УДК 621.3 **DOI** 10.15622/sp.2019.18.6.1269-1300

Ю.К. Язов, О.С. Авсентьев, А.О. Авсентьев, И.О. Рубцова

МЕТОД ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ПРИМЕНЕНИЕМ АППАРАТА СЕТЕЙ ПЕТРИ — МАРКОВА

Язов Ю.К., Авсентьев О.С., Авсентьев А.О., Рубцова И.О. **Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри — Маркова.**

Аннотация. Традиционные подходы к оцениванию эффективности защиты информации, основанные на сравнении возможностей реализации угроз безопасности информации в условиях отсутствия и применения мер защиты, не позволяют анализировать динамику пресечения мерами защиты процессов реализации угроз. Предложен новый показатель эффективности защиты электронных документов, позволяющий оценивать возможности опережения мерами защиты процесса реализации угроз в системах электронного документооборота и учитывающий вероятностно-временные характеристики динамики применения мер защиты и реализации угроз электронным документам. Разработаны с использованием аппарата сетей Петри — Маркова математические модели и получены аналитические соотношения для расчета предложенного показателя на примере реализации угрозы «туннелирования трафика» (размещение пакетов нарушителя в пакетах доверенного пользователя) и несанкционированного доступа (сетевых атак) к электронным документам, а также угрозы внедрения вредоносной программы путем проведения атаки «неслепой IP-спуфинг» (подмены сетевого адреса). Приведены примеры расчета предложенного показателя и графики его зависимости от вероятности обнаружения сетевых атак системой обнаружения вторжений и от вероятности обнаружения вредоносных программ системой антивирусной защиты. Получены количественные зависимости эффективности защиты электронных документов за счет опережения мерами защиты процессов реализации угроз как от вероятности обнаружения вторжения или вероятности обнаружения вредоносной программы, так и от соотношения времени, затрачиваемого системой защиты на обнаружение попытки реализации угрозы и принятие мер по пресечению процесса ее реализации, и времени реализации угрозы. Модели позволяют не только оценивать эффективность мер защиты электронных документов от угроз уничтожения, копирования, несанкционированных изменений и тому подобное, но и количественно обосновывать требования к времени реакции адаптивных систем защиты на обнаруживаемые действия, направленные на нарушение безопасности электронных документов, а также выявлять слабые места в системах защиты, связанные с динамикой реализации угроз и реакцией на такие угрозы систем защиты электронного документооборота.

Ключевые слова: показатель эффективности, структурно-функциональная модель, сеть Петри — Маркова, система электронного документооборота, угроза безопасности, мера защиты, вероятность обнаружения, система обнаружения вторжений, система антивирусной защиты.

1. Введение. Необходимость оценивания эффективности защиты информации (ЗИ) в информационных системах (ИС) отмечается в целом ряде документов федерального уровня. Так, в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646,

указано, что «планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности» являются «задачами государственных органов…». Вместе с тем в настоящее время методики оценивания эффективности ЗИ (или обеспечения безопасности информации) в практическом плане остаются неразвитыми. Это относится и к ИС с системами электронного документооборота (СЭД). Сегодня действия, направленные на копирование и несанкционированное распространение, подделку (модификацию), уничтожение электронных документов (ЭД) в ИС с СЭД, внедрение вредоносных программ (ВП) с целью выполнения таких действий и так далее, становятся важными составляющими информационного противоборства и обусловливают принятие эффективных мер защиты.

В теоретическом плане во многих научных публикациях предлагались весьма разноплановые подходы к оцениванию эффективности ЗИ.

Так, в [1] для оценивания эффективности защиты от отдельных угроз предлагалось в качестве показателя использовать вероятность того, что в условиях применения мер защиты угроза безопасности информации не будет реализована; в [2, 3] были разработаны аналитические модели и методики расчета этой вероятности для различных ИС и угроз. В основе указанных моделей лежит теория риска, понимаемого как произведение вероятности нанесения ущерба определенного уровня (или среднего ущерба) на вероятность реализации угрозы, которая приводит к этому ущербу [4]. При этом, как правило, ущерб от реализации угрозы полагается неприемлемым, и риск понимается только как риск реализации угрозы. Это обусловлено тем, что аналитические методы оценивания ущерба от реализации угроз безопасности информации пока недостаточно развиты.

Указанные показатели используются в интересах выработки решений по управлению рисками [5], при риск-ориентированном выборе мер контроля защищенности информации в ИС [6], при управлении рисками для системно-связанных объектов [7], для оценивания защищенности информации в ИС, построенных на основе «облачных технологий» [8], и так далее.

Вместе с тем разрабатывались и иные подходы. Так, в [9] оценивание эффективности, понимаемой как «степень соответствия результатов защиты информации цели защиты информации», предложено проводить с применением абсолютного, относительного и относительно-разностного показателей, которые рассчитываются путем сравнения вероятностей реализации угроз без мер защиты и в условиях применения мер защиты. Кроме того, наряду с указанными

показателями, рассчитываемыми аналитическими методами, для оценивания эффективности защиты информации в ИС как в России, так и за рубежом использовались и качественные показатели, например при функциональном подходе, который основан на сравнении состава реализуемых мер защиты с составом, заданным нормативными документами [9]; или при подходе, который основан на введении оценочных уровней доверия в соответствии с идеологией международного стандарта ИСО/ МЭК 15408. Широкое применение на практике также нашел подход, реализующий балльный метод, суть которого состоит в экспертной оценке риска реализации угрозы по баллам, определяемым по заранее введенным шкалам. Этот подход используется сегодня в целом ряде программных продуктов, таких как инструментарий стандарта ISO 17799 (стандарт по информационной безопасности, опубликованный в 2005 г. организациями ISO и IEC, в 2013 г. сменил название на ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью»), например, программный продукт COBRA или программный продукт, реализующий метод CRAMM (Central Computer and Telecommunications Agency. Risk Analysis & Management Method — Центральное агентство по компьютерам и телекоммуникациям Великобритании. Метод анализа и контроля рисков), программный продукт RiskWatch и другие. Вместе с тем применение оцениваемых экспертным методом качественных показателей эффективности, в том числе с использованием балльного метода, приводит не только к неполной, но и зачастую к некорректной оценке, поскольку в них практически не учитывается фактор времени, большое разнообразие способов реализации угроз, применяемых мер защиты и так далее.

С учетом изложенного все большее внимание в последнее время уделяется количественным методам оценивания эффективности ЗИ. При этом в качестве цели ЗИ, как правило, рассматривается парирование всех выявленных актуальных угроз безопасности информации, а в качестве показателей используются или вероятностные показатели, или среднестатистические показатели возможностей парирования угроз. Так как рассматриваемые процессы реализации угроз являются случайными, для их аналитического моделирования используется теория случайных процессов, вероятностно-временные характеристики которых определяются с использованием аппарата марковских или полумарковских процессов [10].

Вместе с тем моделирующие возможности указанных аппаратов весьма ограничены и не позволяют учесть важные факторы, которые

определяют динамику реализации многих угроз безопасности информации в информационных системах. Так, в виде марковских моделей невозможно представить разветвленные процессы, характерные для реализации большинства угроз безопасности информации в ИС, и тем более учесть логические условия, которые вводятся для обеспечения адекватности моделей рассматриваемым процессам. Полумарковские модели позволяют представлять процессы разветвленными и анализировать динамику их выполнения, то есть оценивать количественно время выполнения процесса, однако только в том случае, если в нем отсутствуют логические условия его выполнения.

Логику протекания процесса реализации угроз можно представить сетью Петри [11], однако аналитически учитывать временной фактор в моделях, разработанных на основе этого аппарата, практически невозможно. Сегодня аппарат сетей Петри (Е-сети, временные сети Петри и т.д.) применяют для весьма затратного по времени имитационного моделирования. В [12] в интересах реализации требования стандарта функциональной безопасности IEC 61508 предложено использовать для оценивания достигаемой безопасности защищаемой системы при случайных отказах оборудования методы многофазных сетей Маркова и стохастических сетей Петри с предикатами; а в [13] для моделирования и анализа производительности системы аварийно-спасательной логистики — сочетание сетей Петри с марковскими процессами с выводом линейных уравнений для количественного анализа основных показателей эффективности системы. В [14] объединение стохастических сетей Петри с описанием динамики их срабатывания с применением аппарата марковских процессов позволило связать определяемый сетью Петри порядок выполнения моделируемого процесса со случайным временем выполнения парциальных процедур, составляющих этот процесс. Однако предложенные подходы крайне сложно или невозможно применять, когда одновременно нужно учитывать логические условия выполнения моделируемых процессов, их разветвленность, параллельность и время выполнения, что характерно было и для традиционного аппарата марковских и полумарковских процессов.

Для устранения указанных недостатков марковских и полумарковских моделей в [15] был предложен аппарат сетей Петри — Маркова, позволяющий в отличие от сетей Петри аналитически рассчитывать показатели эффективности защиты информации в ИС с учетом фактора времени, а в отличие от аппарата марковских и полумарковских процессов — наряду с разветвленностью моделируемых процессов и параллельностью выполнения во времени

составляющих эти процессы процедур учитывать влияние логических условий на динамику протекания процессов реализации угроз. При этом при помощи сетей Петри — Маркова могут быть получены аналитические соотношения для расчета времени выполнения процесса и указанных выше вероятностных показателей оценки эффективности, рассчитываемых путем сравнения возможностей реализации угроз в условиях отсутствия и применения выбранных мер защиты.

Однако этими показателями оценивается «итоговый эффект» защиты, и они весьма опосредованно учитывают время реакции систем защиты на попытки реализации угроз. В условиях, когда применяются системы адаптивной защиты, к которым относятся, например, системы обнаружения вторжений (СОВ), системы антивирусной защиты (САВЗ), DLP-системы (Data Loss Prevention, системы блокирования попыток несанкционированной передачи данных во внешние сети [16]) и SIEM-системы (объединяют в своем названии аббревиатуры двух терминов: SIM — Security information management, управление информационной безопасностью, и SEM, управление событиями безопасности [17-19]) и так далее, необходимо анализировать зависимости эффективности защиты от времени реакции этих систем на попытки реализации угроз, указанные показатели оказываются мало приемлемыми.

В данной статье предлагается иной подход к оцениванию эффективности ЗИ в ИС с СЭД, основанный на показателях возможности опережения мерами защиты процесса реализации угроз электронному документообороту.

2. Показатели оценки эффективности защиты электронных документов в СЭД на основе определения возможности опережения мерами защиты процесса реализации угроз электронному документообороту. Возможности опережения мерами защиты процесса реализации угрозы электронному документообороту предлагается оценивать вероятностью того, что суммарное время обнаружения факта реализации угрозы и принятия адекватных действий по ее парированию будет меньше времени проникновения в операционную среду СЭД СН до момента начала выполнения несанкционированного действия. Такое опережение оценивается в том случае, когда меры защиты выбираются и применяются в ходе функционирования СЭД СН в зависимости от содержания действий нарушителя или выполняемых функций иного источника угрозы (например, программной закладки, ВП и т.п.), то есть при применении адаптивных мер защиты информации. Применительно к упомянутым мерам защиты ниже приводятся математические модели расчета указанного показателя оценки эффективности защиты электронного документооборота.

Так как реализация большинства угроз и применения мер защиты возможна при выполнении ряда логических условий, а сами процессы реализации, как правило, являются разветвленными и разделяются на параллельно выполняемые подпроцессы, то для построения математических моделей использовался аппарат сетей Петри — Маркова. Ниже такие модели рассматриваются применительно к системам обнаружения вторжений и антивирусной защиты.

Особенность таких моделей заключается в том, что с их использованием оценивается время $\tau_{res.u} = \tau_{det.u} + \tau_{rep.u}$, необходимое СОВ для обнаружения факта вторжения или САВЗ для обнаружения ВП ($\tau_{det.u}$) и пресечения возможности выполнения несанкционированного действия при попытке реализации u-й угрозы ($\tau_{rep.u}$).

Длительность реализации угрозы составляет случайную величину τ_u, включающую в себя продолжительность τ_0 этапа, который предваряет начало функционирования СОВ (или САВЗ), распаковки пакета (или пакетов).

Обозначим разницу $\tau_u - \tau_0$ как $\tau_u^{(0)}$.

Пусть плотности распределения вероятностей величин $\tau_{res.u}$ и $\tau_u^{(0)}$ равны $w_{res}(\tau_{res.u})$ и $w_u(\tau_u^{(0)})$ соответственно.

Угроза не будет реализована, если $\tau_u^{(0)} > \tau_{res.u}$.

Так как рассматриваемые случайные величины являются независимыми, то в соответствии с [20] плотность распределения вероятностей случайной величины $y = \tau_u^{(0)} - \tau_{res.u}$ определяется из соотношения:

$$w_{exc}(y) = \int_0^\infty w_u(y + \tau_{res.u}) \cdot w_{res}(\tau_{res.u}) \cdot d\tau_{res.u}. \qquad (1)$$

Тогда вероятность того, что текущее время реализации угрозы в каждой попытке такой реализации будет превышать время принятия адекватных мер защиты, определяется из соотношения:

$$p_{exc}(\tau_u^{(0)} - \tau_{res.u} > 0) = \int_0^\infty w_{exe}(y) \cdot dy, \qquad (2)$$

а среднее время реализации угрозы $\overline{\tau_u^{(ЗИ)}}$ с учетом [21, 22] — величину:

$$\overline{\tau_u^{(ЗИ)}} = \overline{\tau_0} + \frac{\overline{\tau_u^0}}{1 - p_{exc}(\tau_u^{(0)} - \tau_{res.u})}, \quad (3)$$

где $\overline{\tau_0}$ и $\overline{\tau_u^{(0)}}$ — математические ожидания величин τ_0 и $\tau_u^{(0)}$ соответственно.

В соответствии с формулой (3) происходит вероятностное прореживание исходного потока событий, описывающего процесс реализации u -й угрозы.

В [21, 22] показано, что для получаемого путем прореживания с вероятностью p потока характеристическая функция $\chi_*(s)$ для интервала времени между соседними событиями в прореженном потоке имеет вид:

$$\chi_*(s) = \frac{p \cdot \chi(s)}{1 - (1-p) \cdot \chi(s)}, \quad (4)$$

где $\chi(s)$ — характеристическая функция для интервала времени между соседними событиями в исходном потоке.

В качестве меры близости потока к пуассоновскому можно использовать коэффициент вариации, определяемый как отношение среднеквадратического отклонения паузы θ между событиями в потоке к его математическому ожиданию:

$$K_{\text{var}} = \frac{\sigma_\theta}{M_\theta} = \frac{\sqrt{\chi''(s) - (\chi'(s))^2}}{\chi'(s)}\Big|_{s=0}, \quad (5)$$

где $\chi'(s)$ и $\chi''(s)$ — первая и вторая производные от характеристической функции $\chi(s)$.

При этом крайними случаями являются детерминированный периодический поток, для которого $K_{\text{var}} = 0$, и пуассоновский поток, для которого $K_{\text{var}} = 1$.

Коэффициент вариации для прореженного с вероятностью p потока K_{var}^* рассчитывается по формуле, аналогичной формуле (5), где вместо характеристической функции исходного потока $\chi(s)$ используется характеристическая функция прореженного потока $\chi_*(s)$, которая определяется по формуле (4).

С учетом изложенного коэффициент вариации для прореженного потока K^*_{var} связывается с коэффициентом вариации исходного потока K_{var} соотношением:

$$K^*_{\text{var}} = \frac{\sqrt{\chi^{''}_*(s) - (\chi^{'}_*(s))^2}}{\chi^{'}_*(s)}\Big|_{s=0} = \sqrt{K_{\text{var}} \cdot p + 1 - p}, \qquad (6)$$

представленном в виде графической зависимости на рисунке 1. Из рисунка 1 видно, что с уменьшением вероятности прореживания результирующий поток быстро приближается к пуассоновскому.

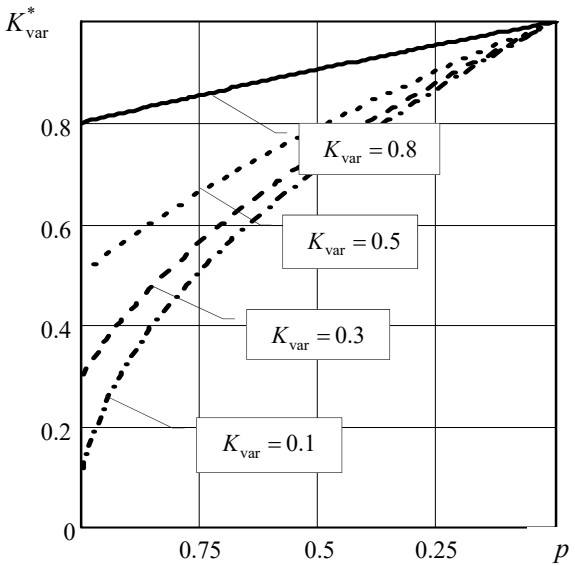

Рис. 1. Зависимость коэффициента вариации прореженного потока от вероятности прореживания и коэффициента вариации исходного потока

При этом даже при вероятности прореживания менее 0.3 для большинства имеющих место на практике потоков ошибка с заменой любой одномодальной плотности распределения на экспоненциальную составляет единицы процентов. Это некритично для результатов оценивания и обусловливает возможность при моделировании процессов, в которых имеет место то или иное вероятностное прореживание исходного потока, использовать только экспоненциальный вид распределения без заметных отклонений в оценках характеристик прореженных потоков.

Представляя плотности распределения $w_{res}(\tau_{res.u})$ и $w_u(\tau_u^{(0)})$ в виде экспонент, нетрудно получить из формул (1) и (2) зависимость:

$$p_{exc}(\tau_u^{(0)} - \tau_{res.u} > 0) = \frac{\overline{\tau_u^{(0)}}}{\overline{\tau_{res.u}} + \overline{\tau_u^{(0)}}}, \tag{7}$$

где $\overline{\tau_{res.u}}$ — среднее время реакции системы защиты на попытку реализации u-й угрозы,

$$\overline{\tau_{res.u}} = \frac{\overline{\tau_{det.u}}}{P_{det.u}} + \frac{\overline{\tau_{rep.u}}}{P_{rep.u}}, \overline{\tau_{det.u}} > 0, \tag{8}$$

P_{det} и P_{rep} — вероятности обнаружения и пресечения процесса реализации u-й угрозы.

С учетом соотношения (8) формула (7) преобразуется к виду:

$$p_{exc.u}(\tau_u^{(0)} - \tau_{res.u} > 0) = \frac{1}{\frac{\overline{\tau_{det}}}{\overline{\tau_u^{(0)}} \cdot P_{det.u}} + \frac{\overline{\tau_{rep.u}}}{\overline{\tau_u^{(0)}} \cdot P_{rep.u}} + 1}. \tag{9}$$

Как правило, если процесс реализации угрозы обнаружен, то пресечение происходит с вероятностью, близкой к единице, то есть $P_{rep.u} \approx 1$. Тогда:

$$\overline{\tau_{res.u}} = \frac{\overline{\tau_{det.u}}}{P_{det.u}} + \overline{\tau_{rep.u}}; \tag{10}$$

$$p_{exc.u}(\tau_u^{(0)} - \tau_{res.u} > 0) = \frac{1}{\frac{\overline{\tau_{det}}}{\overline{\tau_u^{(0)}} \cdot P_{det.u}} + \frac{\overline{\tau_{rep.u}}}{\overline{\tau_u^{(0)}}} + 1}. \tag{11}$$

Вероятность опережения мерой защиты процесса реализации угрозы может быть использована в качестве частного показателя эффективности защиты ЭД. На рисунке 2 в графическом виде

приведена зависимость данного показателя от вероятности обнаружения при различных отношениях $\frac{\overline{\tau_{det.u}}}{\overline{\tau_u^{(0)}}}$ и $\frac{\overline{\tau_{rep.u}}}{\overline{\tau_u^{(0)}}}$.

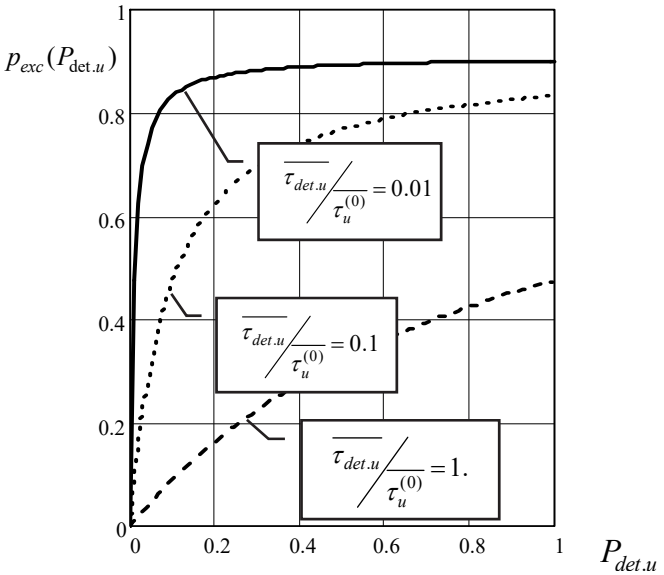

Рис. 2. Зависимость вероятности опережения процесса реализации угрозы мерой защиты

Приведенный показатель позволяет учитывать влияние времени реакции системы защиты на процесс реализации угрозы. Вместе с тем даже при очень высокой эффективности защиты, оцененной по данному показателю, в силу статистического характера процесса реализации угрозы всегда существует вероятность того, что угроза за некоторое конечное время t будет реализована. В связи с этим в качестве основного показателя эффективности защиты ЭД целесообразно использовать вероятность того, что угроза за заданное время не будет реализована. Эта вероятность рассчитывается по формуле:

$$\eta_{exc.u}(t) = \exp\left\{-\frac{t \cdot p_{exc.u}(\overline{\tau_u^{(0)}} - \overline{\tau_{res.u}} > 0)}{\overline{\tau_u^{(0)}}}\right\} = \exp(-\frac{t}{\overline{\tau_0} + \overline{\tau_u^{(0)}} + \overline{\tau_{res.u}}}). \quad (12)$$

Если необходимо оценить эффективность защиты электронного документооборота в СЭД СН на основе определения возможности

опережения мерами защиты процесса реализации совокупности угроз, то показатель эффективности рассчитывается следующим образом.

Пусть имеется множество U угроз, которые могут быть реализованы в СЭД СН за время t независимо друг от друга относительно как отдельных документов, так и СЭД СН в целом. Для парирования каждой u-й угрозы применяется соответствующая мера защиты, при этом мера защиты должна опередить процесс реализации угрозы.

Тогда показатель эффективности совокупности применяемых мер защиты рассчитывается по формуле:

$$\eta_{exc}^{(U)}(t)=\prod_{u=1}^{U}\exp\left(-\frac{t}{\overline{\tau_u}\cdot\left(1+\frac{\overline{\tau_{res.u}}}{\tau_u}\right)}\right)=\exp\left\{-t\cdot\sum_{u=1}^{U}\left(\frac{1}{\overline{\tau_u}\cdot\left(1+\frac{\overline{\tau_{res.u}}}{\tau_u}\right)}\right)\right\}. \quad (13)$$

Для расчета предложенных показателей необходимо моделирование процесса реализации каждой угрозы с использованием аппарата сетей Петри — Маркова.

3. Структурно-функциональная модель и сети Петри — Маркова, моделирующие процессы реализации угроз электронному документообороту в условиях применения мер защиты. В интересах формирования сетей Петри — Маркова разрабатывались структурно-функциональные модели процессов реализации угроз [23]. Структурно-функциональная модель отражает содержание, взаимосвязь и последовательность выполнения процедур и функций в процессе реализации угрозы в течение всего цикла обработки ЭД [24] и реакцию системы защиты на попытку реализации угрозы.

На рисунке 3 для примера приведена структурно-функциональная модель реализации угрозы сетевой атаки туннелирования трафика в условиях применения СОВ, а на рисунке 4 — угрозы внедрении ВП путем проведения атаки «неслепой IP-спуфинг» в условиях применения САВЗ.

Обозначение и содержание функций, выполняемых в ходе реализации указанных угроз приведены в таблице 1.

На основе этих моделей формировались соответствующие сети Петри — Маркова, моделирующие во времени процессы реализации угроз. Графы сетей Петри — Маркова для указанных выше угроз приведены на рисунках 5 и 6 соответственно, а обозначение и описание позиций и переходов сетей Петри — Маркова для обеих атак приведены в таблице 2.

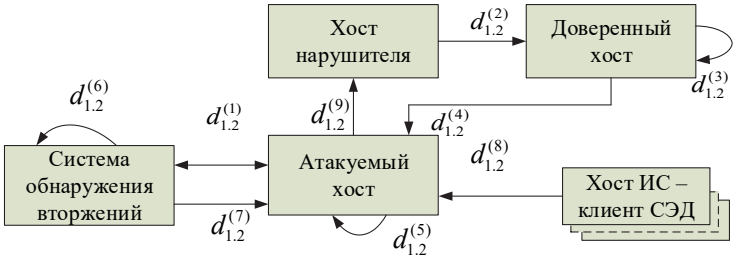

Рис. 3. Структурно-функциональная модель процесса реализации угрозы сетевой атаки с внедрением ВП по сети, реализуемой путем «туннелирования» трафика с использованием протоколов IP или ICMP

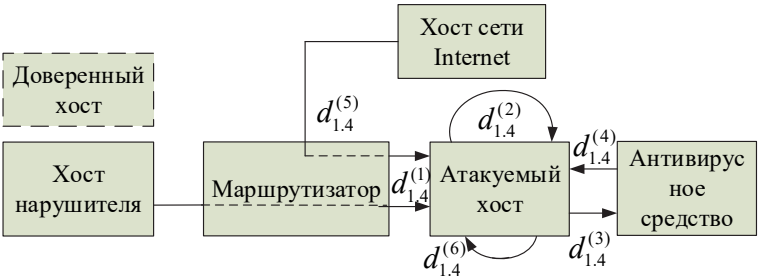

Рис. 4. Структурно-функциональная модель процесса реализации угрозы сетевой атаки с внедрением ВП от имени доверенного хоста путем подмены сетевого адреса в интересах перехвата трафика («неслепой IP-спуффинг») в условиях применения САВЗ

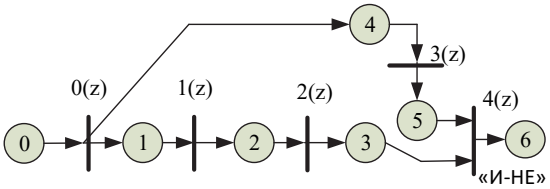

Рис. 5. Сеть Петри – Маркова, моделирующая процесс реализации угрозы сетевой атаки с внедрением ВП путем «туннелирования» трафика с использованием протоколов IP или ICMP в условиях применения СОВ

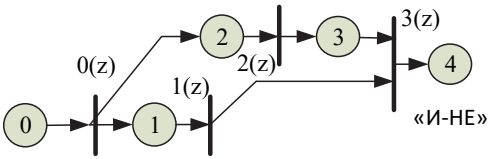

Рис. 6. Сеть Петри – Маркова, моделирующая процесс реализации угрозы внедрения ВП от имени доверенного хоста с подменой сетевого адреса в интересах перехвата трафика («неслепой IP-спуффинг») в условиях применения САВЗ

Таблица 1. Обозначения и содержание функций, выполняемых при реализации угроз туннелирования трафика и проведения атаки «неслепой IP-спуфинг»

Наименование атаки	Содержание функций, выполняемых при реализации угрозы сетевой атаки	Обозначение функции
Сетевая атака туннелирования трафика в условиях применения СОВ	СОВ анализирует входящий трафик на наличие подозрительных команд, ВП и т.п. (по сигнатурам или по аномалиям)	$d_1^{(1)}$
	Инкапсуляция пакетов хоста нарушителя в пакеты, передаваемые на хост, который является доверенным для атакуемого хоста, передача пакетов на доверенный хост	$d_1^{(2)}$
	Распаковка пакета сообщения с хоста нарушителя, обнаружение в поле данных инкапсулированного пакета для атакуемого хоста, в полях адресов которого указан сетевой адрес получателя – атакуемого хоста и адрес отправителя – доверенного хоста, а в поле данных – скрипт, специальная программа-шпион (типа «сниффер», программа наблюдения за операционной средой атакуемого хоста типа Real SPY Monitor и др.)	$d_1^{(3)}$
	Отправка выявленного пакета по адресу атакуемого хоста	$d_1^{(4)}$
	Распаковка полученного пакета и запуск ВП	$d_1^{(5)}$
	СОВ обнаруживает вторжение (вредоносную программу), оповещает пользователя и подготавливает команду на блокирование действий по выполнению программы	$d_1^{(6)}$
	СОВ направляет команду на блокирование действий по выполнению ВП	$d_1^{(7)}$
	Один из хостов ИС-клиентов СЭД направляет ЭД для атакованного хост	$d_1^{(8)}$
	Перехваченный ЭД направляется на хост нарушителя	$d_1^{(9)}$

Продолжение таблицы 1.

Сетевая атаки «неслепой IP-спуфинг» с внедрением вредоносной программы	С хоста нарушителя по протоколу UDP (без установления виртуального канала) от имени доверенного хоста посылается сообщение с ВП через маршрутизатор на атакуемый хост	$d_2^{(1)}$
	Атакуемый хост принимает пакет от «доверенного хоста», распаковывает его. При этом вложенная в него ВП, например, предназначена для уничтожения файлов с ЭД с расширением *.doc и *.docx. ВП запускается операционной системой и готова к поиску документов	$d_2^{(2)}$
	Антивирусное средство просматривает файловую систему хоста на предмет обнаружения ВП, по ее сигнатуре или по аномалиям, режим работы сетевой карты на предмет выявления ВП или следов ее функционирования	$d_2^{(3)}$
	Антивирусное средство обнаруживает и блокирует ВП	$d_2^{(4)}$
	ЭД высылается на атакуемый хост доверенным хостом сети Internet	$d_2^{(5)}$
	ВП на атакуемом хосте обнаруживает появившийся на хосте ЭД и уничтожает его.	$d_2^{(6)}$

При этом учитывалось следующее.

Каждая сеть Петри — Маркова имеет в своем составе набор позиций (на графе обозначены кружочками с номерами 0(a), 1(a) и т.д.) и набор переходов (на графе обозначены жирными линиями с номерами 0(z), 1(z) и т.д.), включающий в себя простые переходы и логические переходы. Позиции и переходы соединены дугами со стрелками, указывающими направления перемещения по графу меток, которые обозначают текущее состояние моделируемого процесса. Простые переходы срабатывают при поступлении в них метки от предстоящих состояний, а логические переходы — при поступлении метки и при выполнении заданных логических условий. Для расчета времени срабатывания сети, то есть перемещения моделируемого процесса из начального в конечное состояние, вся сеть разбивается на участки между начальным состоянием до первого логического перехода, между логическими переходами и от последнего логического перехода до последнего логического состояния (рисунок 7).

В общем случае для такого участка в соответствии с [10] необходимо составить систему уравнений:

$$\Phi_{ij}(d,t) = \pi_{ik}(d) \cdot \int_0^t f_{ik}(d,\tau) \cdot \Phi_{kj}(d,t-\tau) \cdot d\tau. \qquad (14)$$

Таблица 2. Обозначения и описание позиций и переходов сетей Петри-Маркова, моделирующих процессы реализации угроз туннелирования трафика и проведения атаки «неслепой IP-спуфинг»

Наименование атаки	Обозначение элемента сети Петри-Маркова	Описание элемента сети Петри – Маркова
Сетевая атака туннелирования трафика в условиях применения СОВ	Позиции сети	
	0(a)	Начальное состояние процесса, нарушитель готов к проведению атаки, сформировал пакет для передачи на доверенный хост, в который инкапсулировал пакет с программой-шпионом
	1(a)	Сообщение с инкапсулированным пакетом поступило на доверенный хост
	2(a)	Инкапсулированный пакет выделен из сообщения и установлен адрес его пересылки на атакуемый хост; 3(a) — пакет с вредоносной программой от доверенного хоста поступил на атакуемый хост и распакован
	4(a)	На атакуемом хосте включена СОВ
	5(a)	С вероятностью $p_{обн}$ обнаружено вторжение на атакуемом хосте и отправлена команда на пресечение вторжения; 6(a) – угроза не реализована
	Переходы сети	
	0(z)	Передача сообщения с инкапсулированным пакетом на доверенный хост
	1(z)	Распаковка сообщения с инкапсулированным пакетом на доверенном хосте, передача с одного из хостов – клиентов СЭД на атакуемый хост
	2(z)	Инкапсулированный пакет передан на атакуемый хост
	3(z)	Осуществляется обнаружение вторжения по сигнатуре или по аномалиям
	4(z)	Логический переход «И-НЕ», срабатывающий, если к данному моменту времени поступила команда на пресечение вторжений от СОВ, а команда на запуск ВП не поступила, то есть угроза реализована

Продолжение таблицы 2

Сетевая атаки «неслепой IP-спуфинг» с внедрением вредоносной программы	Позиции сети	
	0(a)	Начальное состояние процесса: на атакуемом хосте находится ЭД, нарушитель готов к проведению атаки, сформировал UDP-пакет с адресом доверенного хоста и с программой, предназначенной для уничтожения ЭД с расширением *.doc и *.docx
	1(a)	Пакет с ВП получен на атакуемом хосте и распакован; 2(a) — на атакуемом хосте функционирует система антивирусной защиты
	3(a)	С вероятностью $p_{обн}$ обнаружена ВП и отправлена команда на ее блокирование
	4(a)	Угроза реализована
	Переходы сети	
	0(z)	Передача сообщения с ВП на доверенный хост, запуск на нем антивирусного средства
	1(z)	Запуск ВП
	2(z)	Осуществляется поиск вредоносной программы
	3(z)	Логический переход «И-НЕ», срабатывающий, если не поступила команда на блокирование ВП, а ВП запущена на выполнение, угроза реализуется

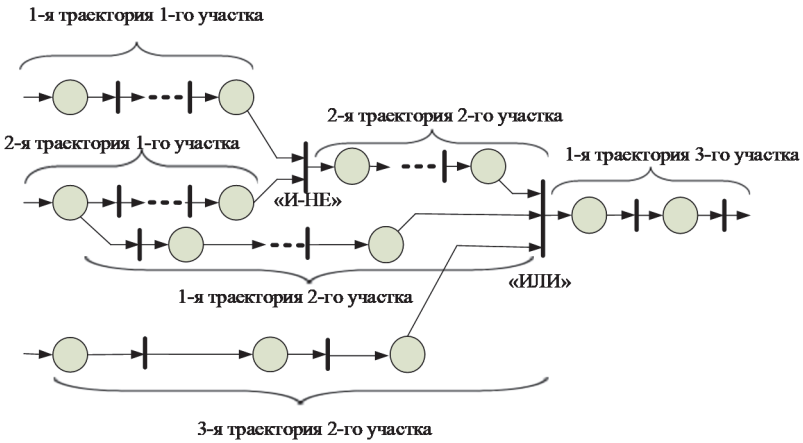

Рис. 7. Пример разбиения сети Петри — Маркова на участки и траектории

$\Phi_{ij}(d,t)$ — вероятность перемещения процесса по траектории d за время t из позиции с номером i в переход с номером j; $f_{ik}(d,\tau)$ — плотность распределения вероятностей времени перемещения процесса по траектории d из i-й позиции в k-й переход; $\pi_{i,k}(d)$ — вероятность того, что процесс пойдет по дуге, соединяющей i-ю позицию с k-м переходом, находящимся на траектории d (при отсутствии разветвлений для инцидентных позиции и перехода эта вероятность равна 1; если позиция не соединяется с переходом по рассматриваемой траектории, то вероятность равна 0).

Если по данной траектории метка из позиции с номером i может достичь перехода с номером k и позиция и переход не являются инцидентными, то имеют место равенства:

$$\pi_{i,j}(d) = \prod_{h_d=1}^{H_d} \pi_{i+h_d,r+h_d}(d); \tag{15}$$

$$\begin{aligned} f_{i,j}(d,t) = f_{i,r}(d,t) * f_{i+1_d,r+1_h}(d,t) * \ldots * \\ * f_{i+h_d,r+h_d}(d,t) * \ldots * f_{i+H_d,r+H_d}(d,t), \end{aligned} \tag{16}$$

где h_d — текущий номер перехода по траектории d при перемещении из позиции с номером i в переход с номером j, $h_d = \overline{1,H_d}$; H_d — общее количество переходов между позицией с номером i и переходом с номером j на траектории d; * — операция свертки [20, 21].

Если на участке имеет место несколько траекторий перемещения, сходящихся на логическом переходе, то время перемещения рассчитывается для каждой траектории.

При этом среднее время выполнения процесса по d-й траектории определяется следующим образом:

$$\overline{\tau_d} = \chi'_{\Sigma_d}(s)\big|_{s=0}, d = \overline{1,D}, \tag{17}$$

где $\chi'_{\Sigma_d}(s)$ — производная от характеристической функции $\chi_{\Sigma_d}(s)$ суммы времен выполнения функций, составляющих процедуры, реализуемые по d-й траектории сети [9, 20]:

$$\chi_{\Sigma_d}(s) = \prod_{r=1}^{R_d} \chi_r(s), r = \overline{1, R_d}, \quad (18)$$

Независимо от того, какому закону подчиняются распределения времен перемещения по дуге (в соответствии с теорией сетей Петри — Маркова [15] время перемещения процесса из позиции в переход считается случайным конечным, а из перехода в позицию — мгновенным), D — общее количество выделенных траекторий; R_d — общее количество ненулевых по времени перемещений на d-й траектории.

Время срабатывания логических переходов существенно зависит не только от количества входящих дуг, но и от того, сколько входящих дуг соответствует логическому условию «И», «ИЛИ», «НЕ» или их сочетаниям (рисунок 8).

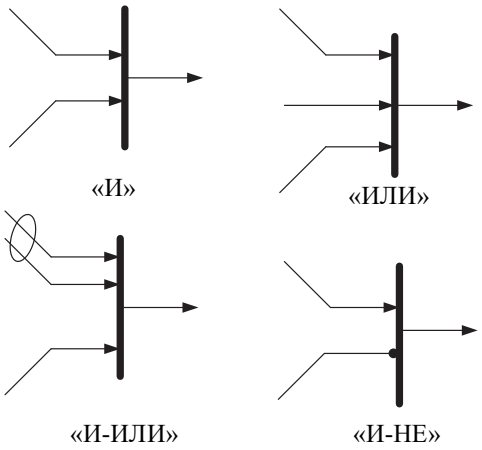

Рис. 8. Некоторые логические переходы, встречающиеся при моделировании процессов реализации угроз в ИС

Соотношения для расчета времен срабатывания логических переходов наиболее часто встречающихся при моделировании процессов реализации угроз безопасности информации в ИС, приведены в соответствии с [25] в таблице 3.

С учетом приведенных соотношений рассчитывались средние времена срабатывания сетей Петри — Маркова, моделирующие угрозу сетевой атаки путем «туннелирования» трафика (рисунок 5) и угрозу «неслепой IP-спуффинг» (рисунок 6).

Таблица 3. Соотношения для расчета времени срабатывания некоторых логических переходов

Логическое условие	Формула для расчета
«И»	Для двух входящих дуг: $\overline{\tau}_{"И"} = \frac{\overline{\tau_1}^2 + \overline{\tau_1}\cdot\overline{\tau_2} + \overline{\tau_2}^2}{\overline{\tau_1} + \overline{\tau_2}}$; для трех входящих дуг: $\overline{\tau}_{"И"} = \overline{\tau_1} + \overline{\tau_2} + \overline{\tau_3} + \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}} + \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}}} + \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_3}}} + \frac{1}{\frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}}$
«ИЛИ»	Для двух входящих дуг: $\overline{\tau}_{"ИЛИ"} = \frac{\overline{\tau_1}\cdot\overline{\tau_2}}{\overline{\tau_1} + \overline{\tau_2}}$; Для трех входящих дуг: $\overline{\tau}_{"ИЛИ"} = \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}}$
«И-НЕ»	Для двух входящих дуг (первая соответствует условию «И», вторая – условию «НЕ»): $\overline{\tau}_{"И-НЕ"} = \overline{\tau_1}\cdot\left(1 + \frac{\overline{\tau_1}}{\overline{\tau_2}}\right)$; Для трех входящих дуг (первая и вторая соответствует условию «И», третья – условию «НЕ»): $\overline{\tau}_{"И-НЕ"} = \frac{\overline{\tau_1}^2 + \overline{\tau_1}\cdot\overline{\tau_2} + \overline{\tau_2}^2}{\overline{\tau_1} + \overline{\tau_2}}\cdot\left(1 + \frac{\overline{\tau_1}^2 + \overline{\tau_1}\cdot\overline{\tau_2} + \overline{\tau_2}^2}{(\overline{\tau_1} + \overline{\tau_2})\cdot\overline{\tau_3}}\right)$
«И-ИЛИ»	Для трех входящих дуг (первая и вторая дуги или третья дуга): $\overline{\tau_{"И-ИЛИ"}} = \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}} + \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}}} + \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_3}}}$

Так, для первой из указанных угроз среднее время ее реализации в условиях применения СОВ определяется из соотношений:

$$\overline{\tau_u^{(ЗИ)}} = \overline{\tau_{0,4}} = \overline{\tau_{0,0}} + \overline{\tau_{"И-НЕ"}};\ \overline{\tau_{"И-НЕ"}} = \overline{\tau_{1,4}}\cdot\left(1 + \frac{\overline{\tau_{1,4}}}{\overline{\tau_{4,4}}}\right), \qquad (19)$$

где $\overline{\tau_{1,4}} = \overline{\tau_{1,1}} + \overline{\tau_{2,2}} + \overline{\tau_{3,4}}$ и $\overline{\tau_{4,4}} = \overline{\tau_{4,3}} + \overline{\tau_{5,4}} = \frac{\overline{\tau_{\det}}}{p_{\det}} + \overline{\tau_{rep}}$.

Здесь $\overline{\tau_{0,0}} \equiv \overline{\tau_0}$ (см. формулу (3)), $\overline{\tau_u^{(0)}} \equiv \overline{\tau_{1,4}}$ и $p_{exc}(\tau_u^{(0)} - \tau_{res.u} > 0) = \dfrac{\overline{\tau_{4,4}}}{\overline{\tau_{4,4}} + \overline{\tau_{1,4}}}$.

Если положить все средние времена переходов, в том числе среднее время пресечения, кроме среднего времени обнаружения вторжения, примерно равными $\bar{\tau}$, то время реализации угрозы определяется из соотношения:

$$\overline{\tau_u^{(ЗИ)}} = \bar{\tau} \cdot \left[4 + \frac{9}{1 + \dfrac{\overline{\tau_{det}}}{P_{det} \cdot \bar{\tau}}} \right]. \qquad (20)$$

Для второй из указанных угроз среднее время ее реализации в условиях применения САВЗ определяется из соотношения:

$$\overline{\tau_u^{(ТЗИ)}} = \overline{\tau_{0,3}} = \overline{\tau_{0,0}} + \overline{\tau_{"И\text{-}НЕ"}}, \qquad (21)$$

где $\overline{\tau_{"И-НЕ"}} = \overline{\tau_{1,3}} \cdot (1 + \dfrac{\overline{\tau_{1,3}}}{\overline{\tau_{2,3}}})$ и $\overline{\tau_{2,3}} = \overline{\tau_{2,2}} + \overline{\tau_{3,3}} = \overline{\tau_{rep}} + \dfrac{\overline{\tau_{det}}}{p_{det}}$.

Здесь $\overline{\tau_0} \equiv \overline{\tau_{0,0}}$ (см. формулу (3)), $\overline{\tau_u^{(0)}} \equiv \overline{\tau_{1,4}}$ и $p_{exc}(\tau_u^{(0)} - \tau_{res.u} > 0) = \dfrac{\overline{\tau_{2,3}}}{\overline{\tau_{2,3}} + \overline{\tau_{1,3}}}$.

Если положить, что все средние времена переходов, в том числе среднее время пресечения, кроме среднего времени обнаружения вредоносной программы, примерно равны $\bar{\tau}$, то среднее время реализации угрозы определяется из соотношения:

$$\overline{\tau_u^{(ЗИ)}} = \bar{\tau} \left\{ 2 + \frac{1}{1 + \dfrac{\overline{\tau_{det}}}{p_{det} \cdot \bar{\tau}}} \right\}. \qquad (22)$$

С учетом приведенных соотношений по формуле (12) рассчитывались зависимости показателя эффективности СОВ от вероятности обнаружения вторжения для угрозы сетевой атаки с внедрением ВП путем «туннелирования» трафика, которые приведены в графическом виде на рисунках 9 и 10. На рисунках 11 и 12 представлены путем проведения атаки «неслепой IP-спуффинг» от вероятности обнаружения вредоносной программы.

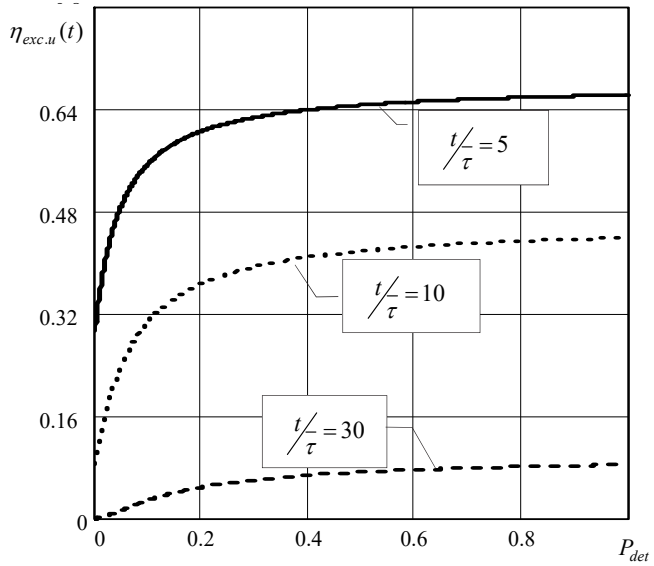

Рис. 9. Зависимость показателя эффективности защиты информации при использовании СОВ от вероятности обнаружения вторжения при $\overline{\tau_{det}}/\tau = 0.1$

Анализ полученных зависимостей показывает, что эффективность защиты ЭД за счет опережения мерами защиты процессов реализации угроз существенно зависит не только от вероятности обнаружения вторжения или вероятности обнаружения вредоносной программы, но и от времени реакции СОВ и САВЗ.

Это обусловливает необходимость формирования требований к СОВ и САВЗ в части ограничения времени, затрачиваемого на обнаружение и пресечение нарушений в СЭД СН, связанных с сетевыми атаками и применением вредоносных программ. Сегодня такие требования в нормативных документах отсутствуют.

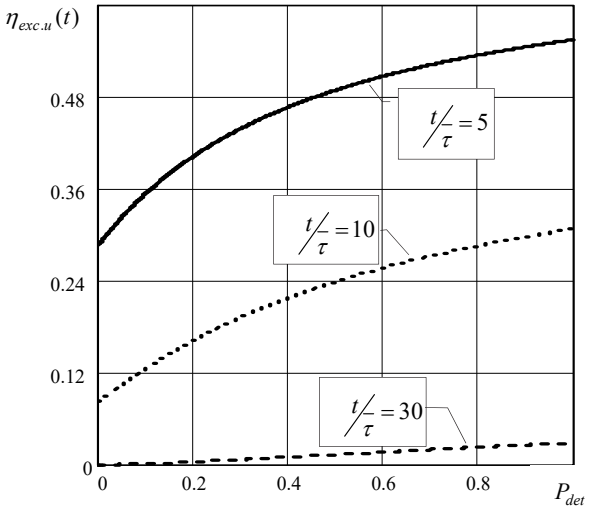

Рис. 10. Зависимость показателя эффективности защиты информации при использовании СОВ от вероятности обнаружения вторжения при $\overline{\tau_{det}}/\tau = 1$

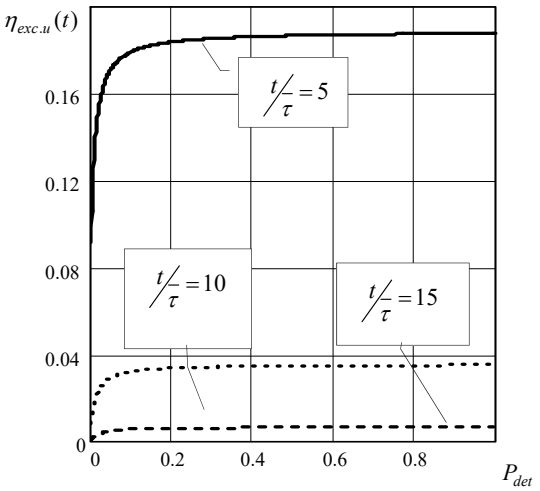

Рис. 11. Зависимость эффективности защиты информации при использовании САВЗ от вероятности обнаружения вредоносной программы при $\overline{\tau_{det}}/\tau = 0.01$

Труды СПИИРАН. 2019. Том 18 № 6. ISSN 2078-9181 (печ.)
ISSN 2078-9599 (онлайн) www.proceedings.spiiras.nw.ru

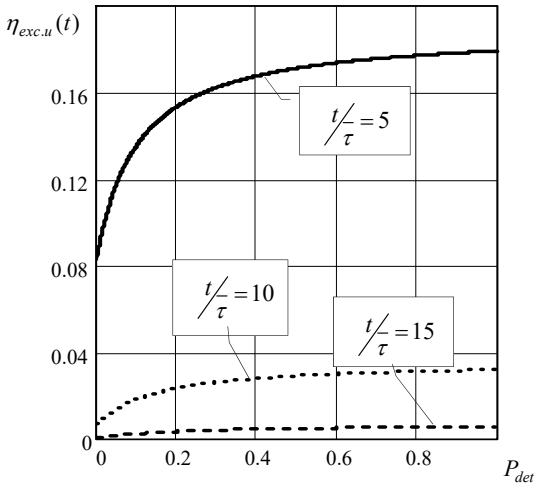

Рис. 12. Зависимость показателя эффективности защиты информации при использовании САВЗ от вероятности обнаружения вредоносной программы при $\overline{\tau_{det}}/\tau = 0.1$

4. Экспериментальные результаты. Для проверки адекватности разработанных моделей и корректности получаемых оценок эффективности защиты ЭД были проведены экспериментальные исследования в форме вычислительного эксперимента с использованием известного методического аппарата функционального моделирования IDEF0 (Integrated Computer Aided Manufacturing DEFinition) в соответствии с Рекомендациями по стандартизации Р 50.1.028-2001 «Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования».

Для формирования перечня процедур и функций, выполняемых в ходе электронного документооборота, были использованы сведения о структуре и функционале широко применяемой в органах власти и государственных организациях СЭД типа «Дело» [26].

На рисунке 13 приведены состав программно-аппаратных компонентов и задачи, решаемые с применением такой СЭД, а также перечень и порядок выполнения функций обработки документов в ней на примере входящего ЭД, которые были положены в основу проведения экспериментальных исследований.

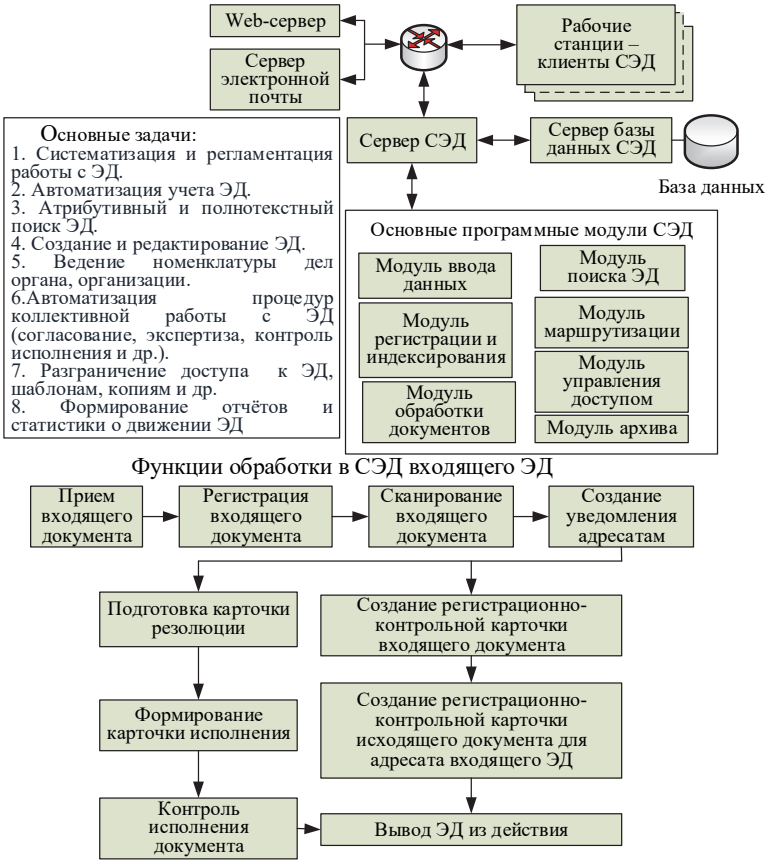

Рис. 13. Состав и задачи СЭД, перечень и порядок выполнения функций обработки документов на примере входящего ЭД, которые учитывались в вычислительном эксперименте

В ходе эксперимента задавалось время реакции системы защиты (СОВ и САВЗ) и сравнивались результаты теоретической оценки времени реализации угроз электронному документообороту с использованием аппарата сетей Петри — Маркова со временем, рассчитываемым по результатам моделирования с использованием IDEF0, а затем по формуле (12) рассчитывался показатель эффективности для модели на сети Петри — Маркова и для модели, разработанной с использованием аппарата IDEF0.

Вычислительный эксперимент показал, что расхождение в результатах оценки эффективности защиты электронного

документооборота по указанным моделям применительно к угрозам туннелирования трафика и «неслепого IP-спуффинга» не превысило 18%.

Это свидетельствует о достаточно высокой адекватности моделей, разрабатываемых с использованием аппарата сетей Петри—Маркова, и корректности получаемых оценок эффективности защиты электронного документооборота.

Важным практическим вопросом применения разработанного подхода является оценивание эффективности адаптивных мер защиты, для чего необходима разработка соответствующей методики и ее реализация в виде программного продукта. Порядок действий по оцениванию эффективности защиты ЭД в СЭД, который может быть положен в основу разработки такой методики, приведен на рисунке 14.

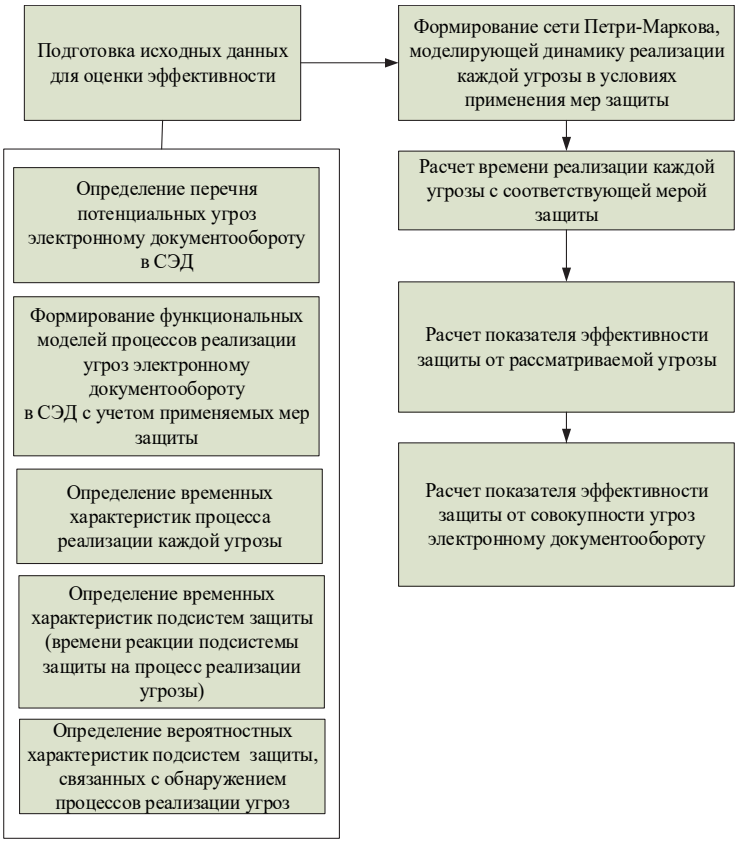

Рис. 14. Порядок действий, составляющий содержание методики оценивания эффективности защиты электронных документов в СЭД на основе определения возможности опережения мерами защиты процесса реализации угроз

4. Заключение. Традиционный подход к оцениванию показателей эффективности защиты электронного документооборота на основе сравнения возможностей реализации угроз безопасности информации без применения и с применением мер защиты в случае, когда применяются адаптивные меры защиты информации, оказывается недостаточным.

Предложенный новый показатель эффективности защиты электронного документооборота, направленный на оценивание возможности опережения мерами защиты процесса реализации угроз документообороту, позволяет учесть время реакции систем защиты на факт обнаружения попытки (процесса) реализации угрозы.

Для расчета указанного показателя в работе предложен подход, во-первых, к формированию структурно-функциональных моделей процессов реализации угроз, во-вторых, к построению на их основе математических моделей оценивания вероятностно-временных характеристик этих процессов с использованием аппарата сетей Петри — Маркова, который позволяет количественно обосновывать требования к временным характеристикам функционирования систем защиты ЭД в СЭД.

Проведенные экспериментальные исследования в форме вычислительного эксперимента путем сравнения результатов расчетов показателей эффективности защиты ЭД по моделям, построенным с применением сетей Петри — Маркова и аппарата функционального моделирования IDEF0, показали их достаточно высокую сходимость с отклонением от 3 до 18 %, что свидетельствует о корректности моделей оценивания эффективности защиты электронного документооборота в СЭД с применением аппарата сетей Петри — Маркова.

Перспективами направлениями дальнейших исследований по данной тематике являются:

– расширение состава логических условий реализации процессов документооборота и угроз безопасности информации в СЭД в сочетании с применением аппарата логических сетей и теории предикатов;

– разработка аналитических моделей расчета показателей оценки влияния различных мер и средств защиты информации на процессы реализации угроз электронному документообороту;

– проведение теоретических и экспериментальных исследований по нормированию значений показателей эффективности защиты электронного документооборота в интересах обоснования требований к системам защиты;

– разработка программных средств автоматизации оценивания эффективности защиты электронного документооборота в СЭД.

Литература

1. *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.
2. *Скоредова Ю.В., Гречишников Е.В., Кравченко А.С., Ланкин О.В.* Анализ методик автоматизированной оценки угроз и рисков информационной безопасности информационно-телекоммуникационных систем // Вестник Воронежского института ФСИН России. 2017. № 3. С. 128–133.
3. *Скрыль С.В. и др.* Вероятностные модели информационных процессов в интегрированных системах безопасности в условиях обеспечения защиты информации от несанкционированного доступа // Телекоммуникации. 2015. № 6. С. 26–31.
4. *Muratkhan R., Satybaldina D.Z.* Quantitative method of information security risk assessment by multicomponent threats // Life Science Journal. 2014. vol. 11. no. 11. pp. 372–375.
5. *Al Hadidi M. et al.* Methods of risk assessment for information security management // International Review on Computers and Software. 2016. vol. 11. no. 2. pp. 81–91.
6. *Anisimov V.G., Zegzhda P.D., Anisimov E.G., Bazhin D.A.* A risk-oriented approach to the control arrangement of security protection subsystems of information systems // Automatic Control and Computer Sciences. 2016. vol. 50. no. 8. pp. 717–721.
7. *Кукин С.А., Печерский А.В.* Управление рисками информационных угроз для системно связанных объектов // Сборник статей XV Международной научно-практической конференции «Современные технологии документооборота в бизнесе, производстве и управлении». 2015. С. 41–44.
8. *Makarevich O., Mashkina I., Sentsova A.* The method of the information security risk assessment in cloud computing systems // Proceedings of the 6th International Conference on Security of Information and Networks. 2013. pp. 446–447.
9. *Язов Ю.К., Соловьев С.В.* Защита информации в информационных системах от несанкционированного доступа // Воронеж: Кварта. 2015. 440 с.
10. *Гнеденко Б.В., Коваленко И.Н.* Введение в теорию массового обслуживания. Издание второе, переработанное и дополненное // М.: Наука. 1987.
11. *Котов В.Е.* Сети Петри // М.: Наука. 1984. 160с.
12. *Brissaud F., Luiz F.* Average probability of a dangerous failure on demand: different modelling methods, similar results // arXiv preprint arXiv: 1501.06487. 2015.
13. *Yang M., Wang M., Qu Y.* Modeling and performance analysis of the emergency rescue logistics system based on Petri nets // Journal of Hebei University of Science and Technology. 2017. vol. 38(3). pp. 269–277.
14. *Vazquez C.R., Silva M.* Stochastic Continuous Petri Nets: An Approximation of Markovian Net Models // IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans. 2011. vol. 42. no. 3. pp. 641–653.
15. *Игнатьев В.М., Ларкин Е.В.* Сети Петри-Маркова // ТулГТУ. 1994.
16. *Mohan L.N., Anjaneyulu G.S.G.N.* A secured digital signature using conjugacy and DLP on non-commutative group over finite field // Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications. 2017. pp. 457–465.
17. *Detken K.O. et al.* SIEM approach for a higher level of it security in enterprise networks // 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2015. vol. 1. pp. 322–327.
18. *Majeed A. et al.* Near-miss situation based visual analysis of SIEM rules for real time network security monitoring // Journal of Ambient Intelligence and Humanized Computing. 2018. vol. 10. no. 4. pp. 1509–1526.
19. *Martinasek Z., Blazek P., Silhavy P., Smekal D.* Methodology for correlations discovery in security logs // 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2017. pp. 294–298.
20. *Тихонов В.И.* Статистическая радиотехника // М.: Сов. радио. 1966.
21. *Климов Г.П.* Стохастические системы массового обслуживания // М.: Наука. 1966.

22. *Тараканов К.В., Овчаров Л.А., Тырышкин А.Н.* Аналитические методы исследований систем // М.: Сов радио. 1974. 240 с.
23. *Авсентьев О.С. Рубцова И.О.* Обобщенное представление информационных процессов в системах электронного документооборота специального назначения в условиях угроз безопасности информации // Вестник Воронежского института МВД России. 2017. № 4. С. 108–115.
24. *Hallé S. et al.* Decentralized enforcement of document lifecycle constraints // Information Systems. 2018. vol. 74. pp. 117–135.
25. *Язов Ю.К., Панфилов В.В.* Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри-Маркова // Информация и безопасность. 2006. Т. 9. № 1. С. 117–123.
26. Основные функции системы СЭД «ДЕЛО». URL: http://www.interface.ru/home.asp?artid=21844 (дата обращения: 27.07.2019).

Язов Юрий Константинович — д-р техн. наук, профессор, главный научный сотрудник, Государственный научно-исследовательский, испытательный институт проблем технической защиты информации, Федеральная служба по техническому и экспортному контролю России; профессор, кафедра систем информационной безопасности, Воронежский государственный технический университет. Область научных интересов: применение методов математического моделирования в области обеспечения информационной безопасности объектов различных сфер деятельности, разработка, совершенствование и применение методов и средств защиты информации в процессе сбора, хранения, обработки, передачи и распространения информации. Число научных публикаций — 290. Yazoff_1946@mail.ru; ул. 9 Января, 280 а, 394020, Воронеж, Российская Федерация; р.т.: +7(903)-651-42-69.

Авсентьев Олег Сергеевич — д-р техн. наук, профессор, профессор, кафедра информационной безопасности, Воронежский институт Министерства внутренних дел России; профессор, кафедра организации и технологии защиты информации, Белгородский университет кооперации, экономики и права. Область научных интересов: применение методов математического моделирования в области обеспечения информационной безопасности объектов различных сфер деятельности, разработка, совершенствование и применение методов и средств защиты информации в процессе сбора, хранения, обработки, передачи и распространения информации. Число научных публикаций — 101. osaos@mail.ru; пр. Патриотов, 53, 394065, Воронеж, Российская Федерация; р.т.: +7-(473)-500-52-42; факс: +7(473)-200-52-00.

Авсентьев Александр Олегович — канд. техн. наук, старший преподаватель, кафедра физики, Воронежский институт Министерства внутренних дел России. Область научных интересов: применение методов математического моделирования в области обеспечения информационной безопасности объектов различных сфер деятельности, разработка, совершенствование и применение методов и средств защиты информации в процессе сбора, хранения, обработки, передачи и распространения информации. Число научных публикаций — 40. aoaao8787@mail.ru; пр. Патриотов, 53, 394065, Воронеж, Российская Федерация; р.т.: +7-(473)-500-52-66; факс: +7-(473)-200-52-00.

Рубцова Ирина Олеговна — аспирант, кафедры организации и технологии защиты информации, Белгородский университет кооперации, экономики и права. Область научных интересов: разработка, совершенствование и применение методов и средств защиты информации в процессе сбора, хранения, обработки, передачи и распространения информации; обеспечения информационной безопасности объектов политической, социально-экономической, оборонной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации. Число научных публикаций — 15. irinka23@bk.ru; ул. Садовая, 116 А, 308023, Белгород, Российская Федерация; р.т.: +7-(4722)-26-38-31; факс: +7-(4722)-26-49-65.

DOI 10.15622/sp.2019.18.6.1269-1300

YU.K. YAZOV, O.S. AVSENTEV, A.O. AVSENTEV, I.O. RUBTSOVA

METHOD FOR ASSESSING EFFECTIVENESS OF PROTECTION OF ELECTRONIC DOCUMENT MANAGEMENT USING THE PETRI AND MARKOV NETS APPARATUS

Yazov Yu.K., Avsentev O.S., Avsentev A.O., Rubtsova I.O. **Method for Assessing Effectiveness of Protection of Electronic Document Management using the Petri and Markov Nets Apparatus.**

Abstract. Traditional approaches to assessing the effectiveness of information security, based on a comparison of the possibilities of realizing threats to information security in absence and application of protection measures, do not allow to analyze the dynamics of suppression by security measures of the process of implementing threats. The paper proposes a new indicator of the effectiveness of protection of electronic documents, aimed at assessing the possibility of advancing security measures of the process of implementing threats in electronic document management systems using the probability-time characteristics of the dynamics of the application of protection measures and the implementation of threats to electronic documents. Mathematical models were developed using the Petri-Markov network apparatus and analytical relationships were obtained for calculating the proposed indicator using the example of the "traffic tunneling" threat (placing intruder packets in trusted user packets) and unauthorized access (network attacks) to electronic documents, as well as the threat of intrusion of malicious program by carrying out an "blind IP spoofing" attack (network address spoofing). Examples of calculating the proposed indicator and graphs of its dependence on the probability of detecting network attacks by the intrusion detection system and on the probability of malware detection by the anti-virus protection system are given. Quantitative dependencies are obtained for the effectiveness of protection of electronic documents due to being ahead of protection measures for threat realization processes, both on the probability of detecting an intrusion or the probability of detecting a malicious program, and on the ratio of the time spent by the protection system on detecting an attempt to implement a threat and taking measures to curb its implementation, and threat implementation time. Models allow not only to evaluate the effectiveness of measures to protect electronic documents from threats of destruction, copying, unauthorized changes, etc., but also to quantify the requirements for the response time of adaptive security systems to detectable actions aimed at violating the security of electronic documents, depending on the probability -temporal characteristics of threat realization processes, to identify weaknesses in protection systems related to the dynamics of threat realization and the reaction of defense systems to such threats electronic document.

Keywords: Efficiency Indicator, Functional Model, Petri-Markov Network, Security Threat, Security Measure, Intrusion Detection System, Anti-Virus Protection System.

Yazov Yuri Konstantinovich — Ph.D., Dr.Sci., Professor, Chief Researcher, Testing Institute of Problems of Technical Protection of information, Federal Service for Technical and Export Control of Russia; Professor, Department of Information security systems, Voronezh state technical University. Research interests: application of mathematical modeling methods in the field of information security of objects of various fields of activity, development, improvement and application of methods and means of information security in the process of collection, storage, processing, transmission and dissemination of information. The number of publications — 290. Yazoff_1946@mail.ru; 280 a, 9 January str., 394020, Voronezh, Russian Federation; office phone: +7(903)-651-42-69.

Avsentev Oleg Sergeevich — Ph.D., Dr.Sci., Professor, Professor, Department of Information Security, Voronezh Institute of the Ministry of Interior of Russia; Professor, Department of

Organization and Technology of Information Protection, Belgorod University of Cooperation, Economics and Law. Research interests: application of mathematical modeling methods in the field of information security of objects of various fields of activity, development, improvement and application of methods and means of information security in the process of collection, storage, processing, transmission and dissemination of information. The number of publications — 101. osaos@mail.ru; 53, pr. Patriotov, 394065, Voronezh, Russian Federation; office phone: +7-(473)-500-52-42; fax: +7(473)-200-52-00.

Avsentev Alexander Olegovich — Ph.D., senior lecturer, Department of Physics, Voronezh Institute of the Ministry of Interior of Russia. Research interests: application of mathematical modeling methods in the field of information security of objects of various fields of activity, development, improvement and application of methods and means of information security in the process of collection, storage, processing, transmission and dissemination of information. The number of publications — 40. aoaao8787@mail.ru; 53, pr. Patriotov, 394065, Voronezh, Russian Federation; office phone: +7-(473)-500-52-66; fax: +7-(473)-200-52-00.

Rubtsova Irina Olegovna — Ph.D. Student, Department of Organization and Technology of Information Security, Belgorod University of Cooperation, Economics and Law. Research interests: development, improvement and application of methods and means of information security in the process of collection, storage, processing, transmission and dissemination of information; information security of objects of political, socio-economic, defense and other fields of activity from external and internal threats of theft, destruction and/or modification of information. The number of publications — 15. irinka23@bk.ru; 116 A, Sadovaya str., 308023, Belgorod, Russian Federation; office phone: +7-(4722)-26-38-31; fax: +7-(4722)-26-49-65.

References

1. Skryl' S.V. Lavrukhin YU.N., Kurilo A.P., Bagaev D.A. [Justification of indicators for evaluating the effectiveness of information processes in information and telecommunication systems in the face of threats to information security]. *Informatsiya i bezopasnost' – Information and security*. 2009. vol. 3. pp. 429–432. (In Russ.).
2. Skoredova Yu.V., Grechishnikov E.V., Kravchenko A.S., Lankin O.V. [Analysis of methods for automated evaluation of threats and risks to information security information and telecommunication systems]. *Vestnik Voronezhskogo instituta FSIN Rossii – Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service.* 2017. vol. 3. pp. 128–133. (In Russ.).
3. Skryl' S.V. et al. [Probabilistic models of information processes in integrated security systems in the conditions of information protection from unauthorized access]. *Telekommunikatsii – Telecommunications*. 2015. vol. 6. pp. 26–31. (In Russ.).
4. Muratkhan R., Satybaldina D.Z. Quantitative method of information security risk assessment by multicomponent threats. *Life Science Journal.* 2014. vol. 11. no. 11. pp. 372–375.
5. Al Hadidi M. et al. Methods of risk assessment for information security management. *International Review on Computers and Software*. 2016. vol. 11. no. 2. pp. 81–91.
6. Anisimov V.G., Zegzhda P.D., Anisimov E.G., Bazhin D.A. A risk-oriented approach to the control arrangement of security protection subsystems of information systems. *Automatic Control and Computer Sciences.* 2016. vol. 50. no. 8. pp. 717–721.
7. Kukin S.A., Pecherskij A.V. [Risk management of information threats for systemically connected objects]. *Sbornik statej XV Mezhdunarodnoj nauchno-prakticheskoj konferentsii "Sovremennye tekhnologii dokumentooborota v biznese, proizvodstve i upravlenii"* [Collection of articles XV International scientific and practical conference "Modern technologies of document circulation in business, production and management"]. 2015. pp. 41–44. (In Russ.).

8. Makarevich O., Mashkina I., Sentsova A. The method of the information security risk assessment in cloud computing systems. Proceedings of the 6th International Conference on Security of Information and Networks. 2013. pp. 446–447.
9. Yazov YU.K., Solov'ev S.V. *Zashhita informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa* [Protection of information in information systems from unauthorized access]. Voronezh: Kvarta. 2015. 440 p. (In Russ.).
10. Gnedenko B.V., Kovalenko I.N. *Vvedenie v teoriyu massovogo obsluzhivaniya. Izdanie vtoroe, pererabotannoe i dopolnennoe* [Introduction to Queuing theory. Second edition, revised and expanded]. M.: Nauka. 1987. (In Russ.).
11. Kotov V.E. *Seti Petri* [Petri Nets]. M.: Nauka. 1984. 160 p. (In Russ.).
12. Brissaud F., Luiz F. Average probability of a dangerous failure on demand: different modelling methods, similar results. arXiv preprint arXiv: 1501.06487. 2015.
13. Yang M., Wang M., Qu Y. Modeling and performance analysis of the emergency rescue logistics system based on Petri nets. *Journal of Hebei University of Science and Technology.* 2017. vol. 38(3). pp. 269–277.
14. Vazquez C.R., Silva M. Stochastic Continuous Petri Nets: An Approximation of Markovian Net Models. *IEEE Transactions on Systems, Man, and Cybernetics* – Part A: Systems and Humans. 2011. vol. 42. no. 3. pp. 641–653.
15. Ignat'ev V.M., Larkin E.V. *Seti Petri-Markova* [Petri-Markov Nets]. TulGTU. 1994. (In Russ.)
16. Mohan L.N., Anjaneyulu G.S.G.N. A secured digital signature using conjugacy and DLP on non-commutative group over finite field. Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications. 2017. pp. 457–465.
17. Detken K.O. et al. SIEM approach for a higher level of it security in enterprise networks. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2015. vol. 1. pp. 322–327.
18. Majeed A. et al. Near-miss situation based visual analysis of SIEM rules for real time network security monitoring. *Journal of Ambient Intelligence and Humanized Computing.* 2018. vol. 10. no. 4. pp. 1509–1526.
19. Martinasek Z., Blazek P., Silhavy P., Smekal D. Methodology for correlations discovery in security logs. 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2017. pp. 294–298.
20. Tikhonov V.I. *Statisticheskaya radiotekhnika* [Statistical radio engineering]. M.: Sov. radio. 1966. (In Russ.).
21. Klimov G.P. *Stokhasticheskie sistemy massovogo obsluzhivaniya* [Stochastic queueing systems]. M.: Nauka. 1966. (In Russ.).
22. Tarakanov K.V., Ovcharov L.A., Tyryshkin A.N. *Analiticheskie metody issle-dovanij system* [Analytical methods of research systems]. M.: Sov radio. 1974. 240 p. (In Russ.).
23. Rubtsova, I.O. Avsentev O.S. [A consolidated view of information processes in systems of electronic document circulation of special purpose in terms of threats to information security]. *Vestnik Voronezhskogo instituta MVD Rossii – The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia.* 2017. vol 4. pp. 108–115.
24. Hallé S. et al. Decentralized enforcement of document lifecycle constraints. *Information Systems.* 2018. vol. 74. pp. 117–135.
25. Yazov Yu.K., Tekunov V.V. [Modeling of the dynamics of realization of the threats to information security using the apparatus of Petri nets and Markov]. *Informatsiya i bezopasnost' – Information and security*. 2006. Issue 9. vol. 1. pp. 117–123.
26. Osnovnye funkcii sistemy SED "DELO" [The main functions of the system EDMS "CASE"]. Available at: http://www.interface.ru/home.asp?artid=21844 (accessed: 27.07.2019).