К ВОПРОСУ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Язов Ю.К.[1], Авсентьев О.С.[2], Рубцова И.О.[3]

Цель статьи: *разработка математической модели оценки эффективности защи-ты от угроз нарушения целостности, доступности и конфиденциальности электронных документов в условиях ограниченной длительности их жизненного цикла в системах электронного документооборота.*

Метод: *математическое моделирование процессов электронного документообо-рота и реализации угроз безопасности информации с использованием аппарата сетей Петри-Маркова, позволяющего учитывать логические условия, определяющие возможно-сти выполнения рассматриваемых процессов, случайный характер, наличие разветвлений и параллельность исполнения составляющих эти процессы процедур и функций.*

Полученный результат: *предложен новый показатель оценки эффективности защиты электронных документов, направленный на сравнение вероятностно-временных характеристик процессов реализации угроз в системах электронного документооборота в условиях применения мер защиты и процессов обработки электронных документов, что впервые позволяет учесть время обработки документов в оценке эффективности их за-щиты. Разработана на основе аппарата сетей Петри-Маркова математическая модель и получены аналитические соотношения для расчета предложенного показателя на при-мере жизненного цикла входящих электронных документов с учетом времени выполнения типовых процедур и функций их обработки, времени реализации угроз, таких как несанк-ционированная замена физических адресов сетевых адаптеров компьютеров в составе системы электронного документооборота, а также применения мер защиты – исполь-зования специальных программ обнаружения фактов подмены физических адресов. Раз-работанная модель позволяет не только оценивать эффективность предпринимаемых мер защиты электронных документов от конкретных угроз, но и обосновывать на коли-чественной основе требования к времени обработки электронных документов в зависи-мости от вероятностно-временных характеристик реализации угроз, выявлять слабые места в системах электронного документооборота, которые могут использованы для реализации угроз, и условия, при которых такие угрозы могут быть реализованы.*

Ключевые слова: *показатель эффективности, функциональная модель, сеть Пет-ри-Маркова, угроза безопасности, мера защиты.*

DOI: *10.21681/2311-3456-2019-1-25-34*

Введение

Необходимость оценки эффективности (ЗИ) в информационных системах (ИС) от-мечается в целом ряде документов федерального уровня. Так, в федеральном законе Рос-сийской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва «О внесении изменений в Фе-деральный закон «О персональных данных»» указывается, что «обеспечение безопасности персональных данных достигается, в частности: оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных...». В Доктрине информацион-ной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646, отмечается, что «планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности» является «задачей государственных органов...» и т.д. Вместе с тем сегодня методическое обеспечение оценки эффективности ЗИ (или обеспечения безопасности информации) в практическом плане остается неразвитым. Это относится и к ИС с системами электронно-го документооборота (СЭД). Сегодня действия, направленные на копирование и несанк-ционированное распространение, подделку (модификацию), уничтожение электронных документов (ЭД) в ИС с СЭД, внедрение вредоносных программ с целью выполнения та-ких действий и т.д. становятся непременным элементом информационного противобор-ства и обусловливают принятие эффективных мер защиты.

В теоретическом плане во многих научных публикациях предлагались весьма раз-нопланов ые подходы к оценке эффективности ЗИ [1 – 10]. В их основе, как правило, ле-жало определение понятия эффективности как «степени соответствия результатов защиты информации цели защиты информации». В соответствии с этим определением сегодня из-вестно несколько подходов к оценке эффективности ЗИ, в том числе а) функциональный подход, основанный на сравнении состава реализуемых

1 Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж, Россия. E-mail: Yazoff_1946@mail.ru.

2 Авсентьев Олег Сергеевич, доктор технических наук, профессор, профессор кафедры информаци-онной безопасности Воронежского института МВД России, г. Воронеж, Россия. E-mail: osaos@mail.ru.

3 Рубцова Ирина Олеговна, аспирант кафедры организации и технологии защиты информации Бел-городского университета кооперации, экономики и права, г. Белгород, Россия. E-mail kaf-otzi-zav@bukep.ru.

мер защиты с составом, заданным нормативными документами, б) подход, основанный на введении оценочных уровней до-верия в соответствии с идеологией международного стандарта ИСО/ МЭК 15408, в) под-ход, реализующий балльный метод оценки, используемый в целом ряде международных стандартов и программных продуктов, таких как стандарт ISO 17799[4] и его инструментарий, например, программный продукт COBRA или программный продукт, реализующий метод CRAMM (CCTA[5] Risk Analysis & Management Method метод CCTA анализа и кон-троля рисков), программный продукт RiskWatch и др. Наиболее широко в настоящее вре-мя используется метод CRAMM. Однако эти подходы используют экспертные процедуры анализа защищенности информации и оценки эффективности ее защиты. Применение та-ких подходов к оценке эффективности защиты ЭД в СЭД приводит не только к неполной, но и зачастую к некорректной оценке, поскольку в них практически не учитывается фак-тор времени.

Наиболее глубоким является подход к оценке эффективности ЗИ, основанный на теории риска и использующий теорию марковских [11], полумарковских процессов [12] и аппарат сетей Петри-Маркова [5, 13, 14]. При этом в качестве цели ЗИ, как правило, рас-сматривается парирование всех выявленных актуальных угроз безопасности информации, а риск понимается только как риск реализации угроз, то есть ущерб от такой реализации считается неприемлемым. В качестве показателей оценки эффективности в [5] предложе-но использовать вероятностные абсолютный, относительный и относительно-разностный показате

абсолютный – $$\eta_{abs}(t) = P_u^{(0)}(t) - P_u^{(ЗИ)}(t);$$ (1)

относительный – $$\eta_{rel}(t) = \frac{P_u^{(ЗИ)}(t)}{P_u^{(0)}(t)},\ P_u^{(0)}(t) > 0;$$ (2)

относительно-разностный

$$\eta_{rd}(t) = \frac{\left|P_u^{(0)}(t) - P_u^{(ЗИ)}(t)\right|}{P_u^{(0)}(t)},\ P_u^{(0)} > 0,$$ (3)

где $P_u^{(0)}(t), P_u^{(ЗИ)}(t)$ – вероятность реализации угрозы безопасности информации за время *t* в условиях соответственно отсутствия и применения мер защиты.

Однако применение таких показателей для оценки эффективности защиты ЭД в СЭД оказывается состоятельным в том случае, когда длительность жизненного цикла ЭД достаточно велика и не влияет на оценку возможности реализации угроз, направленных на выполнения несанкционированных действий с этими ЭД. К таким документам относятся те, которые долгое время хранятся в базах (хранилищах) данных СЭД, на компьютерах пользователей СЭД или являются постоянно востребованными и циркулируют в СЭД. Ес-ли же длительность жизненного цикла документа ограничена и в пределах этого жизненного цикла требуется защитить ЭД или меры защиты применяются в ходе обработки ЭД до вывода его из действия (например, завершения отработки входящего документа и от-правки ответа на него, после чего сам ЭД отправляется в архив – электронное хранилище), то необходимо использовать иные показателя оценки эффективности. В данной статье предлагается подход к оценке эффективности защиты ЭД в условиях ограниченной дли-тельности их жизненного цикла.

Показатели оценки эффективности защиты электронных документов в СЭД в условиях ограниченной длительности их жизненного цикла

Обозначим длительность жизненного цикла *i*-го ЭД как $\tau_{doc,i}$. Эта величина явля-ется случайной, зависящей от многих факторов, таких как количество и длительность процедур и функций, которые выполняются при обработке документа, его объема, квали-фикации исполнителей и т.д. Пусть время реализации *u*-й угрозы в условиях применения оцениваемой меры защиты составляет случайную величину $\tau_u^{(ЗИ)}$. Для эффективной защи-ты необходимо, чтобы $\tau_u^{(ЗИ)} > \tau_{doc,i}$.

Пусть плотности распределения вероятностей величин $\tau_{doc,i}$ и $\tau_u^{(ЗИ)}$ соответственно равны $w_{doc}(\tau_{doc,i})$ и $w_u(\tau_u^{(ЗИ)})$. Так как рассматриваемые случайные величины являются не-зависимыми, то в соответствии с [15] плотность распределения вероятности того, что для величины $y = \tau_u^{(ЗИ)} - \tau_{doc,i}$ в каждой попытке реализации угрозы будет выполняться условие $y > 0$ определяется из соотношения:

$$p_{exc}(\tau_u^{(ЗИ)} - \tau_{doc,i} > 0) = \int_0^\infty \int_0^\infty w_u(y + \tau_{doc,i}) \cdot w_{doc}(\tau_{doc,i}) \cdot d\tau_{doc,i} \cdot dy$$ (4)

Тогда, среднее время реализации угрозы $\overline{\tau_{ui}^{(ЗИ)}}$ с условием, что время реализации угрозы в каждой попытке не превышает длительность жизненного цикла, составляет с учетом [16] величину

$$\overline{\tau_{ui}^{(ЗИ)}} = \frac{\overline{\tau_u^{(ЗИ)}}}{1 - p_{exc}(\tau_u^{(ЗИ)} - \tau_{doc,i})},$$ (5)

где $\overline{\tau_{ui}^{(ЗИ)}}$ – среднее значение времени $\tau_{ui}^{(ЗИ)}$.

Таким образом, в соответствии с формулой (5) происходит прореживание исходно-го потока, описывающего процесс реализации -й угрозы. Как показано в [5, 16,17], при таком прореживании результирующий поток с уменьшением вероятности быстро при-ближается к пуассоновскому, при этом даже при вероятности 0.3 – 0.4 ошибка с заменой любой одномодальной плотности распределения на экспоненциальную составляет едини-цы процентов. В связи с этим из формулы (4) следует, что

$$p_{exc}(\tau_u^{(ЗИ)} - \tau_{doc,i} > 0) = \frac{\overline{\tau_{doc,i}}}{\overline{\tau_{doc,i}} + \overline{\tau_u^{(ЗИ)}}},$$ (6)

4 Стандарт ISO/IES 17799 стандарт по информационной безопасности, опубликованный в 2005 г. организа-циями ISO и IEC. В 2013 г. сменил название на ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью».

5 CCTA (Central Computer and Telecommunications Agency) Центральное агентство по компьютерам и теле-коммуникациям Великобритании

Тогда вероятность того, что угроза относительно *l*-го ЭД не будет реализована за время , которая может быть использована в качестве показателя эффективности защиты, рассчитывается по формуле:

$$\eta_{exc}(t) = exp\left\{-\frac{t}{\overline{\tau_u^{(ЗИ)}} \cdot (1 + \frac{\overline{\tau_u^{(ЗИ)}}}{\tau_{doc,i}})}\right\}. \quad (7)$$

Из приведенного соотношения видно, что чем больше среднее время реализации угрозы или чем меньше длительность жизненного цикла ЭД, тем эффективность защиты выше, однако с течением времени эффективность падает.

Функциональная и математическая модели процесса обработки ЭД

Для расчета времени обработки ЭД строится сначала функциональная модель про-цесса обработки [18 – 20], а затем на ее основе сеть Петри-Маркова, моделирующая дина-мики обработки ЭД. Рассмотрим эти модели на примере обработки в СЭД входящего ЭД.

Функциональная модель процесса обработки (жизненного цикла) входящего ЭД, содержащая описание и порядок выполнения процедур и функций обработки документа, приведена в табл.1, а соответствующая ей сеть Петри-Маркова [5, 14], моделирующая данный процесс во времени, – на рис.1.

Алгоритм расчета времени срабатывания сети сводится к следующему.

1. В сети Петри-Маркова (см. рис.1) выделяются три траектории[6]:

первая – 0(a)→ ... → 11(z); вторая – 12(a) → ... → 26(z); третья – 23(a) →... → 26(z).

2. Среднее время выполнения процесса по *d*-й траектории определяется следую-щим образом:

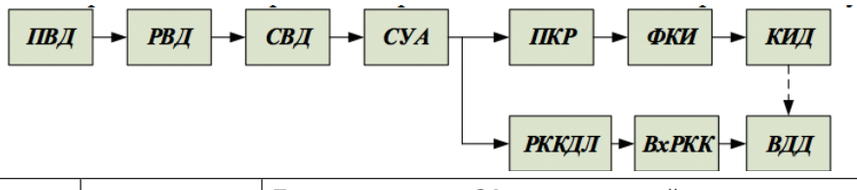
$$\overline{\tau_d} = \chi'_{\Sigma_d}(s)\big|_{s=0}, d = \overline{1, D}; \quad (8)$$

где $\chi_{\Sigma_d}(s)$ – производная от характеристической функции суммы времен выполне-ния функций, составляющих процедуры, реализуемые по *d*-й траектории сети,

$$\chi_{\Sigma_D}(s) = \prod_{r=1}^{R_d} \chi_r(s), r = \overline{1, R_d} \quad (9)$$

Таблица 1

Процедуры и функции обработки входящего электронного документа в СЭД

Наименование про-цедуры	Обозначе-ние про-цедуры	Наименование функции	Обозначе-ние функ-ции
Графической представление процесса обработки входящего электронного документа 			
Процедура приема входящего ЭД (ПВД)	$pr_{1.1}$	Прием входящего ЭД по электронной почте	$f_{1.1.1}$
		Размещение всех видов поступающих документов в буфере рабочей станции делопроизводителя (РСД),	$f_{1.1.2}$
Процедура реги-страции входящих документов (РВД)	$pr_{1.2}$	Формирование регистрационно-контрольной карточки	$f_{1.2.1}$
		Установка двухсторонних связей между документами («в ответ на...» и т. д.) с возможностью графического отображения дерева установленных связей	$f_{1.2.2}$
		Фиксация сопроводительных писем, включая внесе-ние текста	$f_{1.2.3}$
		Внесение в базу данных содержания ЭД в виде текста письма электронной почты	$f_{1.2.4}$
Процедура скани-рования входящего ЭД (СВД)	$pr_{1.3}$	Контроль размера присоединяемых файлов	$f_{1.3.1}$
		Фиксация сопроводительных писем	$f_{1.3.2}$
		Внесение в базу данных содержания документа в виде файлов образов документов	$f_{1.3.3}$
Процедура созда-ния уве-домления адресатам (СУА)	$pr_{1.4}$	Направление уведомления адресатам	$f_{1.4.1}$
		Перенаправление уведомления тем руководителям, кому переадресован документ	$f_{1.4.2}$

6 В теории сетей Петри-Маркова принято обозначать позиции номером с буквой «a» (на рис.1 для упрощения буква опущена), а переходы – номером с буквой «z». Принято также, что перемещение из позиции в переход происходит за случайное конечное время, а из перехода в позиции - мгновенно

Процедура подго-товки карточки резолюции (ПКР)	$pr_{1.5}$	Определение исполнителей ЭД	$f_{1.5.1}$
		Определение ответственных исполнителей	$f_{1.5.2}$
		Фиксация выданных адресатами резолюций	$f_{1.5.3}$
		Создание и печать на бланках проектов резолюций по ЭД	$f_{1.5.4}$
Процедура форми-рования карточки исполнения (ФКИ)	$pr_{1.6}$	Фиксация приема документа на исполнение	$f_{1.6.1}$
		Фиксация перепоручения исполнения документа	$f_{1.6.2}$
Процедура кон-троля исполнения документа (КИД)	$pr_{1.7}$	Задание признака ответственного исполнителя	$f_{1.7.1}$
		Постановка на контроль	$f_{1.7.2}$
		Фиксация отчетов о ходе исполнения резолюции	$f_{1.7.3}$
		Фиксация исполнения документа	$f_{1.7.4}$
		Снятие с контроля	$f_{1.7.5}$
Процедура созда-ния регистрацион-но-контрольной карточки исходя-щего документа (ИсхРКК)	$pr_{1.8}$	Расписывание документа должностным лицам взаимодей-ствующих подразделений	$f_{1.8.1}$
		Автоматическое создание регистрационно-контроль-ной карточки для этих должностных лиц	$f_{1.8.2}$
Процедура созда-ния регистрацион-но-контрольной карточки входяще-го документа (ВхРКК)	$pr_{1.9}$	Фиксация поступления ответа по получению документа	$f_{1.9.1}$
		Создание входящей регистрационно-контрольной карточ-ки	$f_{1.9.2}$
		Перенаправление карточки и документа должностным лицам взаимодействующих подразделений	$f_{1.9.3}$
Процедура вывода доку-мента из дей-ствия (ВДД)	$pr_{1.10}$	Уничтожение электронного документа;	$f_{1.10.1}$
		Передача электронного документа на архивное хранение	$f_{1.10.2}$

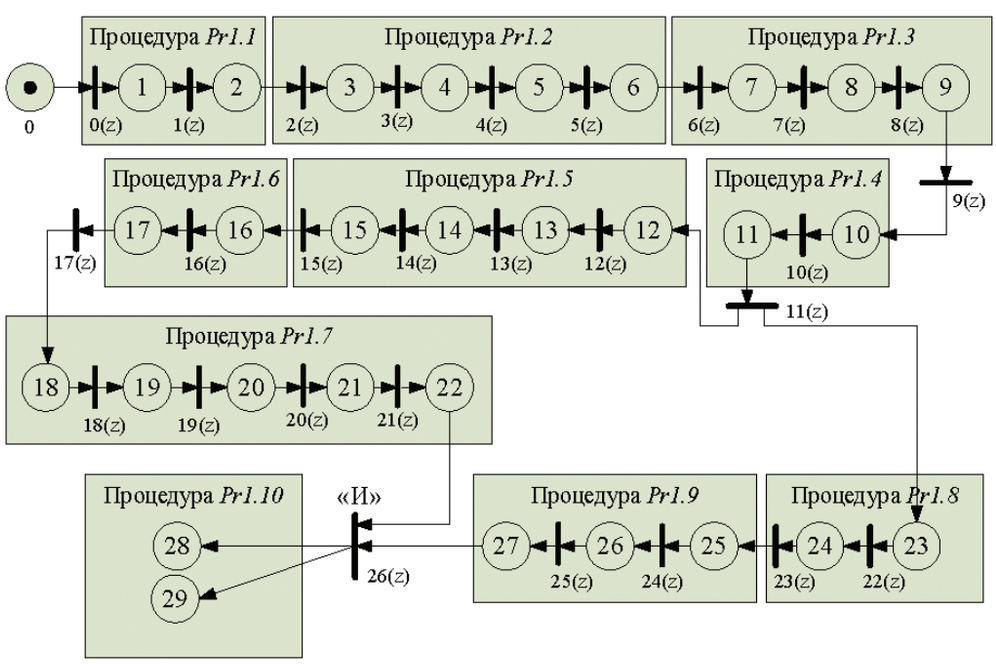


Рис. 1. Граф сети Петри-Маркова, моделирующей процесс циркуляции ЭД в СЭД

независимо от того, какому закону подчиняются распределения времен выполнения каж-дой функции;

D – общее количество выделенных траекторий;

R_d – количество участков «позиция-переход» на *d*-й траектории сети Петри-Маркова.

$$\overline{\tau_{0,11}} = \sum_{r=1}^{R_{0,11}} \overline{\tau_r^{(0,11)}},\ \overline{\tau_{12,26}} = \sum_{r=1}^{R_{12,26}} \overline{\tau_r^{(12,26)}},\ \overline{\tau_{23,26}} = \sum_{r=1}^{R_{23,26}} \overline{\tau_r^{(23,26)}}, \quad (10)$$

где $\overline{\tau_r^{(a,z)}}$ – средняя продолжительность выполнения *r*-ой функции по траектории от позиции a до перехода z;

$\overline{\tau_{i,j}}$ – среднее суммарное время выполнения совокупности функций от состояния с номером *i* до перехода с номером *j*.

3. Длительность выполнения перехода 26(z) с логикой «И» в соответствии с [7] рассчитывается по формуле:

$$\overline{\tau_{"И"}} = \frac{\overline{\tau_{12,26}}^2 + \overline{\tau_{12,26}} \cdot \overline{\tau_{23,26}} + \overline{\tau_{23,26}}^2}{\overline{\tau_{12,26}} + \overline{\tau_{23,26}}}. \quad (11)$$

4. Среднее время исполнения входящего документа определяется из соотношения

$$\overline{\tau_{doc}^{(вх)}} = \overline{\tau_{0,11}} + \overline{\tau_{"И"}}. \quad (12)$$

Для гипотетической ситуации, когда среднее время срабатывания всех простых пе-реходов примерно одинаково и равно $\overline{\tau_{func}}$, время жизненного цикла входящего документа при выполнении всех указанных функций его обработки составляет величину $25\overline{\tau_{func}}$.

Функциональная и математическая модели процесса реализации угроз безопасности электронного документооборота

Для расчета времени реализации угрозы в условиях применения мер защиты снача-ла также разрабатывается функциональная модель процесса реализации угрозы, а затем для этой модели строится сеть Петри-Маркова и определяется среднее время реализации угрозы. Пример такой функциональной модели для атаки «ARP-спуффинг» [1] в условиях применения программы типа remarp или arpwatch, предназначенных для обнаружения подмены MAC-адресов хостов в сети, приведен в графическом виде на рис.2, а соответ-ствующая ей сеть Петри-Маркова – на рис.3.

Время срабатывания этой сети Петри-Маркова рассчитывается следующим обра-зом:

$$\overline{\tau_u} = \overline{\tau_{0,1(z)}} + \overline{\tau_{"ИЛИ"}} + \overline{\tau_{7,4(z)}}, \quad (13)$$

где $\overline{\tau_{0,1(z)}}$ - среднее время перемещения процесса из позиции 0(a) в переход 1(z), определя-емое с учетом того, что переход срабатывает в соответствии с логикой «И-НЕ», то есть

$$\overline{\tau_{0,1(z)}} = \overline{\tau_{0,0(z)}} + \overline{\tau_{"И-НЕ"}}; \quad (14)$$

$\overline{\tau_{"И-НЕ"}}$ - среднее время срабатывания логического перехода «И-НЕ», когда ARP-ответ от хоста нарушителя поступил на маршрутизатор, а от хостов «А» и «Б» нет, при этом в соответствии с [21]

$$\overline{\tau_{"И-НЕ"}} = \overline{\tau_{1,1(z)}} \cdot \left(1 + \frac{\overline{\tau_{1,1(z)}}}{\overline{\tau_{2\&3}}}\right); \quad (15)$$

$$\overline{\tau_{2\&3}} = \frac{\overline{\tau_{2,1(z)}}^2 + \overline{\tau_{2,1(z)}} \cdot \overline{\tau_{3,1(z)}} + \overline{\tau_{3,1(z)}}^2}{\overline{\tau_{2,1(z)}} + \overline{\tau_{3,1(z)}}}$$

$$\overline{\tau_{7,4(z)}} = \overline{\tau_{7,3(z)}} + \overline{\tau_{8,4(z)}}. \quad (16)$$

Время срабатывания перехода «ИЛИ» определяется с учетом того, что программа обнаружения подмены MAC-адресов с некоторой вероятностью выявляет такую подмену, при этом угроза реализуется, если ни в одном из хостов и в маршрутизаторе не будет об-наружена подмена. Если считать, что эта вероятность примерно одинакова для всех хо-стов

сети, то в соответствии с [21] время срабатывания логического перехода «ИЛИ» опреде-ляется по формуле:

$$\overline{\tau_{"ИЛИ"}} = \frac{1}{(1-p_{MAC})^3 \cdot \left(\frac{1}{\overline{\tau_{4,2(z)}}} + \frac{1}{\overline{\tau_{5,2(z)}}} + \frac{1}{\overline{\tau_{6,2(z)}}}\right)}. \quad (17)$$

Пусть время срабатывания простых переходов в сети Петри-Маркова, моделирую-щей реализацию угрозы, одинаково для всех переходов и равно $\overline{\tau_{tr}}$. Тогда среднее время реализации угрозы составит величину:

$$\overline{\tau_u} = \left[14 + \frac{1}{(1-p_{MAC})^3}\right] \cdot \frac{\overline{\tau_{tr}}}{3}. \quad (18)$$

Если положить, что все функции обработки документа выполняются в среднем за одно и то же время $\overline{\tau_{func}}$, то показатель эффективности защиты ЭД с учетом соотношения (7) рассчитывается по формуле:

$$\eta_{exc}(t) = exp\left\{-\frac{3 \cdot t}{\overline{\tau_{tr}} \cdot \left[14 + \frac{1}{(1-p_{MAC})^3}\right] \cdot \left[1 + \frac{(14 + \frac{1}{(1-p_{MAC})^3}) \cdot \overline{\tau_{tr}}}{75 \cdot \overline{\tau_{func}}}\right]}\right\}. \quad (19)$$

Зависимости эффективности защиты ЭД от существенных параметров в графиче-ском виде представлены на рис.4 – 6, здесь $\overline{\tau_{tr}} = 0.5$ и $\overline{\tau_{func}} = 1$.

Из графика видно, что при малом времени обработки ЭД в сравнении с временем реализации угроз и при высоких вероятностях обнаружения факта подмены MAC-адресов может быть обеспечена достаточно высокая эффективность защиты от подобных угроз.

Аналогичные зависимости были получены и для других видов электронных доку-ментов (исходящих, организационно-распорядительных и иных документов органов государственной власти, организаций и предприятий), применительно ко всем актуальным угрозам и мерам защиты от них, которые могут сегодня реализовываться в СЭД.

Такие зависимости позволяют не только оценивать эффективность предпринимае-мых мер защиты электронных документов от конкретных угроз, но и обосновывать на ко-личественной основе требования к времени обработки ЭД в зависимости от вероятностно-временных характеристик реализации угроз, выявлять слабые места в СЭД, которые могут использованы для реализации угроз, и условия, при которых такие угрозы реализуются в конкретных СЭД.

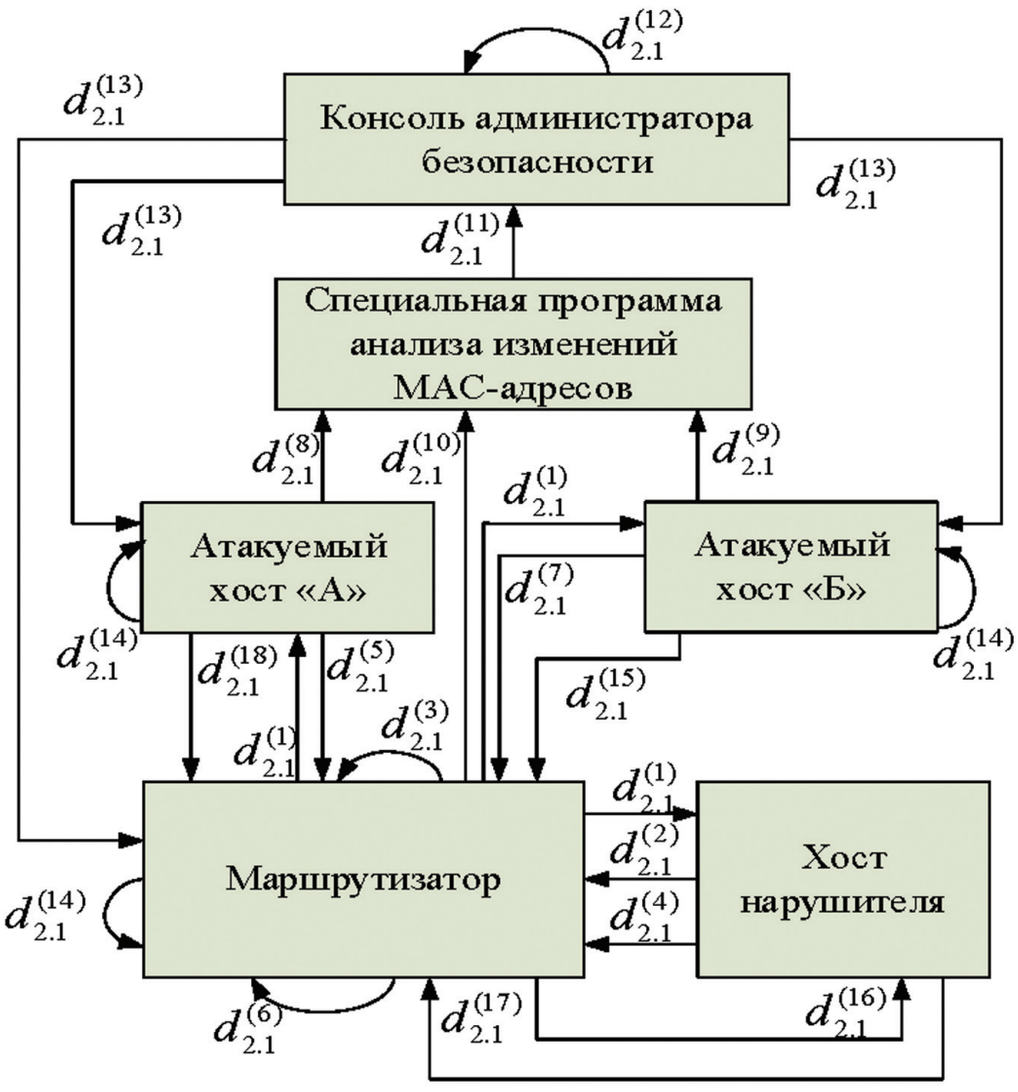


Рис.2. Графическое представление модели атаки «ARP-спуффинг» в условиях применения программы обнаружения подмены MAC-адресов хостов в сети

$d_{2.1}^{(1)}$ – Отправка широковещательного запроса по протоколу ARP всем хостам сегмента ИС;
$d_{2.1}^{(2)}$ – Отправка ложного ARP-ответа нарушителем от имени (сетевого адреса) хоста «А» маршрутизатору, в котором указывается IP-адрес хоста «А» и свой MAC-адрес;
$d_{2.1}^{(3)}$ – Меняется запись в таблице маршрутизации маршрутизатора для хоста «А»;
$d_{2.1}^{(4)}$ –Отправка ложного ARP-ответа нарушителем маршрутизатору от имени (сетевого адреса) хоста «Б», в котором указывается IP-адреса хоста «Б» и свой MAC-адрес
$d_{2.1}^{(5)}$ – Хост «А» пытается передать истинный ARP-ответ, но ARP-пакет отбрасывается;
$d_{2.1}^{(6)}$ – Меняется запись в таблице маршрутизации маршрутизатора для хоста «Б»;
$d_{2.1}^{(7)}$ – Хост «Б» пытается передать истинный ARP-ответ, но ARP-пакет отбрасывается
$d_{2.1}^{(8)}$ – Программа обнаружения выявляет факт подмены MAC-адреса на хосте «А»;
$d_{2.1}^{(9)}$ – Программа обнаружения выявляет факт подмены MAC-адреса на хосте «Б»;
$d_{21}^{(10)}$ – Программа обнаружения выявляет факт подмены на MAC-адресов на маршрутизаторе;
$d_{2.1}^{(11)}$ – Программа обнаружения передает на консоль администратора сообщение о подмене MAC-адресов;
$d_{21}^{(12)}$ – Администратором принимается решение о восстановлении первоначальных MAC-адресов;
$d_{2.1}^{(13)}$ – Передается команда на восстановление первоначальных MAC-адресов
$d_{2.1}^{(14)}$ – На хостах «А», «Б» и в маршрутизаторе восстанавливаются первоначальные MAC-адреса;
$d_{2.1}^{(15)}$ – Хост «А» передает электронный документ для хоста «Б» на маршрутизатор;
$d_{2.1}^{(16)}$ – Маршрутизатор в соответствии с измененной ARP-таблицей переправляет документ на хост наруши-теля;
$d_{2.1}^{(17)}$ – Нарушитель копирует ЭД (или модифицирует его), а оригинал (или модифицированный ЭД) передает на маршрутизатор для хоста «Б»;
$d_{2.1}^{(18)}$ – Маршрутизатор переправляет ЭД, полученный от нарушителя, на хост «Б»

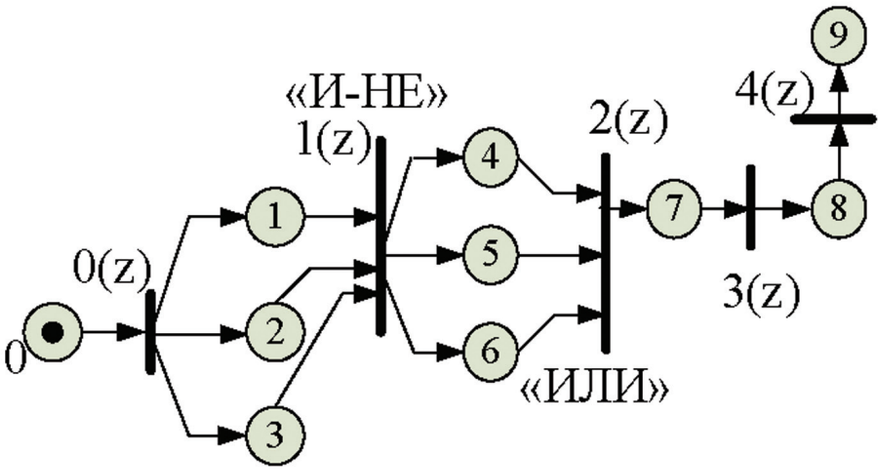


Рис.3. Сеть Петри-Маркова, моделирующая атаку «ARP-спуффинг» в условиях применения программы об-наружения подмены MAC-адресов хостов в сети

0(a) – начальное состояние процесса, нарушитель готов к проведению атаки, маршрутизатор в го-товности направить широковещательный запрос всем хостам сети на подтверждение своих MAC-адресов;
1(a) – широковещательный запрос поступил на хост нарушителя по дуге 0(z)-1(a);
2(a) – широковещательный запрос поступил на хост «А» – клиента СЭД;
3(a) – широковещательный запрос поступил на хост «Б» – клиента СЭД;
4(a) – проведена подмена MAC-адресов на маршрутизаторе и проводится проверка такой подмены программой обнаружения;
5(a) – проведена подмена MAC-адреса на хосте «А» и проводится проверка такой подмены про-граммой обнаруже-ния;
6(a) – проведена подмена MAC-адреса на хосте «Б» и проводится проверка такой подмены про-граммой обнаружения
7(a) – программой обнаружения не выявлен факт подмены MAC-адресов ни на одном хосте сети
8(a) – на маршрутизатор поступило сообщение от хоста «Б» с ЭД для хоста «А»;
9(a) – документ по подменному MAC-адресу поступил на хост нарушителя, атака завершена успеш-но;
0(z) – передача широковещательного ARP-запроса всем хостам ИС;
1(z) – логический переход «И-НЕ», срабатываемый при выполнении условия, что ARP-ответы от хостов «А» и «Б» придут на маршрутизатор позже ответов хоста нарушителя;
2(z) – логический переход «ИЛИ», срабатывающий, если ни на хостах «А» и «Б», ни на маршрути-заторе не обнаружена подмена MAC-адресов;
3(z) – передача ЭД с хоста «Б» на маршрутизатор для хоста «А»;
4(z) – передача маршрутизатором ЭД по подменному MAC—адресу на хост нарушителя или на нужный ему адрес

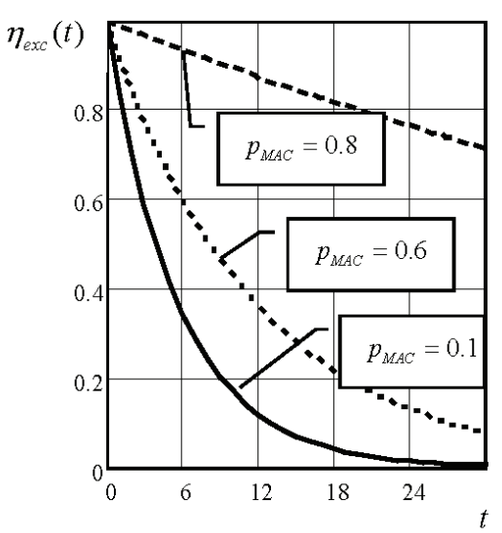


Рис.4. Зависимость эффективности защиты ЭД от времени

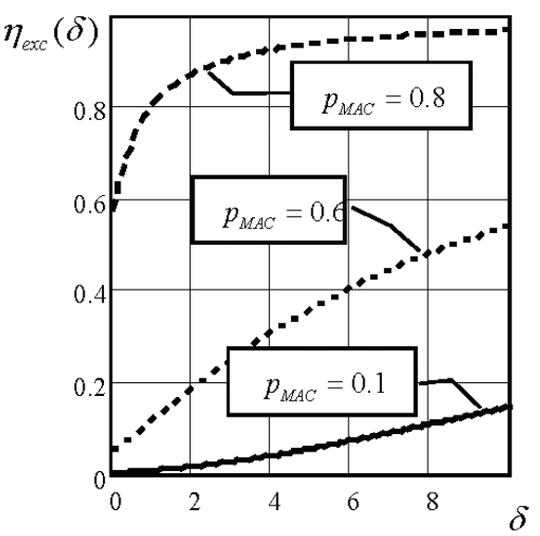


Рис.5. Зависимость эффективности защиты ЭД от вероятности обнаружения подмены MAC-адресов

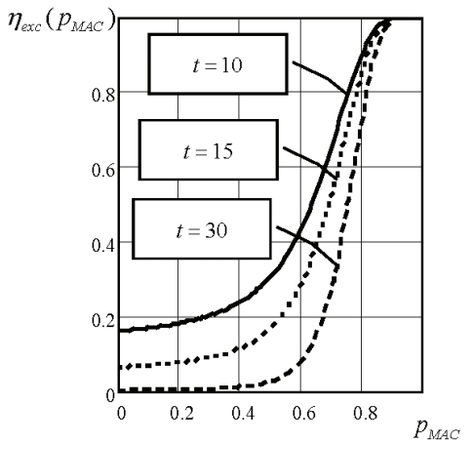


Рис.6. Зависимость эффективности защиты ЭД от со-

отношения $\delta = \dfrac{\overline{\tau_{tr}}}{\tau_{func}}$ *средних времен срабатывания переходов и выполнения функций обработки докумен-та при* $t = 15$ *и* $\tau_{func} = 1$

Выводы

Традиционный, широко применявшийся ранее под-ход к оценке показателей эффек-тивности защиты инфор-мации на основе сравнения возможностей реализации угроз без применения и с применением мер защиты в случае, когда защищаемая информация оста-ется актуальной для пользователей только весьма ограниченное время, оказывается недо-статочным. Именно такая ситуация имеет место в системах электронного докумен-тообо-рота. В этом случае реализация некоторых угроз оказывается возможной лишь относи-тельно устаревших, отработанных документов и не представляет опасности с точки зре-ния нарушения их конфиденциальности, целост-ности или доступности, что приводит к несостоятельности применения традиционно используемых показателей. Предложенный новый показатель оценки, направленный на сравнение вероятностно-временных характе-ристик процессов реализации угроз в СЭД в условиях применения мер защиты и процес-сов обработки электронных документов, впервые позволяет учесть время обработки до-кументов в оценке эффективности их защиты. Для расчета указанного показателя в работе предложен подход к формированию, во-первых, функциональных моделей рассматривае-мых процессов обработки ЭД и реализации угроз безопасности электронного документо-оборота, во-вторых, к построению на их основе математических моделей оценки вероят-ностно-временных характеристик процессов обработки ЭД и реализации угроз с исполь-зованием аппарата сетей Петри-Маркова, что позволяет на количественной основе обос-новывать требования к временным характеристикам функционирования СЭД с позиции решения задач их защиты и к мерам защиты с учетом фактора времени.

Литература:

1. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. – Воронеж: Кварта, 2018. 588 с.
2. Скрыль С.В., Лаврухин Ю.Н., Курило А.П., Багаев Д.А. Обоснование показателей для оценки эффективности информационных процессов в информационно-телекоммуникационных системах в условиях противодействия угрозам информационной безопасности // Информация и безопасность. 2009. №3, с.429 – 432.
3. Авсентьев О.С., Рубцова И.О., Голубков Д.А. Математическая модель показателя защищен-ности информации от несанкционированного доступа в ключевых системах информационной инфраструк-туры / В сборнике: Охрана, безопасность, связь - 2014 материалы международной научно-практической конференции. Воронежский институт МВД России. 2015. С. 18-21
4. Сердечный А.Л. Методическое обеспечение оценивания эффективности ложных информационных систем как средств защиты от несанкционированного доступа. Диссертация на соискание ученой степени кандидата технических наук. Воронежский государственный технический университет. Воронеж, 2014 г.
5. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006, 274 с.: илл.
6. Джоган В.К. Теоретические и организационно-методические основы комплексной оценки защи-щенности информации правоохранительных органов: монография [Текст] / В.К. Джоган, А.П. Курило, Д.Ю. Лиходедов. – Воронеж: Воронежский институт МВД России, 2011. – 88 с.
7. Джоган В.К., Курило А.П. Защищенность информационных ресурсов компьютерных систем как система показателей эффективности защиты информации // Безопасность информационных технологий. 2011. – № 4. С. 164–169.
8. Рубцова, И.О. Показатель безопасности информации в инфокоммуникационных системах спе-циального назначения [Текст] / И.О. Рубцова, Р.Э. Жучков // Охрана, безопасность, связь – 2013: материалы международной научно-практической конференции. Ч. 2. – Воронеж : Воронежский институт МВД России, 2014. – С. 188–191.
9. Скрыль С.В., Сычев А.М., Корчагин В.В., Змеев А.А., Багринцева О.В. Вероятностные модели информационных процессов в интегрированных системах безопасности в условиях обеспечения защиты информации от несанкционированного доступа // Телекоммуникации. 2015. № 6. С. 26–31.
10. Шаньгин, В.Ф. Информационная безопасность. – Москва : ДМК-Пресс, 2014. 702 с.
11. Тихонов В.И., Миронов М.А.. Марковские процессы. М.: Издательство «Советское радио», 1977. 488 с.
12. Гнеденко Б.В.,.Коваленко И.Н. Введение в теорию массового обслуживания. Издание второе, переработанное и дополненное – М.: Издательство «Наука», Главная редакция физико-математической ли-тературы, 1987. 336 с.
13. Иванов Н.Н. Полумарковские процессы во временных стохастических сетях Петри // Автома-тика и телемеханика. 1994. №3. С.117-127.
14. Игнатьев В.М., Ларкин Е.В. Сети Петри-Маркова. Тула: ТулГТУ, 1994. 163 с.
15. Тихонов В.И. Статистическая радиотехника. М.: «Сов. радио», 1966. 678 с.
16. Климов Г.П. Стохастические системы массового обслуживания. – М.: Наука, 1966. 242 с.
17. Тараканов К.В., Овчаров Л.А., Тырышкин А.Н. Аналитические методы исследований систем. М.: Изд-во «Сов радио». 1974. 240 с.
18. Рубцова И.О., Авсентьев О.С. Обобщенное представление информационных процессов в си-стемах электронного документооборота

специального назначения в условиях угроз безопасности информа-ции // Вестник Воронежского института МВД России. 2017. № 4. С. 108–115.
19. Авсентьев, О.С. Функциональные модели действий по несанкционированному доступу к ин-формации и ее защите в автоматизированных информационных системах персональных данных органов государственного управления // Вестник Воронежского института МВД России. 2014. № 4. С. 282–289.
20. Авсентьев О.С., Жучков Р.Э. Функциональные модели действий по несанкционированному до-ступу к информации и ее защите в автоматизированных информационных системах персональных данных органов государственного управления // Вестник Воронежского института МВД России. 2014. № 4. С. 282–289.
21. Язов Ю.К., Текунов В.В. Моделирование динамики реализации угроз безопасности информа-ции с использованием аппарата сетей Петри-Маркова // Информация и безопасность. 2018. Том 17, вып.3. С. 464 – 467.

Рецензент: *Марков Алексей Сергеевич, доктор технических наук, профессор кафедры «Информаци-онная безопасность» МГТУ им. Н.Э. Баумана, г. Москва, Россия. E-mail: a.markov@npo-echelon.ru*

ON THE EVALUATION OF THE EFFECTIVENESS INFORMATION PROTECTION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Yazov Yu. K.[7], Avsentyev O. S.[8], Rubtsova I.O.[9]

Objective of the article: *development of protection efficiency evaluation mathematical model against integrity violation threats, availability and confidentiality of electronic documents in the limited duration of their life cycle in the electronic document management systems.*

Method: *mathematical modeling of electronic document management processes and im-plementation of information security threats using the Petri-Markov network apparatus, which allows to take into account the logical conditions that determine the possibility of performing the processes under consideration, their random nature, the presence of branching, and parallel ex-ecution of the procedures and functions that make up these processes.*

Obtained result: *a new electronic documents protection efficiency evaluation indicator, aimed at comparing the probabilistic-temporal characteristics of the processes of implementa-tion of threats in electronic document management systems in the conditions of application of protection measures and processes of electronic documents processing, which for the first time allows to take into account the documents processing time in their protection efficiency evalua-tion is proposed. The mathematical model is developed on the basis of Petri-Markov network apparatus and analytical relations are obtained for calculating the proposed indicator on the example of the life cycle of incoming electronic documents, taking into account the time of exe-cution of standard procedures and functions of their processing, the time of implementation of threats, like unauthorized replacement of computers network adapters physical addresses as part of the electronic document management system, as well as the use of security measures – the use of special programs to detect the facts of physical addresses substitution. The developed model allows not only to assess the effectiveness of measures taken to protect electronic documents from specific threats, but also to justify on a quantitative basis the requirements for electronic documents processing time, depending on the probabilistic-temporal characteristics of threats implementation, to identify weaknesses in electronic document management systems that can be used to implement threats, and the conditions under which such threats can be implemented.*

Keywords: *efficiency indicator, functional model, Petri-Markov network, security threat, protection measure.*

References

1. Iazov Iu.K., Solov`ev S.V. Organizatciia zashchity` informatcii v informatcionny`kh sistemakh ot nesanktcionirovannogo dostupa. Monografiia. – Voronezh: Kvarta, 2018. 588 s.
2. Skry`l` S.V., Lavruhin Iu.N., Kurilo A.P., Bagaev D.A. Obosnovanie pokazatelei` dlia ocenki e`ffektivnosti informatcionny`kh protcessov v informatcionno-telekommunikatcionny`kh sistemakh v usloviiakh protivodei`stviia ugrozam informatcionnoi` bezopasnosti // Informatciia i bezopasnost`. 2009. №3, s.429 – 432.
3. Avsent`ev O.S., Rubtcova I.O., Golubkov D.A. Matematicheskaia model` pokazatelia zash-chishchen-nosti informatcii ot nesanktcionirovannogo dostupa v cliuchevy`kh sistemakh informatcionnoi` infra-struk-tury` / V sbornike: Okhrana, bezopasnost`, sviaz` - 2014 materialy` mezhdunarodnoi` nauchno-prakticheskoi` konferentcii. Voronezhskii` institut MVD Rossii. 2015. S. 18-21.
4. Serdechny`i` A.L. Metodicheskoe obespechenie ocenivaniia e`ffektivnosti lozhny`kh in-formatcionny`kh sistem kak sredstv zashchity`

7 Yuriy Yazov, Dr.Sc. (in Tech.), Professor, Chief Researcher, Federal Service for Technical and Export Control, Voronezh, Russia. E-mail: Yazoff_1946@mail.ru
8 Avsentyev Oleg, Dr.Sc. (in Tech.), Professor, Department of Information Security, Voronezh Institute of the Ministry of the Interior of the Russian Federation, Voronezh, Russia. E-mail: osaos@mail.ru
9 Irina Rubtsova, postgraduate, Department of organization and technology of information security, Bel-gorod University of Cooperation, Economics and Law, Belgorod, Russia. E-mail: kaf-otzi-zav@bukep.ru

ot nesanktcionirovannogo dostupa. Dissertatciia na soiskanie uchenoi` stepeni kandidata tekhnicheskikh nauk. Voronezhskii` gosudarstvenny`i` tekhnicheskii` universitet. Voro-nezh, 2014 g.
5. Iazov Iu.K. Osnovy` metodologii kolichestvennoi` ocenki e`ffektivnosti zashchity` informatcii v komp`iuterny`kh sistemakh. Rostov-na-Donu: Izd-vo SKNTC VSh, 2006, 274 s.: ill.
6. Joegan B.K. Teoreticheskie i organizatcionno-metodicheskie osnovy` kompleksnoi` ocenki za-shchishchennosti informatcii pravookhranitel`ny`kh organov: monografiia [Tekst] / B.K. Joegan, A.P. Kurilo, D.Iu. Leehodedov. Voronezh: Voronezhskii` institut MVD Rossii, 2011. 88 s.
7. Joegan B.K., Kurilo A.P. Zashchishchennost` informatcionny`kh resursov komp`iuterny`kh sistem kak sistema pokazatelei` e`ffektivnosti zashchity` informatcii // Bezopasnost` informatcionny`kh tekhnologii`. 2011. – № 4. S. 164–169.
8. Rubtcova, I.O. Pokazatel` bezopasnosti informatcii v infokommunikatcionny`kh sistemakh spe-tcial`nogo naznacheniia [Tekst] / I.O. Rubtcova, R.E`. Zhuchkov // Okhrana, bezopasnost`, sviaz` – 2013: materialy` mezhdunarodnoi` nauchno-prakticheskoi` konferentcii. Ch. 2. Voronezh : Voronezhskii` institut MVD Rossii, 2014. S. 188–191.
9. Skry`l` S.V., Sy`chev A.M., Korchagin V.V., Zmeev A.A., Bagrintceva O.V. Veroiatnostny`e modeli informatcionny`kh protcessov v integrirovanny`kh sistemakh bezopasnosti v usloviiakh obespecheniia zash-chity` informatcii ot nesanktcionirovannogo dostupa // Telekommunikatcii. 2015. № 6. S. 26–31.
10. Shan`gin, V.F. Informatcionnaia bezopasnost`. – Moskva : DMK-Press, 2014. 702 s.
11. Tihonov V.I., Mironov M.A.. Markovskie protcessy`. M.: Izdatel`stvo «Sovetskoe radio», 1977. 488 s.
12. Gnedenko B.V.,.Kovalenko I.N. Vvedenie v teoriiu massovogo obsluzhivaniia. Izdanie vtoroe, pererabotannoe i dopolnennoe – M.: Izdatel`stvo «Nauka», Glavnaia redaktciia fiziko-matematicheskoi` li-teratury`, 1987. 336 s.
13. Ivanov N.N. Polumarkovskie protcessy` vo vremenny`kh stohasticheskikh setiakh Petri // Avtoma-tika i telemehanika. 1994. №3. S.117-127.
14. Ignat`ev V.M., Larkin E.V. Seti Petri-Markova. Tula: TulGTU, 1994. 163 s.
15. Tihonov V.I. Statisticheskaia radiotekhnika. M.: «Sov. radio», 1966. 678 s.
16. Climov G.P. Stohasticheskie sistemy` massovogo obsluzhivaniia. – M.: Nauka, 1966. 242 s.
17. Tarakanov K.V., Ovcharov L.A., Ty`ry`shkin A.N. Analiticheskie metody` issledovanii` sistem. M.: Izd-vo «Sov radio». 1974. 240 s.
18. Rubtcova I.O., Avsent`ev O.S. Obobshchennoe predstavlenie informatcionny`kh protcessov v siste-makh e`lektronnogo dokumentooborota spetcial`nogo naznacheniia v usloviiakh ugroz bezopasnosti in-formatcii // Vestneyk Voronezhskogo instituta MVD Rossii. 2017. № 4. S. 108–115.
19. Avsent`ev, O.S. Funktcional`ny`e modeli dei`stvii` po nesanktcionirovannomu dostupu k in-formatcii i ee zashchite v avtomatizirovanny`kh informatcionny`kh sistemakh personal`ny`kh danny`kh organov gosudarstvennogo upravleniia // Vestneyk Voronezhskogo instituta MVD Rossii. 2014. № 4. S. 282–289.
20. Avsent`ev O.S., Zhuchkov R.E`. Funktcional`ny`e modeli dei`stvii` po nesanktcionirovannomu do-stupu k informatcii i ee zashchite v avtomatizirovanny`kh informatcionny`kh sistemakh personal`ny`kh danny`kh organov gosudarstvennogo upravleniia // Vestneyk Voronezhskogo instituta MVD Rossii. 2014. № 4. S. 282–289.
21. Iazov Iu.K., Tekunov V.V. Modelirovanie dinamiki realizatcii ugroz bezopasnosti informa-tcii s ispol`zovaniem apparata setei` Petri-Markova // Informatciia i bezopasnost`. 2018. Tom 17, vy`p.3. S. 464 – 467.