Ирина Г. Дровникова[1], Елена С. Овчинникова[2], Евгений А. Рогозин[3]
*[1-3]Воронежский институт министерства внутренних дел Российской федерации,*
*пр-т Патриотов, 53, Воронеж, 394065, Россия*
*[1]e-mail: idrovnikova@vail.ru, https://orcid.org/0000-0001-5265-5875*
*[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524*
*[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535*

# ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ПРОГРАММНОЙ СРЕДЕ «CPN TOOLS»

*DOI: http://dx.doi.org/10.26583/bit.2021.1.03*

*Аннотация.* В статье представлены результаты имитационного моделирования динамики реализации сетевой атаки в ее конфликтном взаимодействии с системой защиты информации от несанкционированного доступа автоматизированной системы в виде количественных значений вероятностно-временных характеристик атаки. Целью имитационного моделирования является выявление возможности использования полученных результатов при расчете вероятности реализации и проведении количественной оценки опасности реализации сетевых атак на информационный ресурс автоматизированных систем, эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД). Представлена обобщенная формальная модель функционирования дестабилизирующего воздействия и построена сеть Петри-Маркова, отражающая динамику протекания информационного конфликта с учетом различий возможностей конфликтующих сторон. Разработана имитационная модель, описывающая механизм информационного конфликта «Сетевая атака – система защиты», и проведено имитационное моделирование, используя программную среду «CPN Tools». Результаты имитационного моделирования представлены в виде временной статистики процесса реализации сетевой атаки в динамике конфликтного взаимодействия с системой защиты. Приведены средние времена реализации типовых сетевых атак на информационный ресурс защищенных автоматизированных систем ОВД, полученные путем имитационного моделирования данных атак с помощью сети Петри-Маркова. Приведены перспективы использования полученных результатов для повышения защищенности автоматизированных систем при их разработке и эксплуатации на объектах информатизации ОВД.

*Ключевые слова: система защиты информации, несанкционированный доступ, сетевая атака, информационный конфликт, сеть Петри-Маркова, вероятностно-временные характеристики, имитационное моделирование, программная среда «CPN Tools».*

*Для цитирования: ДРОВНИКОВА, Ирина Г.; ОВЧИННИКОВА, Елена С.; РОГОЗИН, Евгений А. ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ПРОГРАММНОЙ СРЕДЕ «CPN TOOLS». Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 29–41, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1318>. Дата доступа: 20 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.03.*

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2], Evgeni A. Rogozin[3]
*[1-3]Voronezh Institute of the Ministry of the Interior,*
*Prospekt Patriotov, 53, Voronezh, 394065, Russia*
*[1]e-mail: idrovnikova@vail.ru, https://orcid.org/0000-0001-5265-5875*
*[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524*
*[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535*

## Simulation of the dynamics of network attacks in automated systems of internal affairs bodies in the "CPN Tools" software environment

*DOI: http://dx.doi.org/10.26583/ bit.2021.1.03*

*Abstract.* The paper presents the results of simulation modeling of the dynamics of the implementation of a network attack in its conflict interaction with the information protection system from unauthorized access of an automated system in the form of quantitative values of the probabilistic and time characteristics of the attack. The aim of simulation modeling is to identify the possibility of using the results obtained in calculating the implementation probability and conducting an accurate quantitative assessment of the risk of network attacks on the information resource of automated systems operated in a protected version at the objects of Informatization of internal Affairs bodies. A generalized formal model of the functioning of a destabilizing influence is presented and a Petri-Markov network is constructed that reflects the dynamics of the information conflict, taking into account the differences in the capabilities of the conflicting parties. A simulation model describing the mechanism of information conflict "Network attack – protection system" was developed, and simulation was performed using the "CPN Tools" software environment. The results of simulation modeling are presented in the form of time statistics of the process of implementing a network attack in the dynamics of conflict interaction with the protection system. The average implementation times of typical network attacks on the information resource of protected automated systems of internal Affairs bodies, obtained by simulating these attacks using the Petri-Markov network in the "CPN Tools" software environment, are given. The prospects of using the results obtained to improve the real security of automated systems in their development and operation at the objects of Informatization of internal Affairs bodies are outlined.

*Keywords: information protection system, unauthorized access, network attack, information conflict, Petri-Markov network, probabilistic-time characteristics, simulation modeling, "CPN Tools" software environment.*

*For citation: DROVNIKOVA, Irina G.; OVCHINNIKOVA, Elena S.; ROGOZIN, Evgeni A. Simulation of the dynamics of network attacks in automated systems of internal affairs bodies in the "CPN Tools" software environment. IT Security (Russia), [S.l.], v. 28, n. 1, p. 29–41, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1318>. Date accessed: 20 jan. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.03.*

## Введение

Процесс функционирования современных автоматизированных систем (АС), эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД), характеризуется применением злоумышленниками все более изощренных методов социальной инженерии, OSINT (Open Source INTelligence) поиска, сбора и анализа информации о структуре системы на основе открытых источников, иных разведывательных методов, приводящих к успешной реализации удаленных воздействий (сетевых атак), результатом которой является нанесение ущерба информационному ресурсу АС ОВД (нарушение конфиденциальности, целостности или доступности служебной информации) в соответствии с предметом атаки [1, 2]. Это приводит к необходимости учета возможной опасности реализации сетевых атак на начальных этапах разработки системы[1], что предполагает проведение количественной оценки опасности их реализации [3].

Анализ открытых литературных источников, международных и отраслевых стандартов Российской Федерации, нормативных документов Федеральной службы по техническому и экспертному контролю (ФСТЭК) России и руководящих документов МВД России, посвященных вопросам информационной безопасности (ИБ) АС[2-6] [4–6],

[1]ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении.
[2]ISO/IEC 15408-2012. Common Criteria for Information Technology Security Evaluation
[3]ГОСТ 34.601-90. Автоматизированные системы. Стадии создания.
[4]ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
[5]ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного

показал недостаточную проработанность данного вопроса, в частности, исследования сетевых атак в динамическом режиме. Это подтверждает актуальность проблемы имитационного моделирования динамики реализации сетевых атак в защищенных АС на объектах информатизации ОВД с целью исследования вероятностно-временных характеристик (ВВХ), необходимых для проведения количественной оценки опасности их реализации.

## 1. Постановка задачи

Процесс имитационного моделирования динамики реализации сетевых атак на информационный ресурс АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, включает следующие этапы:

1. На основе вербальной модели процесса функционирования системы защиты информации (СЗИ) от несанкционированного доступа (НСД), в условиях реализации сетевых атак на информационный ресурс защищенных АС ОВД, создание обобщенной формальной модели функционирования дестабилизирующего воздействия в динамике конфликтного взаимодействия с помощью сети Петри-Маркова (СПМ).
2. Построение имитационной модели, описывающей механизм информационного конфликта «Сетевая атака – СЗИ от НСД», используя программную среду «CPN Tools».
3. Осуществление имитационного моделирования и представление его результатов в табличной форме в виде значений ВВХ сетевой атаки в динамике информационного конфликта с СЗИ от НСД.

## 2. Метод исследования

Реализация сетевых атак на информационный ресурс современных АС ОВД представляет собой сложный динамический процесс, включающий множество взаимовлияющих параллельных процессов. Поэтому предпочтительным инструментом для его моделирования и анализа являются СПМ [7], объединяющие возможности и преимущества двух традиционных подходов к моделированию отказов в сложных системах, основанных на теории сетей Петри и марковских (а в более общем случае полумарковских) процессах [8, 9]. Построение обобщенной динамической модели информационного конфликта «Сетевая атака – СЗИ от НСД» с использованием СПМ, наглядно описывающей все состояния и условия переходов в рассматриваемом конфликте, позволяет исследовать процесс реализации сетевой атаки с определением ее временных и вероятностных характеристик.

Одним из методов определения количественных параметров указанных характеристик служит натурный эксперимент. Преодолеть затруднение, заключающееся в значительном усложнении его практического проведения в случае малого времени реализации сетевой атаки, позволяет использование программной среды имитационного моделирования «CPN Tools» – мощного инструмента моделирования и анализа сетей различного уровня сложности, к которым, несомненно, относятся и СПМ, доступного для ОС семейства Windows и Linux [10]. Имитационное моделирование в «CPN Tools», являясь дискретно-событийным, предполагает мгновенную смену состояний СПМ, что полностью соответствует конечному полумарковскому процессу. Среда «CPN Tools» предоставляет возможность программирования на унифицированном языке моделирования «Unified Modeling Language». Программный продукт «CPN Tools»

---

доступа к информации.

[6]Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169.

позволяет генерировать, анализировать пространство состояний модели, а также получать отчеты о работе сети в виде невременной и временной статистики [11].

При проведении имитационного моделирования процесса реализации сетевой атаки в динамике ее конфликтного взаимодействия с СЗИ от НСД с помощью СПМ вводятся следующие обозначения для элементов сети: $s_i$ – все возможные состояния (позиции) рассматриваемого процесса, $t_j$ – все возможные переходы между состояниями.

## 3. Модели и результаты исследования

Для обеспечения успешности реализации сетевой атаки или успешности защиты информационного ресурса АС ОВД необходимо оценить возможности обеих сторон в информационном конфликте «Сетевая атака – СЗИ от НСД».

В научных исследованиях информационного конфликта традиционно принимается допущение, что изначальные возможности конфликтующих сторон равны и конфликтные действия начинаются ими одновременно [12, 13], что в реальной практике эксплуатации защищенных АС ОВД выполняется крайне редко. Также должна быть учтена возможность выигрыша конфликта стороной, изначально не имеющей преимуществ, в результате возможных ошибок противоположной стороны (запаздывания ее действий, либо неадекватной реакции на воздействие). Следовательно, при разработке формальной модели функционирования дестабилизирующего воздействия в динамике конфликтного взаимодействия необходимо учитывать различия начальных и потенциальных возможностей конфликтующих субъектов.

Развитие и исход информационного конфликта «Сетевая атака – СЗИ от НСД» напрямую зависят от значений средних времен обнаружения сетевой атакой системы защиты, обнаружения системой защиты атаки и начала противодействия системы защиты сетевой атаке. Согласно результатам исследований, опубликованным в [1], средние значения указанных времен соответственно равны: $\tau_{\text{об ат}\rightarrow\text{СЗИ}}$ = 40 с, $\tau_{\text{об СЗИ}\rightarrow\text{ат}}$ = 52 с, $\tau_{\text{непр СЗИ}\rightarrow\text{ат}}$ = 1 с.

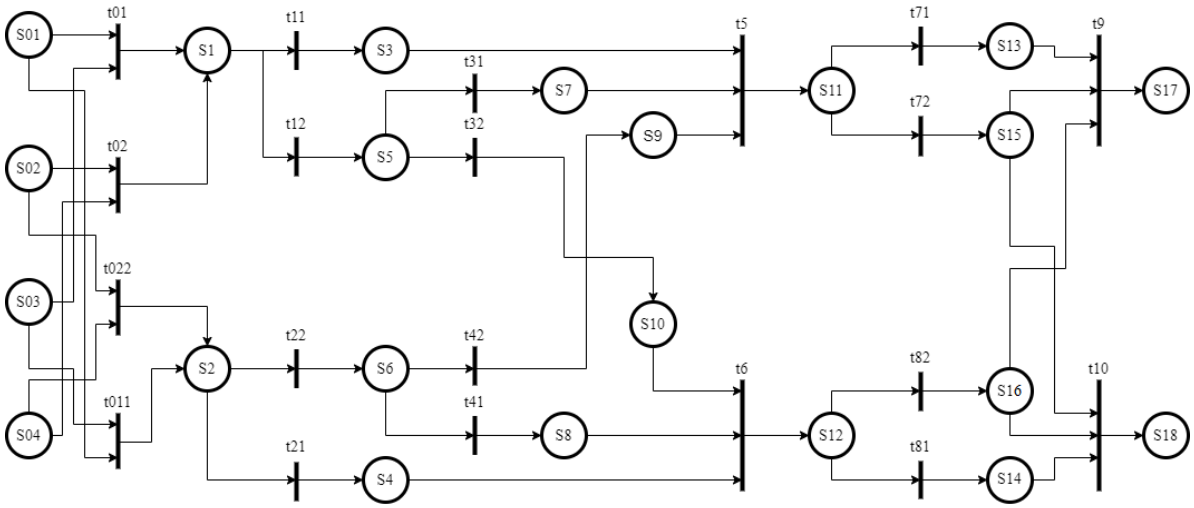
С учетом вышеизложенного для исследования информационного конфликта «Сетевая атака – СЗИ от НСД» в АС ОВД рассмотрим ситуацию, когда ответные действия системы защиты начинаются в процессе реализации сетевой атаки, то есть до наступления момента начала ее действия. В этом случае атака будет реализована, если все действия СЗИ от НСД вплоть до полного устранения эффективности попыток злоумышленника продолжать атаку (запрет обработки сообщений с блокированного адреса) не успеют завершиться к моменту начала действия атаки.

В [14, 15] подробно рассмотрены вербальная, вероятностная и обобщенная графовая модели динамики информационного конфликта «Сетевая атака – Система защиты» в АС ОВД, на основе которых с помощью СПМ построена представленная на рис. 1 обобщенная формальная модель, раскрывающая основные этапы данного конфликта.

Имитационная модель указанной сети, построенная при помощи программного продукта «CPN Tools», приведена на рис. 2.

В качестве начальных возможностей конфликтующих сторон, по которым осуществляется их сравнение в указанных моделях, рассматриваются производительности и объемы памяти сетевой атаки и СЗИ от НСД, определяемые в ходе натурного эксперимента. При этом под производительностью сетевой атаки (СЗИ от НСД) понимается количество выполняемых сетевой атакой (СЗИ от НСД) вредоносных (защитных) функций в единицу времени, а объем памяти сетевой атаки (СЗИ от НСД) представляет собой объем оперативной памяти, отвлекаемой на выполнение вредоносных

(защитных) функций сетевой атакой (СЗИ от НСД) из оперативной памяти АС, используемой для инициирования данной атаки (эксплуатирующей данную систему защиты).




$s_{01}$, $s_{03}$ – производительность сетевой атаки, СЗИ от НСД задана;
$t_{01}$, $t_{011}$ – сравнение производительностей сетевой атаки и СЗИ от НСД;
$s_{02}$, $s_{04}$ – объем памяти сетевой атаки, СЗИ от НСД задан;
$t_{02}$, $t_{022}$ – сравнение объемов памяти сетевой атаки и СЗИ от НСД;
$s_1$, $s_2$ – сетевая атака, СЗИ от НСД изначально имеет преимущество;
$t_{11}$, $t_{21}$ – усиление изначального преимущества сетевой атакой, СЗИ от НСД;
$s_3$, $s_4$ – сетевая атака, СЗИ от НСД усиливает изначально имеющееся преимущество;
$t_{12}$, $t_{22}$ – получение временного преимущества СЗИ от НСД, сетевой атакой;
$s_5$, $s_6$ – СЗИ от НСД противостоит сетевой атаке и получает временное преимущество, сетевая атака противостоит СЗИ от НСД и получает временное преимущество;
$t_{31}$, $t_{41}$ – возвращение утерянного преимущества сетевой атакой, СЗИ от НСД;
$s_7$, $s_8$ – сетевая атака противостоит СЗИ от НСД и возвращает утерянное преимущество, СЗИ от НСД противостоит сетевой атаке и возвращает утерянное преимущество;
$t_{32}$, $t_{42}$ – усиление временного преимущества СЗИ от НСД, сетевой атакой;
$s_9$, $s_{10}$ – сетевая атака, СЗИ от НСД усиливает временное преимущество;
$t_5$, $t_6$ – усиление имеющегося преимущества сетевой атакой, СЗИ от НСД;
$s_{11}$, $s_{12}$ – сетевая атака, СЗИ от НСД усиливает имеющееся преимущество;
$t_{71}$, $t_{81}$ – закрепление преимущества за сетевой атакой, СЗИ от НСД;
$s_{13}$, $s_{14}$ – преимущество за сетевой атакой, СЗИ от НСД закреплено;
$t_{72}$ – противостояние СЗИ от НСД сетевой атаке;
$s_{15}$ – СЗИ от НСД противостоит сетевой атаке;
$t_{82}$ – проведение «взлома» СЗИ от НСД сетевой атакой;
$s_{16}$ – сетевая атака «взламывает» СЗИ от НСД;
$t_9$ – преодоление СЗИ от НСД;
$s_{17}$ – финальное состояние: «взлом» СЗИ от НСД, победа сетевой атаки;
$t_{10}$ – блокирование сетевой атаки;
$s_{18}$ – финальное состояние: защита АС ОВД, победа СЗИ от НСД

*Рис. 1. СПМ, моделирующая информационный конфликт «Сетевая атака – СЗИ от НСД» (Fig. 1. SPM modeling information conflict "Network attack – SPI from NSD")*

Для построения сети и имитации ее функционирования приближенно к реальному взаимодействию сетевой атаки с системой защиты проведем конфигурацию в виде создания сегмента кода на языке UML (рис. 3). Полученная при этом имитационная модель представлена на рис. 4.

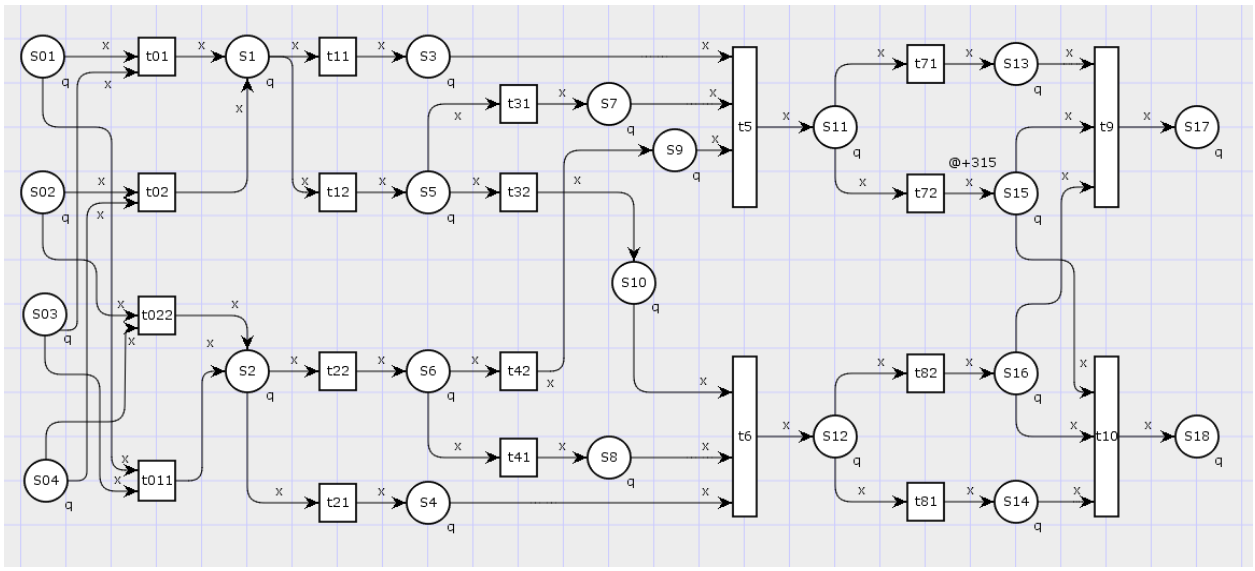


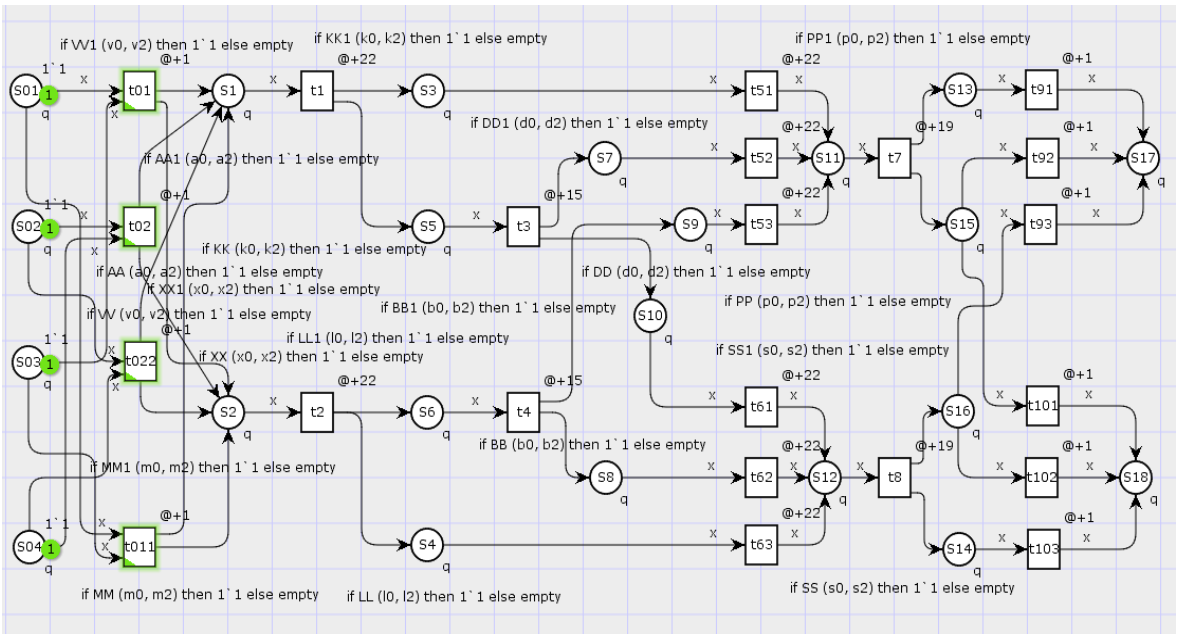

*Рис. 2. Имитационная модель информационного конфликта «Сетевая атака – СЗИ от НСД», построенная в программной среде «CPN Tools»*
*(Fig. 2. Simulation model of information conflict "Network attack – SPI from NSD", built in the software environment "CPN Tools")*

```
Declarations
  Standard priorities
  Standard declarations
    colset UNIT
    colset BOOL
    colset INT
    colset q = INT timed;
    var x : INT;
    fun curTime() = IntInf.toInt(!CPN'Time.model_time)
    colset VV = int with 1..100;
    var v0 : VV;
    val v2 = 10;
    fun VV (v0, v2) = (v0 <= v2);
    fun VV1 (v0, v2) = (v0 > v2);
    colset AA = int with 1..100;
    var a0 : AA;
    val  a2 = 10;
    fun AA (a0, a2) = (a0 <= a2);
    fun AA1 (a0, a2) = (a0 > a2);
    colset XX = int with 1..100;
    var x0 : XX;
    val x2 = 10;
    fun XX (x0, x2) = (x0 <= x2);
    fun XX1 (x0, x2) = (x0 > x2);
    colset MM = int with 1..100;
    var m0 : MM;
    val m2 = 10;
```

*Рис. 3. Настройка сети, имитирующей информационный конфликт «Сетевая атака – СЗИ от НСД»*
*(Fig. 3. Setting up a network that simulates an information conflict "Network attack – SPI from NSD")*

Поскольку представленная на рис. 1 обобщенная формальная модель имеет нелинейный характер, то для проведения имитационного моделирования информационного конфликта «Сетевая атака – СЗИ от НСД» с получением адекватных характеристик на выходе определим необходимое количество прогонов по СПМ на основе методики, изложенной в [10].

Для проверки адекватности модели осуществим необходимое количество шагов, в результате которых суммарное количество фишек в состояниях $s_1$ и $s_2$, $s_{11}$ и $s_{12}$, $s_{17}$ и $s_{18}$ составит 100: в состояниях $s_1$ и $s_2$ – 92 и 8 фишек (рис. 5), в состояниях $s_{11}$ и $s_{12}$ – 94 и 6 фишек (рис. 6), в состояниях $s_{17}$ и $s_{18}$ – 99 и 1 фишка (рис. 7).




$t_{01}$, $t_{011}$ – сравнение производительностей сетевой атаки и СЗИ от НСД;
$t_{02}$, $t_{022}$ – сравнение объемов памяти сетевой атаки и СЗИ от НСД;
$t_1$ – усиление изначального или получение временного преимущества сетевой атакой;
$t_2$ – усиление изначального или получение временного преимущества СЗИ от НСД;
$t_3$ – возвращение утерянного или усиление временного преимущества сетевой атакой;
$t_4$ – возвращение утерянного или усиление временного преимущества СЗИ от НСД;
$t_{51}$, $t_{52}$ , $t_{53}$ – усиление имеющегося преимущества сетевой атакой;
$t_{61}$, $t_{62}$, $t_{63}$ – усиление имеющегося преимущества СЗИ от НСД;
$t_7$ – закрепление преимущества за сетевой атакой или противостояние СЗИ от НСД сетевой атаке;
$t_8$ – закрепление преимущества за СЗИ от НСД или проведение «взлома» СЗИ от НСД сетевой атакой;
$t_{91}$, $t_{92}$, $t_{93}$ – преодоление СЗИ от НСД;
$t_{101}$, $t_{102}$, $t_{103}$ – блокирование сетевой атаки

*Рис. 4. Конфигурированная имитационная модель информационного конфликта «Сетевая атака – СЗИ от НСД»*
*(Fig. 4. Configured simulation model of information conflict "Network attack – SPI from NSD")*

Тогда частоту появления фишек в состояниях $s_1$, $s_{11}$ и $s_{17}$ рассчитаем по формулам:

$$\rho_{s_1 t_{01}} = \frac{46}{100} = 0.46,\ \rho_{s_1 t_{02}} = \frac{46}{100} = 0.46,\ \rho_{s_{11} t_5} = \frac{94}{100} = 0.94,$$

$$\rho_{s_{17} t_9} = \frac{99}{100} = 0.99.$$

Определим необходимое количество прогонов по сети для вероятности появления события с точностью $\varepsilon = 0,01$ и достаточностью $D$ = 0,99 с помощью выражения:

$$N = \frac{\rho(1-\rho)}{\varepsilon^2}\left[\Phi_0^{-1}\frac{D}{2}\right]^2,$$

где $\Phi_0$ – функция Лапласа.

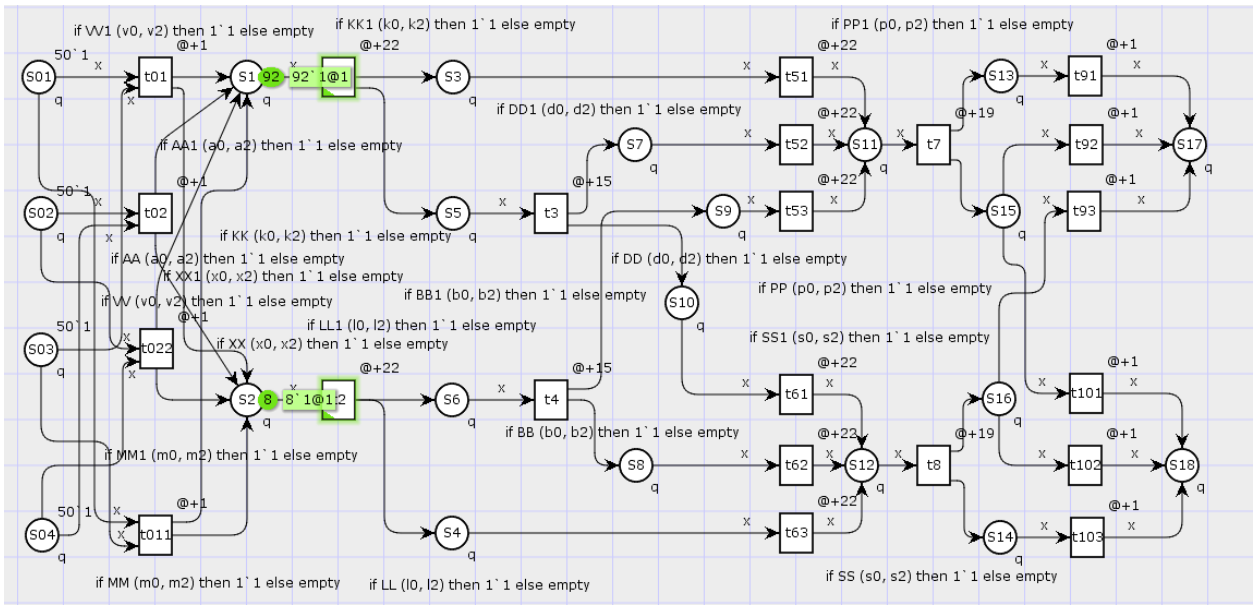



*Рис. 5. Прогон модели для определения количества фишек в состояниях $s_1$ и $s_2$*
*(Fig. 5. Run the model to determine the number of chips in states $s_1$ and $s_2$)*

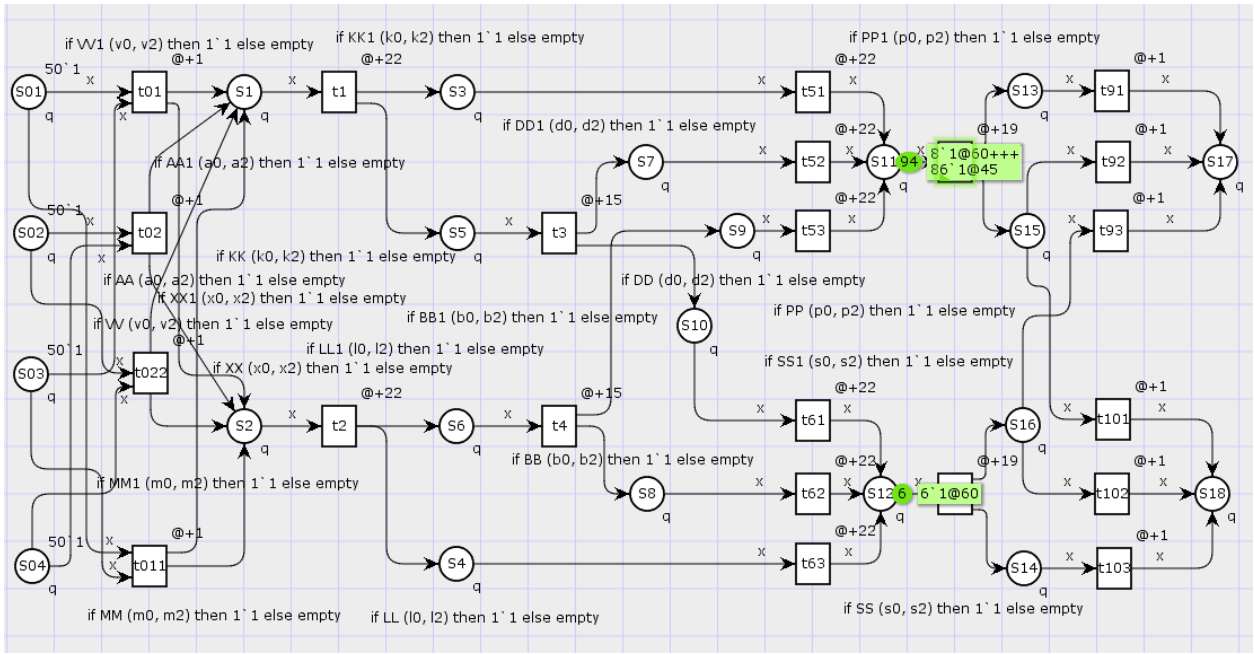



*Рис. 6. Прогон модели для определения количества фишек в состояниях $s_{11}$ и $s_{12}$*
*(Fig. 6. Run the model to determine the number of chips in states $s_{11}$ and $s_{12}$)*

Соответственно, необходимое количество прогонов $N_{s_1t_{01}}$, $N_{s_1t_{02}}$, $N_{s_{11}t_5}$, $N_{s_{17}t_9}$ для данных состояний будет следующим:

$$N_{s_1t_{01}} = \frac{0.46(1-0.46)}{0.01^2} \cdot 2.58^2 = 16534.4976 \approx 16534,$$

$$N_{s_1t_{02}} = \frac{0.46(1-0.46)}{0.01^2} \cdot 2.58^2 = 16534.4976 \approx 16534,$$

$$N_{s_{11}t_5} = \frac{0.94(1-0.94)}{0.01^2} \cdot 2.58^2 = 3754.2096 \approx 3754,$$

$$N_{s_{17}t_9} = \frac{0.99(1-0.99)}{0.01^2} \cdot 2.58^2 = 658.9836 \approx 659.$$

Для определения необходимого количества прогонов по сети выберем максимальное из рассчитанных значений $N \approx 16534$ (рис. 8).

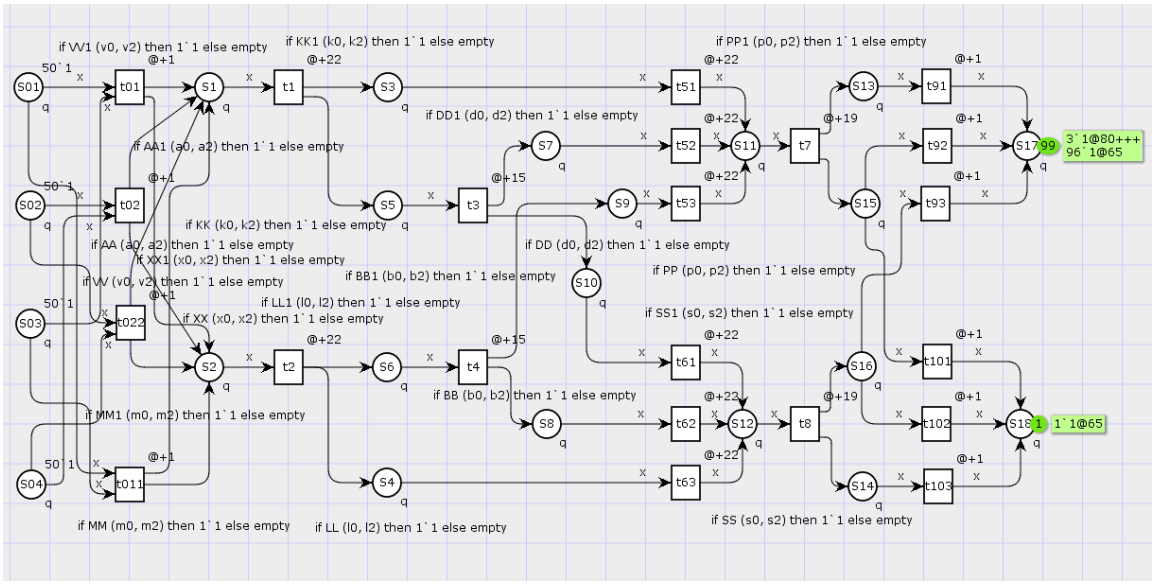



*Рис. 7. Прогон модели для определения количества фишек в состояниях $s_{17}$ и $s_{18}$*
*(Fig. 7. Run the model to determine the number of chips in states $s_{17}$ and $s_{18}$)*

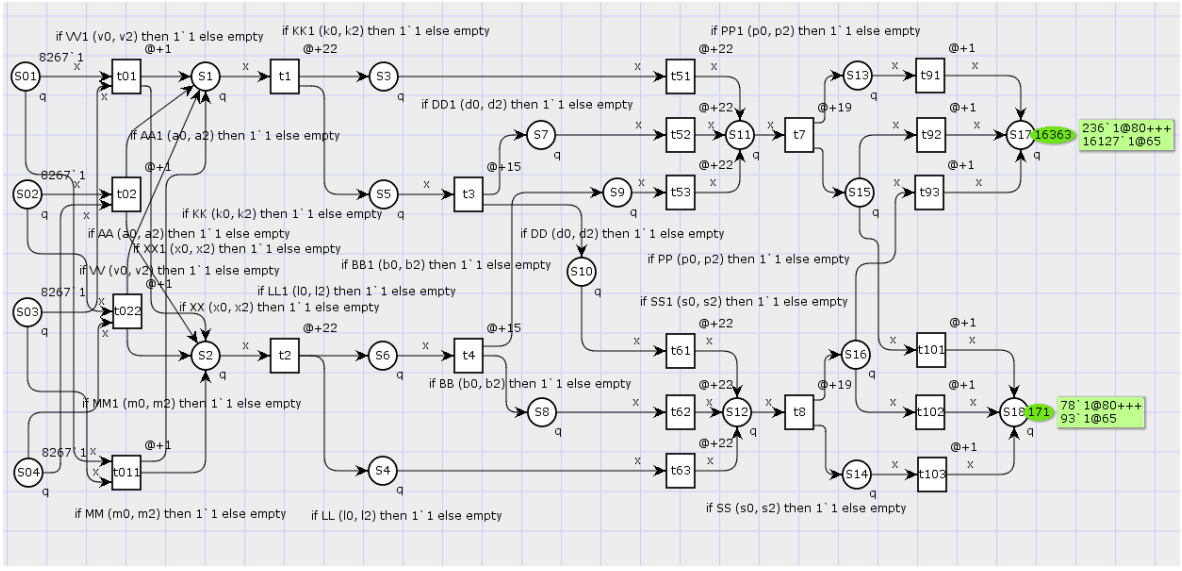



*Рис. 8. Имитационная модель информационного конфликта «Сетевая атака – СЗИ от НСД» с необходимым количеством прогонов*
*(Fig. 8. Simulation model of information conflict "Network attack – SPI from NSD" with the required number of runs)*

Поскольку время в «CPN Tools» представляется в виде целого числа, то для получения временной статистики процесса реализации сетевой атаки устанавливается следующая взаимосвязь между модельным (машинным) и реальным временем: 1 ед. = 1 с.

Временная статистика попадания маркера во все позиции представляется в виде табл. 1, имеющей следующие поля: Name – имя позиции; Count – счетчик проходов по графу, начиная с 0; Sum – суммарное количество попаданий маркера в конкретную позицию, Avrg – среднее количество попаданий маркера в позицию; Max – максимальное количество попаданий маркера в позицию; Time Avrg – среднее время нахождения маркера в одном из состояний графовой модели, формально описывающей реализацию сетевой атаки в АС в динамике ее конфликтного взаимодействия с СЗИ от НСД (количественное значение ВВХ сетевой атаки).

Результаты имитационного моделирования (временная статистика) процесса реализации сетевой атаки на информационный ресурс АС в виде количественных значений ее ВВХ представлены в табл. 1.

*Таблица 1. Временная статистика процесса реализации сетевой атаки в динамике конфликтного взаимодействия с СЗИ от НСД*

| Name | Count | Sum | Avrg | Max | Time Avrg |
|---|---|---|---|---|---|
| Marking_size_Network_attack'S01_1 | 8269 | 0 | 0.000000 | 8267 | 0 |
| Marking_size_Network_attack'S02_1 | 8269 | 0 | 0.000000 | 8267 | 0 |
| Marking_size_Network_attack'S03_1 | 8269 | 0 | 0.000000 | 8267 | 0 |
| Marking_size_Network_attack'S04_1 | 8269 | 0 | 0.000000 | 8267 | 0 |
| Marking_size_Network_attack'S1_1 | 32885 | 6805530 | 206.949367 | 16349 | 1 |
| Marking_size_Network_attack'S2_1 | 16721 | 39157 | 2.341772 | 185 | 1 |
| Marking_size_Network_attack'S3_1 | 32561 | 146986124 | 4514.177215 | 16210 | 22 |
| Marking_size_Network_attack'S4_1 | 188 | 52 | 0.278481 | 1 | 22 |
| Marking_size_Network_attack'S5_1 | 16490 | 638309 | 38.708861 | 139 | 22 |
| Marking_size_Network_attack'S6_1 | 371 | 19010 | 51.240506 | 184 | 22 |
| Marking_size_Network_attack'S7_1 | 278 | 7231 | 26.012658 | 137 | 15 |
| Marking_size_Network_attack'S8_1 | 368 | 12717 | 34.556962 | 182 | 15 |
| Marking_size_Network_attack'S9_1 | 188 | 71 | 0.379747 | 2 | 15 |
| Marking_size_Network_attack'S10_1 | 143 | 54 | 0.379747 | 2 | 15 |
| Marking_size_Network_attack'S11_1 | 32700 | 148879375 | 4552.886076 | 16349 | 22 |
| Marking_size_Network_attack'S12_1 | 372 | 19165 | 51.518987 | 185 | 22 |
| Marking_size_Network_attack'S13_1 | 32537 | 126661187 | 3892.835443 | 16186 | 19 |
| Marking_size_Network_attack'S14_1 | 189 | 91 | 0.481013 | 2 | 19 |
| Marking_size_Network_attack'S15_1 | 16514 | 647391 | 39.202532 | 163 | 19 |
| Marking_size_Network_attack'S16_1 | 370 | 16285 | 44.012658 | 183 | 19 |
| Marking_size_Network_attack'S17_1 | 16358 | 50089645 | 3062.088608 | 16356 | 1 |
| Marking_size_Network_attack'S18_1 | 180 | 2871 | 15.949367 | 178 | 1 |

Полученные значения ВВХ сетевой атаки в виде времен выполнения ею вредоносных функций (средних времен переходов по СПМ, моделирующей информационный конфликт «Сетевая атака – СЗИ от НСД») могут служить исходными данными для расчета вероятностей и оценивания опасности реализации сетевых атак в защищенных АС ОВД на основе разработки аналитической модели, учитывая особенности и реально существующие недостатки эксплуатации защищенных АС на объектах информатизации ОВД, рассмотренные в [3].

В [2] определены и проанализированы наиболее опасные и часто реализуемые в настоящее время (типовые) сетевые атаки, воздействующие на информационный ресурс защищенных АС ОВД. Среднее время реализации каждой атаки, смоделированной в «CPN Tools» (среднее время перемещения по СПМ из начальной позиции до конечного перехода), рассчитанное по методике, изложенной в [12, 16], приведено в табл. 2.

*Таблица 2. Среднее время реализации типовых сетевых атак на информационный ресурс защищенных АС ОВД*

| № п/п | Название атаки | Среднее время реализации атаки, с |
|---|---|---|
| 1 | Анализ сетевого трафика (сниффинг пакетов) | 24 |
| 2 | Сканирование сети | 19 |
| 3 | Парольная атака | 512 |
| 4 | Подмена доверенного объекта сети (IP-spoofing) | 48 |
| 5 | Навязывание ложного маршрута | 107 |
| 6 | Внедрение ложного объекта сети (ARP-spoofing) | 37 |
| 7 | Отказ в обслуживании (SYN-flood) | 17 |
| 8 | Удаленный запуск приложений (IP-hijacking) | 58 |

Зная количественные значения ВВХ сетевой атаки в процессе ее конфликтного взаимодействия с СЗИ от НСД, среднее время реализации каждой из указанных атак, а также задавая математические ожидания и средние квадратичные отклонения объемов памяти и производительностей конфликтующих систем, можно не только наблюдать протекание информационного конфликта в его динамике, но также рассчитать вероятности реализации типовых сетевых атак и провести количественную оценку опасности их реализации в защищенных АС ОВД. Полученные результаты могут быть использованы при обосновании количественных требований к СЗИ от НСД с целью повышения реальной защищенности АС при их разработке и эксплуатации на объектах информатизации ОВД.

## Заключение

Таким образом, на основе вербальной модели процесса функционирования СЗИ от НСД, в условиях реализации сетевых атак на информационный ресурс защищенных АС ОВД, в статье представлена обобщенная формальная модель функционирования дестабилизирующего воздействия в динамике конфликтного взаимодействия с системой защиты, построенная с использованием СПМ.

На основе обобщенной формальной модели разработана имитационная модель, описывающая механизм информационного конфликта «Сетевая атака – СЗИ от НСД», и проведено имитационное моделирование, используя программную среду «CPN Tools».

По результатам имитационного моделирования, представленным в виде временной статистики процесса реализации сетевой атаки в динамике информационного конфликта с СЗИ от НСД, определены количественные значения ее ВВХ.

Представлены средние времена реализации типовых сетевых атак, воздействующих на информационный ресурс защищенных АС ОВД, полученные путем моделирования данных атак с помощью СПМ в программной среде «CPN Tools».

Полученные значения ВВХ сетевой атаки в виде времен выполнения ею вредоносных функций позволят рассчитать вероятности и провести количественную оценку опасности реализации сетевых атак на этапах всего жизненного цикла функционирования защищенных АС ОВД в соответствии с характеристиками типовых сетевых атак, воздействующих на их информационный ресурс, и типовых систем защиты, используемых в АС ОВД. Данные результаты являются актуальными при обосновании количественных требований к перспективным СЗИ от НСД в процессе разработки АС и их эксплуатации в защищенном исполнении на объектах информатизации ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. – 588 с.
2. Дровникова И.Г. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел / И.Г. Дровникова, Е.С. Овчинникова, В.В. Конобеевских // Вестник Дагестан. гос. технич. ун-та. Технич. науки. 2020. Т. 47. № 1(2020). С. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85.
3. Дровникова, Ирина Г., Овчинникова, Елена С., Рогозин, Евгений А. Формирование основных показателей опасности сетевых атак в автоматизированных системах органов внутренних дел. Безопасность информационных технологий, [S.l.]. Т. 27, № 3. С. 6–17, сен. 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1288 (дата обращения: 26.11.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.01.
4. Oliver M. Technological determinism in educational technology research: some alternative ways of thinking about the relationship between learning and technology M. Oliver. Journal of Computer Assisted Learning. 2011. 27(5). P. 373–384. DOI: http://dx.doi.org/10.1111/j.1365-2729.2011.00406.
5. Rebovich G. Enterprise Systems Engineering: Advances in the Theory and Practice G. Rebovich, B. White. Boca Raton: CRC Press, 2011. – 459 p.
6. Djordjevic Nebojsa D. Software quality standards // Vojnoteh. glas. 2017. № 65(1). P. 102–104. URL: https://cyberleninka.ru/article/n/software-quality-standards (дата обращения: 26.11.2020).
7. Дровникова И.Г. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронеж. ин-та МВД России. 2019. № 4. С. 51–63. URL: https://elibrary.ru/item.asp?id=41568748 (дата обращения: 26.11.2020).
8. Акиншин Руслан Н., Ивутин Алексей Н., Есиков Дмитрий О., Страхов Илья А. Применение математического аппарата сетей Петри-Маркова для определения временных и вероятностных характеристик системы управления высоконагруженными веб-порталами с повышенной отказоустойчивостью // Научный вестник МГТУ ГА. 2014. №210 (12). С. 87–90. URL: https://cyberleninka.ru/article/n/primenenie-matematicheskogo-apparata-setey-petri-markova-dlya-opredeleniya-vremennyh-i-veroyatnostnyh-harakteristik-sistemy (дата обращения: 26.11.2020).
9. Моделирование марковских случайных процессов. URL: http://stratum.ac.ru/education/textbooks/modelir/lection33.html (дата обращения: 26.11.2020).
10. Сети Петри. Структура и правила выполнения сетей Петри. URL: https://bit.ly/2TcBs6B (дата обращения: 26.11.2020).
11. Синегубов С.В. Моделирование систем и сетей телекоммуникаций / С.В. Синегубов. – Воронеж: Воронеж. ин-т МВД России, 2016. – 336 с.
12. Романников Д.О. Об использовании программного пакета CPN TOOLS для анализа сетей Петри / Д.О. Романников, А.В. Марков // сб. науч. тр. НГТУ. 2012. № 2(68). С. 105–116. URL: https://elibrary.ru/item.asp?id=22560427 (дата обращения: 26.11.2020).
13. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронеж. госуд. технич. ун-т, 2013. – 265 с.
14. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М.: РадиоСофт, 2010. – 232 с.
15. Дровникова И.Г. К вопросу моделирования процесса функционирования системы защиты информации в условиях реализации сетевых атак на объектах информатизации органов внутренних дел / И.Г. Дровникова, Е.С. Овчинникова // Общественная безопасность, законность и правопорядок в III тысячелетии: матер. междунар. науч.-практич. конф. Ч. 2. Воронеж: ВИ МВД России, 2020. С. 218–225.
16. Дровникова И.Г. Моделирование динамики информационного конфликта в защищенных автоматизированных системах органов внутренних дел на основе сети Петри-Маркова / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронеж. ин-та ФСИН России. 2020. № 4. С. 51–66.
17. Bokova O.I., Drovnikova I.G., Ovchinnikova E.S. and Rodin S.V. Innovative technology for studying the dynamics of network attacks on information resources of the educational environment. ASEDU-2020: 1st International Conference on Advances in Science, Engineering and Digital Education. IOP Conf. Series: Journal of Physics: Conf. Series 1691 (2020) 012063 IOP Publishing. DOI: http://dx.doi.org/10.1088/1742-6596/1691/1/012063.

REFERENCES:

[1] Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph Yu.K. Yazov, S.V. Solovyov. Voronezh: Kvarta, 2018. – 588 p. (in Russian).

[2] Drovnikova I.G. Analysis of typical network attacks on automated systems of internal Affairs bodies I.G. Drovnikova, E.S. Ovchinnikova, V.V. Konobeevskikh. Bulletin of Dagestan state technical University. Technical Sciences. 2020. Vol. 47. no. 1(2020). P. 72–85. DOI: https://doi.org/10.21822/2073-6185-2020-47-1-72-85 (in Russian).

[3] Drovnikova, Irina G., Ovchinnikova, Elena S., Rogozin, Evgeni A. Network attacks main danger indicators formation in Internal Affairs Bodies automated systems. IT Security (Russia), [S.l.]. V. 27, no. 3. P. 6–17, sep. 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1288 (accessed: 26.11.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.01 (in Russian).

[4] Oliver M. Technological determinism in educational technology research: some alternative ways of thinking about the relationship between learning and technology M. Oliver. Journal of Computer Assisted Learning. 2011. 27(5): P. 373–384. DOI: http://dx.doi.org/10.1111/j.1365-2729.2011.00406.

[5] Rebovich G. Enterprise Systems Engineering: Advances in the Theory and Practice G. Rebovich, B. White. Boca Raton: CRC Press, 2011. – 459 p.

[6] Djordjevic Nebojsa D. Software quality standards. Vojnoteh. glas. 2017. no. 65(1). P. 102–104. URL: https://cyberleninka.ru/article/n/software-quality-standards (accessed: 26.11.2020).

[7] Drovnikova I.G. Analysis of existing methods and procedures for assessing the risk of network attacks in automated systems of internal Affairs bodies and aspects of their improvement I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin. Vestnik Voronezh. in-t of the Ministry of internal Affairs of Russia. 2019. № 4. P. 51–63. URL: https://elibrary.ru/item.asp?id=41568748 (accessed: 26.11.2020) (in Russian).

[8] Akinshin Ruslan N. et. al. Application of the mathematical apparatus of Petri-Markov networks to determine the time and probability characteristics of the management system for high-load web portals with increased fault tolerance. R.N. Scientific Bulletin of MSTU GA. 2014. no. 210. P. 87–90. URL: https://cyberleninka.ru/article/n/primenenie-matematicheskogo-apparata-setey-petri-markova-dlya-opredeleniya-vremennyh-i-veroyatnostnyh-harakteristik-sistemy (accessed: 26.11.2020) (in Russian).

[9] Modeling of Markov random processes. URL: http://stratum.ac.ru/education/textbooks/modelir/lection33.html (accessed: 26.11.2020) (in Russian).

[10] Petri Nets. Structure and rules for performing Petri nets. URL: https://bit.ly/2TcBs6B (accessed: 26.11.2020) (in Russian).

[11] Sinegubov S.V. Modeling of telecommunication systems and networks S.V. Sinegubov. Voronezh: Voronezh. in-t of the Ministry of internal Affairs of Russia, 2016. – 336 p. (in Russian).

[12] Romannikov D.O. About using the CPN TOOLS software package for Petri net analysis D.O. Romannikov, A.V. Markov. SB. nauch. Tr. NSTU. 2012. no. 2(68). P. 105–116. URL: https://elibrary.ru/item.asp?id=22560427 (accessed: 26.11.2020) (in Russian).

[13] Radko N.M. Penetration into the computer operating environment: models of malicious remote access N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh state technical University, 2013. – 265 p. (in Russian).

[14] Radko N.M. Risk models of information and telecommunication systems in the implementation of threats of remote and direct access N.M. Radko, I.O. Skobelev. M: Radiosoft, 2010. – 232 p. (in Russian).

[15] Drovnikova I.G. On the issue of modeling the process of functioning of the information protection system in the conditions of implementation of network attacks on the objects of informatization of internal affairs bodies. I.G. Drovnikova, E.S. Ovchinnikova. Public safety, law and order in the third millennium: mater. International Scientific and Practical Conference Part 2. Voronezh: Voronezh. in-t of the Ministry of Internal Affairs of Russia, 2020. P. 218–225 (in Russian).

[16] Drovnikova I.G. Modeling of information conflict dynamics in protected automated systems of internal affairs bodies based on the Petri-Markov network I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin. Vestnik Voronezh. in-ta of the Federal Penitentiary Service of Russia. 2020. no. 4. P. 51–66 (in Russian).

[17] Bokova O.I., Drovnikova I.G., Ovchinnikova E.S. and Rodin S.V. Innovative technology for studying the dynamics of network attacks on information resources of the educational environment. ASEDU-2020: 1st International Conference on Advances in Science, Engineering and Digital Education. IOP Conf. Series: Journal of Physics: Conf. Series 1691 (2020) 012063 IOP Publishing. DOI: http://dx.doi.org/10.1088/1742-6596/1691/1/012063.

*Поступила в редакцию – 23 ноября 2020 г. Окончательный вариант – 15 января 2021 г.*
*Received – November 23, 2020. The final version – January 15, 2021.*