на автоматизированные информационные системы (АИС), приводящие к отказу в обслуживании. Целью статьи является оценка вероятности безотказной работы автоматизированной системы. Моделируется система защиты АИС от DDoS-атак, которая обладает основным защищенным каналом передачи информации и двумя запасными. Осуществляется постановка задачи распределения потока заявок в системе многоканального обслуживания с разной пропускной способностью каналов, связанная с ее формальным описанием дифференциальными уравнениями. Рассматривается полное множество гипотез о порядке выбора каналов при поступлении заявок для обработки в системе. Выводятся формулы для расчета предельных вероятностей отказа системы при установившемся режиме обработки поступающих заявок. Находится полная вероятность отказа АИС в обслуживании. Для простых случаев оцениваются параметры потока заявок, когда необходимо подключать запасные защищенные каналы. Делается вывод, что, для того чтобы избежать отказов в обслуживании потока заявок в ходе реализации DDoS-атак на АИС, необходимо адаптивно подстраивать общую пропускную способность каналов автоматизированных комплексов. Кроме того, в случае возникновения сложностей при аналитическом представлении вероятностей отказа возможно построение имитационной модели системы защиты АИС.

Ключевые слова: автоматизированная система, моделирование, система защиты, система массового обслуживания, вероятностная оценка.

V.A. Minaev, I.D. Korolev, O.V. Petrova, I.O. Ovcharenko

PROTECTION SYSTEM MODELLING OF MULTI-CHANNEL AUTOMATED COMPLEXES FROM DDoS-ATTACKS

We consider a common type of computer attacks – DDoS-attacks on automated information systems (AIS), leading to denial of service. The aim of the article is to assess the probability of failure-free operation of an automated system. Simulated protection system AIS from DDoS-attacks, which has a main protected channel for data transmission and two reserved channels. The problem of the flow allocation in the system of multi-channel service with different channel capacity is presented. The problem connected with its formal description by differential equations. The full set of hypotheses about the order of channels selection at receipt of applications for processing in the system is considered. Formulas for calculating the maximum probability of system failure in the steady-state processing of incoming applications are derived. The full probability of failure of the AIS to service the flow of applications is found. Flow parameters are evaluated for simple cases when there is a need to use additional secure channels. It is concluded that in order to avoid failures in the service flow of applications during the implementation of DDoS-attacks on AIS, it is necessary to adapt the overall bandwidth of automated systems. In addition, in case of difficulties in the analytical representation of failure probabilities, it is possible to build a simulation model of the AIS protection system.

Keywords: automated system, modeling, protection system, queuing system, probabilistic evaluation.

Введение

Сегодня одним из распространенных видов компьютерных атак на автоматизированные информационные системы (АИС), приводящих к отказу в обслуживании, являются DDoS-атаки [1; 2; 4; 5; 6; 7; 8; 9]. Поэтому вопросы защиты от них АИС при их взаимодействии с сетями общего доступа представляются весьма перспективными. В данной статье рассматривается новая модель защиты за счет выявления и применения ее синергетических свойств.

Система защиты должна полностью контролировать как внутренние процессы АИС, так и внешние, связанные с передачей данных по каналам связи. Причем речь идет не только об обеспечении защиты канала связи криптографическими средствами, но и об оптимальном управлении каналами для безотказного обслуживания удаленных пользователей [4; 6; 8]. Это позволяет максимально защитить АИС от компьютерных атак типа «отказ в обслуживании» по минимальной стоимости.

Очевидно, что одиночный канал обслуживания при большой интенсивности воздействия злоумышленника на АИС делает ее работу неэффективной [1; 2; 9]. Предположим, что многопроцессорное, многоканальное аппаратное обеспечение АИС как «обслуживающего прибора» полностью справляется с потоками заявок.

Постановка задачи

Рассмотрим систему защиты АИС от DDoS-атак, которая обладает основным защищенным каналом передачи информации и двумя запасными. Применение трех независимых каналов повышает информационную связность АИС с удаленными пользователями, а следовательно, доступность АИС и устойчивость ее функционирования [1; 2]. Оценку надежности функционирования будем вычислять через показатели отказа в обслуживании АИС после осуществления DDoS-атак.

Пусть имеется подсистема защиты АИС, состоящая из внешнего процесса, обеспечивающего информационное взаимодействие с удаленными абонентами, и внутреннего, обеспечивающего безопасную обработку и хранение данных в АИС. Будем считать, что безотказность работы в АИС на ее внутреннем уровне всегда обеспечивается. Основное внимание уделим обеспечению безотказной работы в АИС на уровне внешнего процесса, описываемого в следующем виде:

$$\Pi_{\text{внеш}} = \langle \text{B}, \text{A}_n \rangle; \; n = 1, 2, 3,$$

где B – система распределения заявок по каналам; A_1 – основной канал с пропускной способностью μ_0; A_2, A_3 – резервные каналы с пропускными способностями μ_1 и μ_2 соответственно.

Введем допущение: при включении запасных каналов их иерархия определяется случайным образом, при этом каналы выбираются последовательно в прямом порядке, освобождаясь также поочередно в обратном порядке.

Получение заявок будем рассматривать как простейший поток событий со следующими параметрами:

λ – плотность потока (среднее число событий, приходящееся на единицу времени);

$F(t) = 1 - e^{-\lambda t}$ – закон распределения вероятности появления одного события за время t;

$P_0(t) = 1 - e^{-\lambda t}$ – вероятность того, что за время t не появится ни одной заявки [3; 10].

В каналах происходит обработка поступивших заявок, причем время обработки заявки $m_{i\text{обр}}$ распределено по показательному закону [3; 9; 10]:

$$g(t) = \mu_i e^{\mu_i t},\ i = 0, 1, 2;$$

$$\mu_i = 1/m_{i\text{обр}},\ i = 0, 1, 2.$$

Итак, будем рассматривать систему защиты АИС как трехканальную систему массового обслуживания с отказами, причем обработка запросов на каждом канале происходит с разной интенсивностью μ_i $(i = 0, 1, 2)$. Имеем следующие состояния системы: 0 – свободны все каналы; 1 – занят первый канал; 2 – заняты первые два канала; 3 – заняты все три канала.

Найдем вероятность безотказной работы рассматриваемой системы защиты.

Решение задачи

Определим вероятности состояния системы в каждый из моментов времени t

$$P_0(t),\ P_1(t),\ P_2(t),\ P_3(t) \qquad (1)$$

при условии

$$\sum_{k=0}^{3} P_k(t) = 1.$$

Составим дифференциальные уравнения для состояний системы (1).

1. Зафиксируем момент времени t и найдем вероятность того, что в момент времени $t + \Delta t$ система будет находиться в состоянии 0. Это возможно при:

A – в момент t система находилась в состоянии 0 и за промежуток времени Δt не переходит в другое состояние;

B – в момент t система находилась в состоянии 1 и за промежуток времени Δt переходит в состояние 0.

$$P_0(t) + P_0(t + \Delta t) = P(A) + P(B). \qquad (2)$$

Вероятность события A

$$P(A) = P_0(t)e^{-\lambda \Delta t} \approx P_0(t)(1 - \lambda \Delta t). \qquad (3)$$

Вероятность события B

$$P(B) = P_1(t)\mu_0 \Delta t. \qquad (4)$$

Подставим в формулу вероятности нахождения системы в состоянии 0 значения из формул (3)–(4) [3]:

$$P_0(t + \Delta t) = P_0(t)(1 - \lambda \Delta t) + P_1(t)\mu_0 \Delta t,$$

$$P_0(t + \Delta t) = P_0(t) = -P_0(t)\lambda \Delta t + P_1(t)\mu_0 \Delta t.$$

Разделим обе части на Δt и при $t \to 0$ перейдем к дифференциальному уравнению

$$\frac{\partial P_0(t)}{\partial t} = -P_0(t)\lambda + P_1(t)\mu_0. \qquad (5)$$

2. Далее зафиксируем момент времени t и найдем вероятность того, что в момент времени $t + \Delta t$ система будет находиться в состоянии 1. Это возможно при:

A – в момент t система находилась в состоянии 1 и за промежуток времени Δt не перешла в другое состояние;

B – в момент t система находилась в состоянии 2 и за промежуток времени Δt перешла в состояние 1;

C – в момент t система находилась в состоянии 3 и за промежуток времени Δt перешла в состояние 1.

$$P_1(t+\Delta t) = P(A) + P(B) + P(C); \tag{6}$$

$$P(A) = P_1(t)e^{-(\lambda+\mu_0)\Delta t} \approx P_1(t)(1-(\lambda+\mu_0)\Delta t); \tag{7}$$

$$P(B) = P_2(t)(1-e^{-\mu_1\Delta t}) \approx P_2(t)\mu_1\Delta t; \tag{8}$$

$$P(C) = P_0(t)e^{-\lambda\Delta t} \approx P_0(t)\lambda\Delta t. \tag{9}$$

Подставим в формулу вероятности (6) значения из формул (7)–(9) [3]:

$$P_1(t+\Delta t) = P_1(t)(1-(\lambda+\mu_0)\Delta t) + P_2(t)\mu_1\Delta t + P_0(t)\lambda\Delta t.$$

Переходя к дифференциальному уравнению, получим

$$\begin{gathered} P_1(t+\Delta t) = P_1(t)(1-(\lambda+\mu_0)\Delta t) + P_2(t)\mu_1\Delta t + P_0(t)\lambda\Delta t, \\ \frac{\partial P_1(t)}{\partial t} = -P(t)(\lambda+\mu_0) + P_2(t)\mu_1 + P_0(t)\lambda. \end{gathered} \tag{10}$$

3. Теперь зафиксируем момент времени t и найдем вероятность того, что в момент времени $t + \Delta t$ система будет находиться в состоянии 2. Опуская промежуточные вычисления, получим дифференциальное уравнение

$$\frac{\partial P_2(t)}{\partial t} = -P_2(t)(\lambda+\mu_1) + P_3(t)\mu_2 + P_1(t)\lambda. \tag{11}$$

4. Наконец, по аналогии получим дифференциальное уравнение

$$\frac{\partial P_3(t)}{\partial t} = -P_3(t)\mu_2 + P_2(t)\lambda. \tag{12}$$

Таким образом, получаем систему дифференциальных уравнений (5), (10)–(12) [Там же]:

$$\begin{cases} \dfrac{\partial P_0(t)}{\partial t} = -P_0(t)\lambda + P_1(t)\mu_0, \\ \dfrac{\partial P_1(t)}{\partial t} = -P_1(t)(\lambda+\mu_0) + P_2(t)\mu_1 + P_0(t)\lambda, \\ \dfrac{\partial P_2(t)}{\partial t} = -P_2(t)(\lambda+\mu_1) + P_3(t)\mu_2 + P_1(t)\lambda, \\ \dfrac{\partial P_3(t)}{\partial t} = -P_3(t)\mu_2 + P_2(t)\lambda. \end{cases} \tag{13}$$

Из (13) найдем предельные вероятности состояний системы в установившемся режиме [Там же]:

$$P_0 = \frac{\mu_0\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}; \tag{14}$$

$$P_1 = \frac{\lambda\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}; \tag{15}$$

$$P_2 = \frac{\lambda^2\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}; \tag{16}$$

$$P_3 = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}. \tag{17}$$

Вероятность отказа системы при заданном порядке обработки поступающих заявок определяется по формуле (17).

Рассмотрим полное множество гипотез о порядке выбора каналов при поступлении заявок для обработки:

Γ_1 – пока не занят канал A_1, заявки поступают на него, если он занят, заявки поступают на A_2, если и A_2 занят, то заявки поступают на A_3;

Γ_2 – пока не занят канал A_1, заявки поступают на него, если он занят, заявки поступают на A_3, если и A_3 занят, то заявки поступают на A_2;

Γ_3 – пока не занят канал A_2, заявки поступают на него, если он занят, заявки поступают на A_1, если и A_1 занят, то заявки поступают на A_3;

Γ_4 – пока не занят канал A_2, заявки поступают на него, если он занят, заявки поступают на A_3, если и A_3 занят, то заявки поступают на A_1;

Γ_5 – пока не занят канал A_3, заявки поступают на него, если он занят, заявки поступают на A_1, если и A_1 занят, то заявки поступают на A_2;

Γ_6 – пока не занят канал A_3, заявки поступают на него, если он занят, заявки поступают на A_2, если и A_2 занят, то заявки поступают на A_1.

Так как заявки распределяются по каналам с различными вероятностями появления каждой гипотезы $P(\Gamma_i)$, то по формуле полной вероятности

$$P_{\text{отк}} = \sum_{i=1}^{6} P(\Gamma_i) P_{\text{откГ}_i}, \tag{18}$$

где $P_{\text{откГ}i}$ – вероятность отказа системы при принятии i-й гипотезы.

$P_{\text{откГ}i}$ рассчитаем, используя формулу (17) и учитывая порядок нумерации каналов:

$$P_{\text{откГ}_1} = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}; \tag{19}$$

$$P_{\text{откГ}_2} = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}; \tag{20}$$

$$P_{\text{откГ}_3} = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_0\mu_2 + \lambda^2\mu_2 + \lambda^3}; \tag{21}$$

$$P_{\text{откГ}_4} = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_0\mu_2 + \lambda^2\mu_0 + \lambda^3}; \tag{22}$$

$$P_{\text{откГ}_5} = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_0 + \lambda^2\mu_1 + \lambda^3}; \tag{23}$$

$$P_{\text{откГ}_6} = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_0 + \lambda^2\mu_0 + \lambda^3}. \tag{24}$$

Подставив формулы (19)–(24) в формулу нахождения полной вероятности отказа системы (18), получим

$$P_{\text{отк}} = \lambda^3 \frac{P(\Gamma_1)}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3} + \frac{P(\Gamma_2)}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_0 + \lambda^3} +$$
$$+ \frac{P(\Gamma_3)}{\mu_0\mu_1\mu_2 + \lambda\mu_0\mu_2 + \lambda^2\mu_2 + \lambda^3} + \frac{P(\Gamma_4)}{\mu_0\mu_1\mu_2 + \lambda\mu_0\mu_2 + \lambda^2\mu_0 + \lambda^3} +$$
$$+ \frac{P(\Gamma_5)}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_0 + \lambda^2\mu_0 + \lambda^3} + \frac{P(\Gamma_6)}{\mu_0\mu_1\mu_2 + \lambda\mu_0\mu_1 + \lambda^2\mu_1 + \lambda^3}. \tag{25}$$

Покажем для простых случаев, как оценивать параметры потока заявок, когда необходимо подключать запасные защищенные каналы [1; 2]. Для этого рассмотрим вначале работу только основного канала [4; 8], т.е. одноканальную систему массового обслуживания с отказами. В этом случае вероятность отказа рассчитывается по формуле

$$P_{\text{отк}} = \frac{\frac{\lambda}{\mu_1}}{1+\frac{\lambda}{\mu_1}} = \frac{\lambda}{\mu_1+\lambda}. \tag{26}$$

Для АИС допустимой вероятностью отказа является значение, не превышающее 0,05 [6; 7]. Найдем максимальное допустимое значение λ, при котором обеспечивается безотказная работа основного канала:

$$P_{\text{отк}} \le 0,05,\ \frac{\lambda}{\mu_1+\lambda} \le 0,05,\ \lambda \le \frac{\mu_1}{19}. \tag{27}$$

Таким образом, при значениях потока заявок, превышающих условие (27), система защиты не может обеспечить безотказную работу АИС и необходимо подключать запасной канал A_2 [5; 7].

Найдем вероятность отказа данной системы при включении запасного канала A_2. Для этого рассмотрим двухканальную систему массового обслуживания с отказами. Введем состояния: 0 – свободны все каналы; 1 – занят первый канал; 2 – заняты два канала.

Исходя из предыдущих рассуждений, найдем вероятность отказа данной системы:

$$\begin{cases} 0 = -P_0\lambda + P_1\mu_0, \\ 0 = -P_0(\lambda+\mu_0) + P_2\mu_1 + P_0\lambda, \\ 0 = -P_2\mu_1 + P_1\lambda, \\ \sum_{k=0}^{2} P_k = 1. \end{cases} \tag{28}$$

$$P_1 = \frac{P_0\lambda}{\mu_0}; \tag{29}$$

$$P_2 = \frac{P_0\lambda^2}{\mu_0\mu_1}; \tag{30}$$

$$P_0 = \frac{\mu_0\mu_1}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2}. \tag{31}$$

Подставим значение из (31) в уравнения (29)–(30):

$$P_1 = \frac{\lambda\mu_1}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2},\ P_2 = \frac{\lambda^2}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2}. \tag{32}$$

Найдем максимальное допустимое значение потока заявок, при котором обеспечивается безотказная работа основного и одного запасного каналов:

$$P_{\text{отк}} \le 0,05,\ \frac{\lambda^2}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2} \le 0,05,\ 38\lambda^2 - \lambda\mu_1 - \mu_1\mu_0 \le 0. \tag{33}$$

Находя и исследуя корни (33), определяем

$$\lambda \le \frac{\mu_1}{38}\left(1+\sqrt{1+76\frac{\mu_0}{\mu_1}}\right). \qquad (34)$$

Таким образом, при значениях параметров потока, не удовлетворяющих условию (34), система защиты не может обеспечить безотказную работу АИС и необходимо подключать второй запасной канал обработки информации A_3.

Выводы

1. Для того чтобы в ходе реализации DDoS-атак на АИС избежать отказа в обслуживании потока заявок, необходимо заблаговременно реагировать на изменения последнего, адаптивно подстраивая общую пропускную способность каналов автоматизированных комплексов в соответствии, например, с (19)–(25) при трехканальной системе.

2. Подобным же образом возможно производить расчеты при большем числе каналов. В случае возникновения сложностей при аналитическом представлении вероятностей отказа возможно построение имитационной модели системы защиты АИС [11; 12].

3. Для предварительных расчетов ограничений потоков применительно к простым системам массового автоматизированного обслуживания целесообразно использовать соотношения (27) и (34).

Литература

1. *Боговик А.В., Игнатов В.В.* Теория управления в системах военного назначения: учебник. СПб.: ВАС, 2008. 460 с.
2. *Боговик А.В., Игнатов В.В.* Эффективность систем военной связи и методы ее оценки : монография. СПб.: ВАС, 2006. 183 с.
3. *Вентцель Е.С.* Теория вероятностей: учебник. 11-е изд., стер. М.: КноРус, 2010. 664 с.
4. *Королев И.Д., Петрова О.В.* Разработка модели защиты информации, обрабатываемой в вычислительных сетях, от компьютерных атак // Известия вузов. Северо-Кавказский регион. Технические науки. 2006. № 1. С. 68–73.
5. *Королев И.Д., Петрова О.В., Исупов А.Б., Юрков В.А.* Моделирование процесса функционирования телекоммуникационной сети в условиях программно-аппаратных воздействий // Научный журнал КубГАУ. 2012. № 81(07). С. 2–12.
6. *Королев И.Д., Петрова О.В., Малышев Д.В., Пугин К.В., Шайков И.Н.* Модель защищенности комплекса средств автоматизации специального назначения // Телекоммуникации. 2016. № 9. С. 41–44.
7. *Королев И.Д., Петрова О.В., Пугин К.В., Мухортов В.В., Солодовников А.С.* Определение параметров защищенности АСУ, работающей в условиях информационного противоборства: свидетельство о государственной регистрации программы для ЭВМ № 2016611851 Российская Федерация. Зарегистрировано в реестре программ для ЭВМ 11.02.2016.
8. *Королев И.Д., Петрова О.В., Сураев А.С.* Разработка модели защиты информации, обрабатываемой в вычислительных сетях, от компьютерных атак: сб. тр. Краснодар: ФВАС, 2011. С. 34–40.
9. *Коценяк М.А., Кулешов И.А., Лаута О.С.* Устойчивость информационно-телекоммуникационных сетей: монография. СПб.: Изд-во Политехнического университета, 2013. 93 с.
10. *Матвеев В.Ф., Ушаков В.Г.* Системы массового обслуживания: учеб. пособие. М.: Изд-во МГУ, 1984. 242 с.

11. *Фисун А.П., Касилов А.Г., Фисенко В.Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р.А., Джевага К.А., Кожухов С.А.* Развитие методологических основ информатики и информационной безопасности систем. М., 2004. 253 с. Деп. в ВИНИТИ 07.07.2004, № 1165-В2004.
12. *Чекалин А.А., Скрыль С.В., Минаев В.А.* Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: учеб. пособие для высших учебных заведений МВД России. Ч. 2: Практические аспекты технической разведки и комплексного технического контроля. М.: Научно-техническое издательство «Горячая линия-Телеком», 2006. 205 с.

Literatura

1. *Bogovik A.V., Ignatov V.V.* Teoriya upravleniya v sistemakh voennogo naznacheniya: uchebnik. SPb.: VAS, 2008. 460 s.
2. *Bogovik A.V., Ignatov V.V.* Effektivnost' sistem voennoy svyazi i metody ee otsenki : monografiya. SPb.: VAS, 2006. 183 s.
3. *Venttsel' E.S.* Teoriya veroyatnostey: uchebnik. 11-e izd., ster. M.: KnoRus, 2010. 664 s.
4. *Korolev I.D., Petrova O.V.* Razrabotka modeli zashchity informatsii, obrabatyvaemoy v vychislitel'nykh setyakh, ot komp'yuternykh atak // Izvestiya vuzov. Severo-Kavkazskiy region. Tekhnicheskie nauki. 2006. № 1. S. 68–73.
5. *Korolev I.D., Petrova O.V., Isupov A.B., Yurkov V.A.* Modelirovanie protsessa funktsionirovaniya telekommunikatsionnoy seti v usloviyakh programmno-apparatnykh vozdeystviy // Nauchnyy zhurnal KubGAU. 2012. № 81(07). S. 2–12.
6. *Korolev I.D., Petrova O.V., Malyshev D.V., Pugin K.V., Shaykov I.N.* Model' zashchishchennosti kompleksa sredstv avtomatizatsii spetsial'nogo naznacheniya // Telekommunikatsii. 2016. № 9. S. 41–44.
7. *Korolev I.D., Petrova O.V., Pugin K.V., Mukhortov V.V., Solodovnikov A.S.* Opredelenie parametrov zashchishchennosti ASU, rabotayushchey v usloviyakh informatsionnogo protivoborstva: svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2016611851 Rossiyskaya Federatsiya. Zaregistrirovano v reestre programm dlya EVM 11.02.2016.
8. *Korolev I.D., Petrova O.V., Suraev A.S.* Razrabotka modeli zashchity informatsii, obrabatyvaemoy v vychislitel'nykh setyakh, ot komp'yuternykh atak: sb. tr. Krasnodar: FVAS, 2011. S. 34–40.
9. *Kotsenyak M.A., Kuleshov I.A., Lauta O.S.* Ustoychivost' informatsionno-telekommunikatsionnykh setey: monografiya. SPb.: Izd-vo Politekhnicheskogo universiteta, 2013. 93 s.
10. *Matveev V.F., Ushakov V.G.* Sistemy massovogo obsluzhivaniya: ucheb. posobie. M.: Izd-vo MGU, 1984. 242 s.
11. *Fisun A.P., Kasilov A.G., Fisenko V.E., Minaev V.A., Afanas'ev V.V., Mityaev V.V., Fisun R.A., Dzhevaga K.A., Kozhukhov S.A.* Razvitie metodologicheskikh osnov informatiki i informatsionnoy bezopasnosti sistem. M., 2004. 253 s. Dep. v VINITI 07.07.2004, № 1165-V2004.
12. *Chekalin A.A., Skryl' S.V., Minaev V.A.* Kompleksnyy tekhnicheskiy kontrol' effektivnosti mer bezopasnosti sistem upravleniya v organakh vnutrennikh del: ucheb. posobie dlya vysshikh uchebnykh zavedeniy MVD Rossii. Ch. 2: Prakticheskie aspekty tekhnicheskoy razvedki i kompleksnogo tekhnicheskogo kontrolya. M.: Nauchno-tekhnicheskoe izdatel'stvo "Goryachaya liniya-Telekom", 2006. 205 s.