УДК 004.056:007 (045)

**Данилина Г.В.**
Криворожский колледж Национального авиационного университета

# УРОВНИ ВЗАИМОДЕЙСТВИЯ И КОНФЛИКТНОГО УПРАВЛЕНИЯ В ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ С ПСЕВДОСЕРВИСАМИ

**Danylina H.V. The levels of interaction and conflict control in protected information systems with pseudo-services.** A mathematical model and method of multi-level protection of network in the conditions of a priori uncertainty of network state and the threats with an active (reasonable) partner is developed. On the basis of theory of the guided Markov processes the method of conflict control with predication of evolution of situation, step-by-step of parameters and state identification and correction results the current analysis is modified. It is shed light on the use of methods of conflict process control of protection of networks it is possible to achieve for winning, even if an enemy has superiority in resources. It is achieved the decision of this task by the reflection control – accounting of strong and weak sides of enemy, purposeful exhaustion of his resources while attacking on false objects and pseudo services ("Honey pots").

***Keywords***: information system, multi-level protection of network, active partner, reasonable partner, conflict control, reflection control , pseudo service, honey pot, escalation pit

**Даниліна Г.В. Рівні взаємодії та конфліктного управління у захищених інформаційних системах із псевдосервісами.** Розроблено математичну модель і методику багаторівневого захисту мережі в умовах апріорної невизначеності стану мережі і загроз з боку активного (розумного) партнера. Модифікований метод конфліктного управління з прогнозуванням розвитку ситуації. Запропонований спосіб захисту мереж на основі рефлексивного управління – урахування сильних і слабких сторін противника, цілеспрямованого виснаження його ресурсів в атаках на помилкові об'єкти і псевдосервіси ("медові пастки").

***Ключові слова***: інформаційна система, багаторівневий захист мережі, активний партнер, розумний партнер, конфліктне управління, рефлексивне управління, псевдосервіс, медова пастка, ескалаційна яма

**Данилина Г.В. Уровни взаимодействия и конфликтного управления в защищенных информационных системах с псевдосервисами.** Разработана математическая модель и методика многоуровневой защиты сети в условиях априорной неопределенности состояния сети и угроз со стороны активного (разумного) партнера. Модифицирован метод конфликтного управления с прогнозированием развития ситуации. пошаговой идентификации параметров и состояния и коррекции по результатам текущего анализа. Предложен способ защиты сетей на основе рефлексивного управления – учета сильных и слабых сторон противника, целенаправленного истощения его ресурсов в атаках на ложные объекты и псевдосервисы ("медовые ловушки").

***Ключевые слова***: информационная система, многоуровневая защита сети, активный партнер, разумный партнер, конфликтное управление, рефлексивное управление, псевдосервис, медовая ловушка, эскалационная яма

## 1. Введение. Постановка задачи

В настоящее время наблюдается большой интерес к методам анализа и оптимизации систем защиты компьютерных и объединенных сетей от атак и несанкционированных вторжений. Однако работы по конкретному применению методов противодействия, конфликтному управлению процессами активной защиты сетей, статистическому оцениванию потенциальной эффективности и асимптотическим характеристикам систем защиты практически отсутствуют.

В данной работе сделана попытка наметить пути решения упомянутых проблем и разработать методический инструментарий применения методов теории конфликта и прикладного конфликтного управления – затягивания противника в "эскалационную яму" путем применения так называемых "медовых ловушек" – псевдосервисов с явно демонстрируемыми уязвимостями.

Судя по результатам анализа многочисленных статей, монографий, материалов научных и практических конференций, задача защиты информационных ресурсов компьютерных сетей от атак со стороны внешних и внутренних нарушителей никогда не потеряет свою актуальность. Для решения данной задачи уже недостаточно обнаруживать и реагировать на действия нарушителей. Необходимо не только прогнозировать такие действия, исключать уязвимости в системах сетевой защиты, но и отвлекать злоумышленников от сетевых узлов, в которых осуществляется хранение и обработка информационных ресурсов.

Еще примерно десятилетие назад возникло понимание того, что прямое противоборство с вредоносными сетевыми воздействиями практически бесполезно. Был сделан вполне логичный вывод о необходимости применения методов, взятых из арсенала системного анализа, исследования операций в военном деле и, наконец, радиоэлектронной борьбы – радиоэлектронной и радиоразведки, радиоэлектронного противодействия, дезинформации и пр. [1].

Для борьбы с троянскими программами наибольший интерес привлек метод так называемой "медовой ловушки" [2] – заманивания на ложные информационные объекты, обладающие высокой уязвимостью. В работе [3] такие медовые ловушки названы псевдосервисами. Целые коллективы работали над разнообразными проектами медовых ловушек [4, 5].

Типичными примерами применения методов активного противодействия угрозам могут служить инструменты *BackOfficer Friendly* как альтернатива *Back Orifice*, *Advanced Port Scanner Honeypot*, *Specter*, *KFSensor*, *Honeyd*, *ManTrap* и др. [1]. Каждое из этих решений представляет собой Honeypot определенного вида: слабого, среднего или сильного взаимодействия. Некоторые из данных решений являются бесплатными (*Open Source*). Часть из данных *Honeypot* может быть запущена на платформе *Unix*, тогда как другая часть – на *Windows* [2].

Рассмотрим одну из простейших, но достаточно эффективных медовых ловушек *BackOfficer Friendly* (*BOF*).

*BackOfficer Friendly* – это серверное приложение подмены, который работает в системе *Windows* или *UNIX* и уведомляет, когда кто-то пытается получить удаленный контроль над системой, например, с помощью инструмента *Back Orifice* (*BO*). В основном, эта программа симулирует сервер *BO*. *BOF* дает злоумышленнику ложные ответы, которые, как представляется, пришли из приложения *BO*. Все это время *BOF* регистрирует *IP*-адрес злоумышленника и все операции, которые хакер пытается выполнить. Он содержит подпрограммы, которые позволяют ему выборочно имитировать множество других услуг. Например, когда кто-то запускает автоматическое сканирование, *BOF* генерирует строку предупреждений о попытках сканирования.

В результате поиска и анализа многочисленных литературных источников нами были обнаружены лишь две статьи, заслуживающие внимания [6, 7]. В частности, в работе [7] глубоко и всесторонне проработан теоретический подход к оцениванию эффективности медовых ловушек (по терминологии статьи – ложных информационных систем).

Средства *Honeypot* имеют несколько недостатков, из-за которых они не заменяют механизмов безопасности, а только расширяют общую архитектуру безопасности.

Главными проблемами средств *Honeypot* являются [2, 3]:

- ограниченная область обнаружения атак;
- возможность раскрытия *Honeypot* злоумышленником;
- риск взлома *Honeypot* и атаки узлов посторонних организаций.

В доступных нам источниках не рассмотрены вопросы анализа возможной реакции противника при обнаружении им медовых ловушек. Также не рассмотрены методы

исключения или хотя бы минимизации событий обнаружения. Эти вопросы также нуждаются в дополнительном анализе.

**2. Цель и задачи исследования**

С учетом вышеизложенного в данной работе поставлена цель – разработать метод управления процессом активной защиты информационной системы на основе теории конфликта [8] и управляемых марковских процессов [9].

Конфликт не может рассматриваться как оптимизационная задача [3]. Он также не может быть разрешен и в рамках теории адаптации. Своими активными действиями противник с вероятностью, стремящейся к единице, достигнет максимального выигрыша. Поэтому основными задачами, которые необходимо решить для достижения поставленной цели, являются:

- анализ возможных стратегий конфликта и выбор наиболее перспективных стратегий для данной задачи;
- выбор математического аппарата для описания процессов развития конфликта;
- разработка математической модели конфликта для получения асимптотических характеристик эффективности.

**3. Разработка модели конфликта и анализ стратегий атак и защиты**

В соответствии с общей теорией конфликта [8] процессы противоборства между атакующей и защищающейся сторонами описываются дифференциально-разностными уравнениями или уравнениями с отклоняющимися аргументами [10]. Это допущение вполне справедливо для дискретных систем с запаздыванием, каковыми являются компьютерные сети и распределенные информационные системы.

В самом общем случае

$$\begin{cases} z'_{ids}(t) = f_1\left(t, z_{ids}(t), \ldots, z_{ids}(t-\tau_1), u_1(t), v_2(t-\tau_2), \xi(t)\right); \\ z'_{icm}(t) = f_2\left(t, z_{icm}(t), \ldots, z_{icm}(t-\tau_2), u_2(t-\tau_2), v_1(t), \eta(t)\right), \end{cases} \quad (1)$$

где $z_{ids}$ и $z_{icm}$ – векторы состояния систем $S_{ids}$ и $S_{icm}$ соответственно;

$u_1(t)$ и $u_2(t)$ – векторы управлений в $S_{ids}$ и $S_{icm}$ соответственно;

$v_1(t)$ – вектор воздействий $S_{ids}$ на $S_{icm}$;

$v_2(t)$ – вектор воздействий $S_{icm}$ на $S_{ids}$;

$\xi(t)$ и $\eta(t)$ – векторы случайных возмущений, действующих на $S_{ids}$ и $S_{icm}$ соответственно;

$\tau_1$ и $\tau_2$ – запаздывания в $S_{ids}$ и $S_{icm}$ соответственно.

Эффективность $Э_1$ системы $S_{ids}$ и эффективность $Э_2$ системы $S_{icm}$ на интервале наблюдения $T$ в общем случае представляют собой нелинейные функционалы состояний $z_{ids}$, $z_{icm}$ и векторов $\xi(t)$, $\eta(t)$ соответственно. Как следует из (1), они взаимозависимы.

Если учесть фактор нормализации случайных процессов в больших системах [2], то можно применить для решения уравнений (1) метод Гауссовской аппроксимации в малой окрестности точек экстремума $Э_1$ и $Э_2$. В этом случае выражения для эффективностей имеют вид

$$Э_1 = \int_0^T z_{ids}(t)\,dt, \quad Э_1 \to \max_{v_1}, \qquad Э_2 = \int_0^T z_{icm}(t)\,dt, \quad Э_2 \to \max_{v_2}. \quad (2)$$

Цель каждой системы – максимально повысить свою эффективность за счет снижения эффективности противной стороны. Однако результат приложенных усилий станет известен только в момент времени $T$. На интервале наблюдения $0 \le t \le T$ можно вырабатывать наилучшие управления $u_1(t)$, воздействия $v_1(t)$ и прогнозировать конечный результат, только опираясь на предположения о стратегии поведении противника и данные о текущем

состоянии $z_{ids}$ и $z_{icm}$. Включение в уравнения (1) функций $v_1(t)$ означает отвлечение части ресурса на формирование защитных или контратакующих воздействий. Следовательно, необходимо решать задачу конфликта или с дополнительным критерием минимизации доли ресурса, отводимой на защиту, или с ограничением на допустимый расход этой доли ресурса.

Рассмотрим особенности работы *Honeypot*-ловушки на уровнях предотвращения (уровень маршрутизатора и межсетевого экрана), обнаружения (демилитаризованная зона) и ответа (интрасеть).

Математическая модель конфликта между атакующей и защищающейся сторонами, модифицированная для случая применения стратегий эскалации в псевдосервисы, стратегии противодействия и атак, разработанные в соответствии с классической теорией конфликта [8] и модифицированные для конкретной рассматриваемой задачи, приведены в [3]. Здесь же рассмотрим набор наиболее наглядных стратегий защиты:

- эшелонирование рубежей защиты типа “внешняя – демилитаризованная – внутренняя зоны безопасности”;
- отказ от получения – простой возврат подозрительного трафика;
- распределенный отказ от получения – трансляция подозрительного трафика на несколько точек и возврат источнику со всех этих точек;
- насыщение рубежей защиты псевдосервисами с воспроизведением хорошо известных уязвимостей – затягивание противника в эскалационную ловушку.

## 4. Статистическая динамика процесса развития конфликта с эскалацией в псевдосервисы

Процесс развития конфликта представляет собой полумарковский процесс типа альтернирующего процесса восстановления, переходные и финальные вероятности которого зависят от соотношения стратегических $(S_{ids}, S_{icm})$ и энергоинформационных $(E_{ids}, E_{icm})$ ресурсов сторон. Текущее состояние процесса можно записать в виде некоторого функционала $\delta R = \Psi\left[\varphi(S_{ids}, E_{ids}), \varphi(S_{icm}, E_{icm})\right]$, которым характеризуется интегральный выигрыш от применения той или иной стратегии с учетом интенсивности её применения. Собственно стратегия оценивается по своей информационной ценности, а интенсивность – по энергетическому ресурсу (например, по числу точек, с которых проводится распределенная атака). В качестве первого приближения для выбора вида функционала можно взять аддитивную меру множества стратегий, а относительное влияние конкретной стратегии учесть весовыми коэффициентами или функциями.

Рассмотрим математическую модель конфликта между распределенными системами атаки и защиты. Алгоритмическая схема процесса моделирования атакующих и контратакующих потоков изображена на рис. 1.

Имеют место последовательности атакующих действий и ответных защитных мер (пассивных, активных или и тех, и других). Предположим, что в результате атаки вероятность штатного функционирования объекта снижается, возможно, до нуля, а в результате применения ответной защитной меры вероятность функционирования объекта повышается, возможно, вплоть до исходной величины. Таким образом, в каждый момент времени система может находиться в одном из $N$ возможных фазовых состояний $\phi_1, \phi_2, \ldots, \phi_N$, характеризующих текущую вероятность функционирования объекта. Известны начальное состояние системы (в начальный момент времени $t_0$ она находится в состоянии $\psi_0 = \phi_i$) и одношаговые вероятности перехода $\rho_{ik} = P\{\psi_l = \phi_k \,|\psi_{l-1} = \phi_i\}$, $i,k = \overline{1,N}$.

Следовательно, если игнорировать случайный характер времени ожидания и интересоваться только моментами перехода, то процесс $\psi_l = \psi(t_l)$ есть вложенная однородная цепь Маркова [3]. Вероятность перехода $\rho_{ik}$ полностью определяется $i$-м состоянием объекта и результатами $k$-го атакующего воздействия.

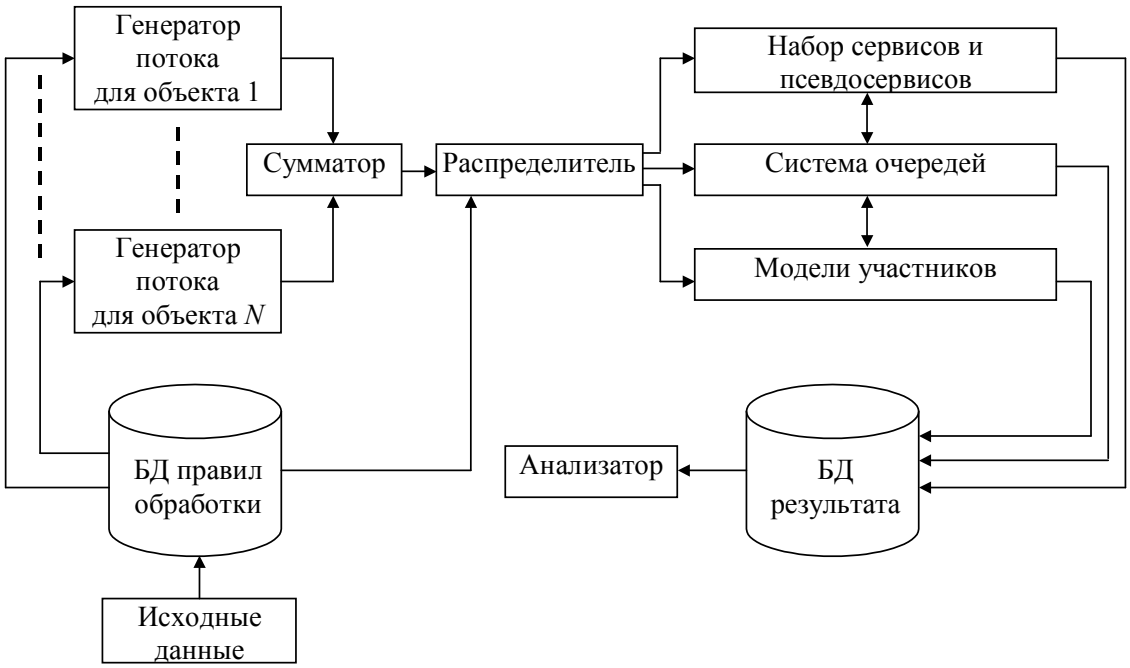


Рис. 1. Алгоритмическая модель

Запаздывания $\tau_1$ и $\tau_2$ в системах $S_{ids}$ и $S_{icm}$ представляют собой дискретные процессы $z_{ids}(\tau_1)$, $z_{icm}(\tau_2)$, которые не обязательно являются марковскими. Однако это не критично для последующего анализа, поскольку сами величины $\rho_{mn}$, $m,n \in M$, дают исчерпывающую информацию об эволюции конфликта.

Сопоставим каждому ненулевому элементу $\rho_{ik}$ матрицы вероятностей перехода случайную величину $\zeta_{ik}$ с функцией распределения $F_{ik}(t) = F_{ik}(\tau_{ik} \le t)$. В рассматриваемой задаче случайную величину $\zeta_{ik}$ будем трактовать как время пребывания атакуемого объекта в состоянии $\phi_i$ при условии, что следующим состоянием, в которое перейдет объект, будет $\phi_k$. При этом величина $\zeta_{ik}$ считается неотрицательной и непрерывной с плотностью вероятности $w_{ik}(t)$. При такой интерпретации величину $\zeta_{ik}$ можно назвать временем нахождения объекта в состоянии $\phi_i$ до перехода в состояние $\phi_k$.

Допустим, что точка, отображающая поведение системы в пространстве состояний, останется в состоянии $\phi_i$ в течение времени $\zeta_{ij}$, прежде чем она перейдет в $\phi_j$ (см. рис. 2 и 3). По достижении состояния $\phi_j$ “мгновенно” (в соответствии с матрицей вероятностей перехода $\{\rho_{ik}\}$) выбирается следующее состояние $\phi_n$, $n = \overline{1,N}$. Здесь “мгновенность” трактуется в том смысле, что длительность перехода является величиной второго порядка малости по сравнению с минимальной длительностью нахождения в текущем состоянии.

Если для точки, отображающей поведение системы и находящейся в $l$-м состоянии, с вероятностью перехода $\rho_{ll}$ вновь выбирается состояние $l$, горизонтальная часть траектории движения точки обозначается линией со стрелкой на конце, как это изображено на графиках, см. рис. 2 и 3. Выражение $x \succ y$ означает доминирование $x$ над $y$.

После того, как следующее состояние $\phi_i$ выбрано, время ожидания в текущем состоянии $\phi_k$ полагается равным $\zeta_{ki}$ с функцией распределения $F_{ki}(t)$ или,

соответственно, с плотностью вероятности $w_{ki}(t)$. Этот процесс в дальнейшем неограниченно продолжается. Каждый раз независимо выбираются следующее состояние и время ожидания. Если через $\psi(t)$ обозначить состояние системы, в котором она находится в момент времени $t$, то полученный случайный процесс является полумарковским. При заданном начальном состоянии дальнейшее поведение процесса полностью определяется матрицей вероятностей перехода $\{\rho_{ik}\}$, $i,k=\overline{1,N}$, и матрицей функций распределения $\{F_{ki}(t)\}$.

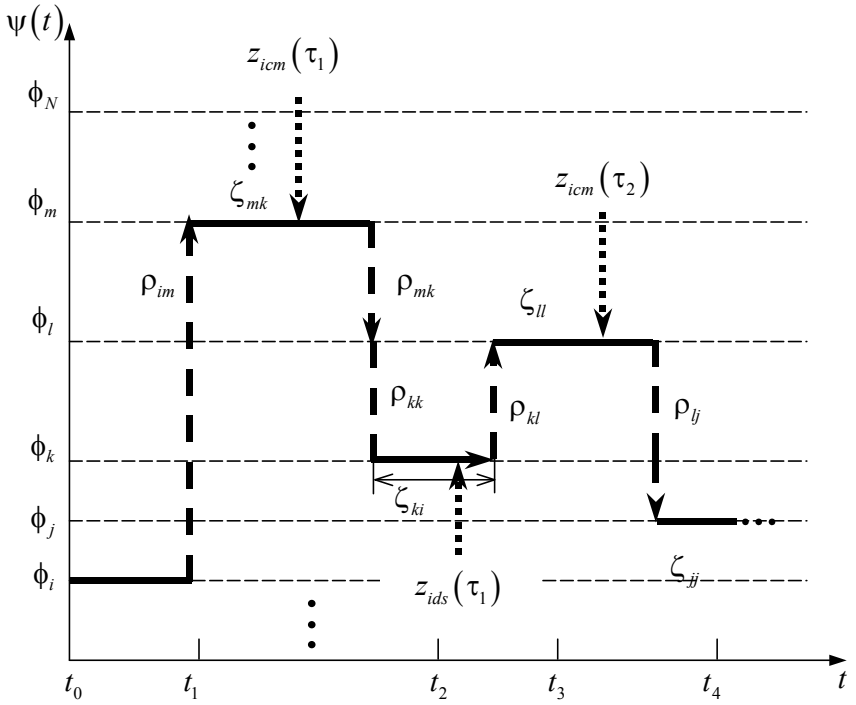


Рис. 2. Изменение вероятностей функционирования объекта с системой защиты.
$z_{icm}(\tau_n) \succ z_{ids}(\tau_n)$

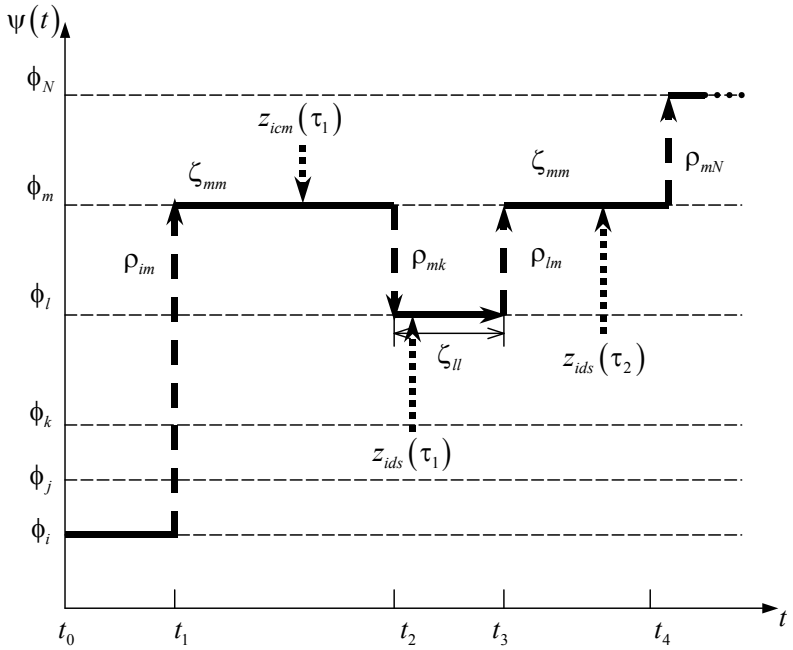


Рис. 3. Изменение вероятностей функционирования объекта с системой защиты.
$z_{ids}(\tau_n) \succ z_{icm}(\tau_n)$

**5. Выводы**

В заключение еще раз необходимо подчеркнуть, что силовое противодействие атакам и вторжениям в компьютерные сети требует отвлечения больших ресурсов и завершается успехом только в редких случаях, например, для случая "распределенная атака – распределенная защита". В то же время разработанная в рамках общей теории конфликта стратегия отвлечения ресурсов противника на псевдосервисы может дать выигрыш даже в случае превосходства ресурсов атаки над ресурсами защиты.

В дальнейшем планируется исследовать эскалационные ловушки с имитацией борьбы с противником путем стохастического управления изменениями уязвимостей псевдосервисов (медовых ловушек).

**Литература**

1. Rittinghouse J.W. Cybersecurity operations hand*BO*ok: the definitive reference on operation cybersecurity / John W. Rittinghouse, William M Hancock. – Elsevier Digital Press. – Burlington, MA, 2003. – 1287 pp.
2. Spitzner L. Honeypots: tracking hackers / L. Spitzner. – Addison-Wesley, 2002. – 480 pp.
3. Виноградов Н.А. Управление псевдосервисами в защищенных информационных системах на основе теории конфликта / Н.А. Виноградов, Г.В. Данилина, Д.В. Домарев, Я.В. Милокум // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №6(34). – С. 5-12.
4. https://www.projecthoneypot.org/
5. www.honeynet.org
6. Котенко И.В. Обманные системы для защиты информационных ресурсов в компьютерных сетях / И.В. Котенко, М.В. Степашкин // Труды СПИИРАН, Санкт-Петербург. – 2004. – Вып. 2, т. 1. – С. 211-230.
7. Язов Ю.К. Методический подход к оцениванию эффективности ложных информационных систем / Ю.К. Язов, А.Л. Сердечный, И.А. Шаров // Вопросы кибербезопасности. – 2014. – №1(2). – С. 55-60.
8. Дружинин В.В. Введение в теорию конфликта / В.В. Дружинин, Д.С. Конторов, М.Д. Конторов. – Москва : Радио и связь, 1989. – 288 с.
9. Дынкин Е.Б. Управляемые марковские процессы и их приложения / Е.Б. Дынкин, А.А. Юшкевич. – Москва : Наука, 1975. – 338 с.
10. Эльсгольц Л.Э. Введение в теорию дифференциальных уравнений с отклоняющимся аргументом / Л.Э., С.Б. Норкин. – Москва : Наука, 1971. – 296 с.

***Автор статті***

**Даниліна Галина Володимирівна** – кандидат технічних наук, заступник директора Криворізького коледжу, Національний авіаційний університет, м. Кривий Ріг. Тел.: +380 (67) 564 91 72. E-mail: danilina@ukr.net.

***Author of the article***

**Danylina Halyna Volodymyrivna –** candidate of sciences (technical), deputy director of the Kryvyi Rih college, National Aviation University, city Kryvyi Rih. Tel.: +380 (67) 564 91 72. E-mail: danilina@ukr.net.

Дата надходження
в редакцію: 24.08.2016 р.

Рецензент:
доктор технічних наук, професор Ю.К. Зіатдінов
Національний авіаційний університет