Инженерный вестник Дона, №9 (2023)
ivdon.ru/ru/magazine/archive/n9y2023/8678

Модель конфигурирования структурно-функциональных характеристик информационных систем ведомственного назначения

М.А. Каплин, С.П. Соколовский, А.А. Горбачев

Краснодарское высшее военное училище

Аннотация: В данной статье рассмотрены условия и факторы, влияющие на безопасность информационных систем, функционирующих в условиях сетевой разведки. В основу разработанной модели положены техники, реализующие динамическую смену доменных имен, сетевых адресов и портов сетевым устройствам информационной системы и ложным сетевым информационным объектам, функционирующим в их составе. Произведена формализация задачи исследования. Теоретической основой разработанной модели являются теории вероятностей и случайных процессов. Приведены результаты расчета вероятностно-временных характеристик целевой системы в зависимости от действий сетевой разведки, позволяющих определить режим настройки разработанных мер защиты и осуществить оценку защищенности целевой системы при различных условиях ее функционирования.
Ключевые слова: информационная система ведомственного назначения, сетевая разведка, структурно-функциональная характеристика, ложный сетевой информационный объект.

В общем случае, информационная система ведомственного назначения (далее ИС ВН) включает множество взаимосвязанных каналами приема и передачи информации аппаратно-программных и технических средств (физические линии связи), объединенных в единое целое из территориально разнесенных элементов. Архитектура современных ИС ВН, как правило, соответствует архитектуре семейства протоколов *TCP/IP* и интегрирована с инфраструктурой транспортных сетей.

Стратегия злоумышленника – распределить ограниченный неоднородный ресурс средств разведки для вскрытия состава, структуры и алгоритмов функционирования ИС ВН с требуемой полнотой, своевременностью и достоверностью. Целью данных мероприятий является определение важных элементов ИС ВН для осуществления преднамеренных деструктивных воздействий и лишения их возможности осуществлять заданный функционал.

Наилучшая стратегия защиты – формировать у злоумышленника ложное (неверное) представление о структуре (топологии) и параметрах (типологии) ИС ВН. Это позволяет влиять на качество решений, принимаемых злоумышленником по результатам сетевой разведки (далее СР), которые обладают высоким временем актуальности в связи со статичностью структурно-функциональных характеристик (далее СФХ) ИС ВН [1, 2], предотвращать деструктивные воздействия на объекты защиты или снижать их результативность и эффективность [3 - 5].

Такая стратегия может быть реализована посредством демонстрации злоумышленнику ложного состава, структуры и алгоритмов функционирования ИС ВН и адаптивного (в зависимости от режимов функционирования ИС ВН и активности средств СР) конфигурирования СФХ ИС ВН. Для демонстрации злоумышленнику ложного состава, структуры и алгоритмов функционирования ИС ВН в настоящее время в ИС ВН применяются ложные сетевые информационные объекты (далее ЛСИО) – honeypot (в переводе с англ. – горшочек с медом), выступающие в качестве приманки для злоумышленника [6 - 8].

Для конфигурирования СФХ ИС ВН, таких как *IP*-адрес, время продолжительности его аренды, номер подсети (маска), сетевой порт и доменное имя используются протокол *DHCP* (*Dynamic Host Configuration Protocol*) – протокол динамической настройки узла, позволяющий автоматически назначать параметры на определённый срок, называемый временем аренды и служба доменных имен *DNS* (*Domain name system*) [9 - 11], предназначенная для получения *IP*-адреса по имени узла. Использование именно этих протоколов, являющихся клиент-серверными, позволяет за счет конфигурирования СФХ ИС ВН обеспечить скрытие состава, структуры и алгоритмов функционирования ИС ВН от СР [12].

Анализ угроз безопасности ИС ВН, а также техник ведения СР и

реализации компьютерных атак [13 - 15], показал, что результативность разрабатываемых мер защиты ИС ВН целесообразно рассматривать с позиции вероятностной оценки реализации опасных программно-технических (информационно-технических) воздействий, включающих в себя эксплуатацию уязвимостей ИС ВН злоумышленником. Количественная оценка защищенности ИС ВН от опасных программно-технических воздействий будет определяться, как вероятность отсутствия опасного воздействия P_d в течение заданного периода функционирования ИС ВН T_z [16].

Также при определении режима конфигурирования СФХ ИС ВН необходимо учитывать необходимые ресурсные затраты, а также другие критерии, влияющие на результативность защиты ИС ВН в условиях СР.

При формализации задачи исследования необходимо [17], используя математическую запись, сформулировать суть решаемой задачи, критерий ее решения, входные и выходные данные, существенные факторы и условия задачи. Тогда, в терминах математического моделирования, задача поиска формы отображения множества входных характеристик (которые содержат СФХ объекта исследования) на выходные (включающие в себя вероятностную оценку информационно-технического воздействия на ИС ВН), имеет следующий общий вид:

$$f : \Omega \to Y;$$
$$\Omega = \{X, A\};$$
$$X, A, Y \in Q.$$

где f – форма модельного оператора (уравнение связи); Ω – множество входных характеристик; Y – множество выходных характеристик, то есть, показателей защищенности ИС ВН, ресурсных затрат на реализацию мер защиты, в частности, вероятность информационно-технического воздействия на ИС ВН; X – множество факторов-аргументов, представляющее собой

управляемые параметры вариации СФХ ИС ВН посредством которых изменяются значения показателей Y; A – множество неконтролируемых (неуправляемых) параметров (характеризующих условия внешней среды и внутреннюю структуру ИС ВН) функционирования ИС ВН в условиях СР, влияющих на значения показателей Y; Q – допустимое множество значений для X, A, Y.

Структура допустимого множества учитывает специфику функционирования ИС ВН, аналитические, технические и организационные ограничения на значения характеристик модели.

С целью определения формы модельного оператора в вышеописанной задаче, необходимо разработать математическую модель функционирования ИС ВН при реализации конфигурирования СФХ ИС ВН в условиях СР, позволяющую получить вероятностную оценку опасных информационно-технических воздействий на ИС ВН при конфигурировании СФХ ИС ВН.

Математическая модель конфигурирования структурно-функциональных характеристик информационных систем ведомственного назначения. Вероятностный характер внешних воздействий по отношению к объекту исследования, то есть, поступающих запросов от клиентов и злоумышленников на узлы ИС ВН, позволяет использовать теорию случайных процессов, в частности, марковские и полумарковские цепи для моделирования процесса информационного обмена и воздействий средств СР и реализации компьютерных атак на узлы ИС ВН. Использование математического аппарата случайных процессов при моделировании сложных технических систем поднимает вопрос адекватности применяемых методов и моделей реальным свойствам моделируемого объекта. Элементы теории случайных процессов широко используются при описании взаимодействия информационных систем в условиях деструктивных воздействий и конфликтов [18, 19]. Анализ

предметной области показал, что использование математических моделей марковских случайных процессов в рамках исследования сложных систем принимается в соответствии с существующим предположением о том, что большинство реальных потоков событий, представляющих собой сумму большого числа независимых потоков малой интенсивности, являются простейшими [14, 15].

При использовании полумарковских случайных процессов либо ограничиваются рассмотрением стационарных вероятностных характеристик для произвольных распределений времени ожидания событий, либо оценка вероятностно-временных характеристик производится только для показательного закона распределения. Показательный закон распределения времени ожидания события, инициирующего эволюцию случайного процесса, обеспечивает соблюдение марковского свойства в любой момент времени.

Ограничения и допущения. Функционирование ИС ВН рассматривается на уровне детализации информационно-технического воздействия, как последовательность процедур, реализующих процесс СР и эксплуатации уязвимостей объектов воздействия – узлов вычислительной сети. Указанные процедуры определяют дискретное пространство состояний процесса.

Для марковского процесса имеет место более строгое ограничение на наличие свойства отсутствия последействия не только в моменты перехода случайного процесса, но и в любой другой момент, что обуславливает требование – закон распределения длительности ожидания переходов случайного процесса должен быть исключительно экспоненциальным (показательным).

Управляемыми СФХ являются: частоты конфигурирования *IP*-адресов узлов, номеров сетевых портов взаимодействия и доменных имен, а также

количество ЛСИО в подсети ИС ВН. Пусть применяемые ЛСИО, помимо имитации ложного состава и структуры ИС ВН, в целях реалистичности ее функционирования, также осуществляют генерацию ложного сетевого трафика, составляющего величину 10 Кбит/с. Приведенные данные позволяют оценить ресурсные ограничения на использование ЛСИО. В работе принято допущение, что ресурсные затраты канала передачи данных на формирование дополнительных ЛСИО прямо пропорциональны их количеству.

Также в исследовании вводится допущение о равновероятности (равновозможности) воздействий средств СР на все узлы подсети ИС ВН, включая ЛСИО (отсутствие априорной информации у злоумышленника относительно классов узлов).

Количественные ограничения на значения характеристик модели определяются, исходя из их физического смысла, структуры и технических характеристик оборудования ИС ВН, на основе которого функционирует объект моделирования [18].

Качественное описание модели конфигурирования структурно-функциональных характеристик информационных систем ведомственного назначения. Система эволюционирует (переходит из одного состояний в другое) под воздействием потока случайных событий, вероятностные характеристики которого в общем случае неизвестны. То есть, система с некоторого начального момента пребывает в состоянии i в течение случайного промежутка времени, распределенного по экспоненциальному закону, и после появления события, инициирующего эволюцию системы, осуществляет переход в состояние j с переходной вероятностью p_{ij} [13]. Тогда случайный процесс определяется следующими характеристиками:

дискретное конечное множество $\{S_i\}$ состояний системы размерностью n (см. табл. 1);

Таблица № 1

Характеристика дискретного пространства состояний объекта моделирования

№ п/п	Обозначение	Состояние процесса
1	S_1	Ожидание потока *ICMP*- и *DNS*-запросов злоумышленника по идентификации *IP*-адреса и маски подсетей, определения пути к целевым узлам ИС ВН
2	S_2	Ожидание вскрытия средств сетевой защиты и идентификации открытых сетевых портов ИС ВН (*IP*-адреса и маски подсетей идентифицированы злоумышленником)
3	S_3	Ожидание идентификации типов и версий операционных систем, сервисов и служб, используемого в ИС ВН программного обеспечения (средства сетевой защиты и открытые сетевые порты идентифицированы злоумышленником)
4	S_4	Ожидание узлом ИС ВН начала эксплуатации уязвимостей (типы и версии операционных систем, сервисы и службы, используемого программного обеспечения, идентифицированы злоумышленником)
5	S_5	Состояние, в котором злоумышленник вскрыл СФХ ИС ВН и осуществляет эксплуатацию уязвимостей ИС ВН

функции распределения $\{F_{ij}(t)\}$ непрерывных случайных величин $\{T_{ij}\}$ времени ожидания перехода системы из соответствующих состояний (см. табл. 2);

в исследовании используются функции распределения вида:

$$F_{ij}(t) = 1 - e^{-\lambda_{ij} t},$$

где, λ_{ij} – интенсивности потоков событий, приводящих к переходу системы из состояний i в j;

переходные вероятности полумарковской цепи $\{p_{ij}\}$;

Таблица № 2

Характеристика параметров функций распределения $F_{ij}(t)$ длительностей ожидания случайных событий, инициирующих эволюцию случайного процесса

№ п/п	Обозначение	Описание параметра
1	λ_{12}	Интенсивность потока *ICMP*- и *DNS*-запросов (определение пути к узлу ИС ВН и его активности) с учетом применения ЛСИО
2	λ_{23}	Интенсивность потока *TCP*- и *UDP*-запросов (определение открытых сетевых портов ИС ВН) с учетом применения ЛСИО
3	λ_{34}	Интенсивность потока *TCP*-, *UDP*- и *ICMP*-запросов (определение типа и версии операционных систем, сервисов и служб ИС ВН) с учетом применения ЛСИО
4	λ_{45}	Интенсивность потока событий по эксплуатации уязвимостей ИС ВН с учетом наличия в сети ЛСИО
5	λ_{21}	Интенсивность потока событий по конфигурированию *IP*-адресов узлов, изменяемых в рамках нескольких подсетей ИС ВН с учетом применения ЛСИО
6	λ_{31}	Интенсивность потоков событий по конфигурированию номеров сетевых портов, изменяемых в рамках пространства динамических портов с учетом применения ЛСИО
7	λ_{41}	Интенсивность потоков событий по конфигурированию доменных имен с учетом применения ЛСИО

произведение переходных вероятностей p_{ij} на соответствующие функции распределения $F_{ij}(t)$ представляют собой элементы $Q_{ij}(t)$ полумарковской матрицы Q. Процесс функционирования ИС ВН при конфигурировании ее СФХ, моделируемый полумарковским процессом, однозначно идентифицируется ориентированным графом, представленным на рис. 1.

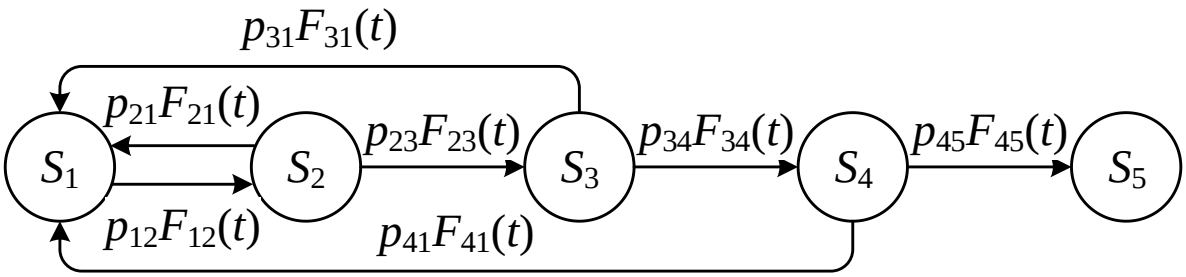


Рис. 1. – Ориентированный граф моделируемой системы

Исходя из принятого допущения о равновероятности воздействия средств СР на ИС ВН, поток запросов средств СР к ИС ВН, подвергается редукции пропорционально количеству узлов в ИС ВН:

$$\lambda_{12} = \frac{\lambda_{12}'}{1+z},$$

где, λ_{12}' – начальная интенсивность потока *ICMP*- и *DNS*-запросов злоумышленника; z – количество ЛСИО, формируемых средствами защиты ИС ВН.

В общем случае, искомыми вероятностно-временными характеристиками полумарковского процесса являются:

вероятности $P_{ij}(t)$ пребывания системы в состоянии j в момент времени t, при условии, что в момент времени $t = 0$, система находилась в состоянии i (интервально-переходные вероятности);

функция распределения $G_{ij}(t)$ времени первого посещения системой состояния j, при условии, что в момент времени $t = 0$, система находилась в состоянии i. Данная характеристика позволяет определить показатель защищенности ИС ВН, заявленный при постановке задачи на конфигурирование СФХ ИС ВН.

Количественное описание модели функционирования ИС ВН при конфигурировании СФХ в условиях СР. Определение значений $P_{ij}(t)$ полумарковского процесса осуществляется в следующей последовательности:

определение переходных вероятностей вложенной цепи Маркова исходя из следующего соотношения:

$$p_{ij} = \int_0^{\infty} f_{ij}(t) \prod_{k \neq i, k=1}^{n} (1 - F_{ik}(t)) dt,$$

где $f_{ij}(t) = \frac{dF_{ij}(t)}{dt}$ — функции плотности вероятности непрерывных случайных величин T_{ij} времени ожидания перехода системы из соответствующих состояний.

Определение безусловных функций распределения полного времени ожидания во всех состояниях:

$$F_i(t) = \sum_{j=1}^{n} p_{ij} f_{ij}(t),$$

Определение вероятностей того, что система не покинет соответствующие состояния в момент времени t:

$$\Psi_i(t) = 1 - F_i(t) = 1 - \sum_{j=1}^{n} p_{ij} f_{ij}(t),$$

Оценка вероятностей $P_{ij}(t)$ осуществляется на основе решения системы интегральных уравнений Вольтерра 2 рода с интегральным ядром разностного типа (типа «свертки»):

$$P_{ij}(t) = \delta_{ij} \Psi_i(t) + \sum_{k=1}^{n} p_{ik} \int_0^t f_{ik}(t) P_{kj}(t - \tau) d\tau,$$

где δ_{ij} – символ Кронекера: δ_{ij}=1 при i=j и δ_{ij}=0 при i≠j.

Как правило, решение подобных уравнений осуществляется с использованием преобразования Лапласа либо численных методов. Одностороннее преобразование Лапласа от функции $f(t)$ представляет собой выражение:

$$f(s)=\int_0^{\infty} e^{-st} f(t)dt.$$

Преобразование Лапласа является характеристическим преобразованием случайной величины, однозначно определяющее её функцию плотности распределения. В соответствии с теоремой о свертывании, преобразование Лапласа позволяет упростить решение сложных уравнений, в частности, система линейных интегральных уравнений с ядром разностного типа в форме преобразования Лапласа представляют собой систему линейных алгебраических уравнений в форме изображений, в которых интеграл с разностным ядром заменяется произведением функций $f_{ik}(s)P_{jk}(s)$ от комплексной переменной s. Применив преобразование Лапласа к системе линейных интегральных уравнений для интервально-переходных вероятностей $P_{ij}(t)$, получим:

$$P_{ij}(s)=\delta_{ij}\Psi_i(s)+\sum_{k=1}^{n} p_{ik} f_{ik}(s)P_{kj}(s),$$

Решение системы алгебраических уравнений в форме преобразования Лапласа в матричном виде имеют вид:

$$\mathbf{P}(s)=|\mathbf{I}-\mathbf{p}\times\mathbf{f}(s)|^{-1}\,\mathbf{\Psi}(s),$$

где $\mathbf{I}$ – единичная матрица размерностью n; символом «×» обозначено почленное произведение элементов матриц $\mathbf{p}$ и $\mathbf{f}(s)$.

Функции плотности распределения $g_{ij}(t)$ и распределения $G_{ij}(t)$ определяются из выражения в матричной форме как: $\mathbf{G}(s)=\frac{1}{s}\mathbf{g}(s)$,

$$\mathbf{g}(s)=\mathbf{p}\cdot\mathbf{f}(s)\cdot(\mathbf{I}-\mathbf{p}\cdot\mathbf{f}(s))^{-1}\cdot\left[\mathbf{I}\times(\mathbf{I}-\mathbf{p}\cdot\mathbf{f}(s))^{-1}\right]^{-1},\ \mathbf{G}(s)=\frac{1}{s}\mathbf{g}(s).$$

С использованием обратного преобразования Лапласа к матрице $P(s)$ определяется матрица искомых функций $P(t)$:

$$\mathbf{P}(t) = \lim_{x\to\infty} \frac{1}{2\pi j} \int_{x-j\omega}^{x+j\omega} e^{ts}\mathbf{P}(s)ds,$$

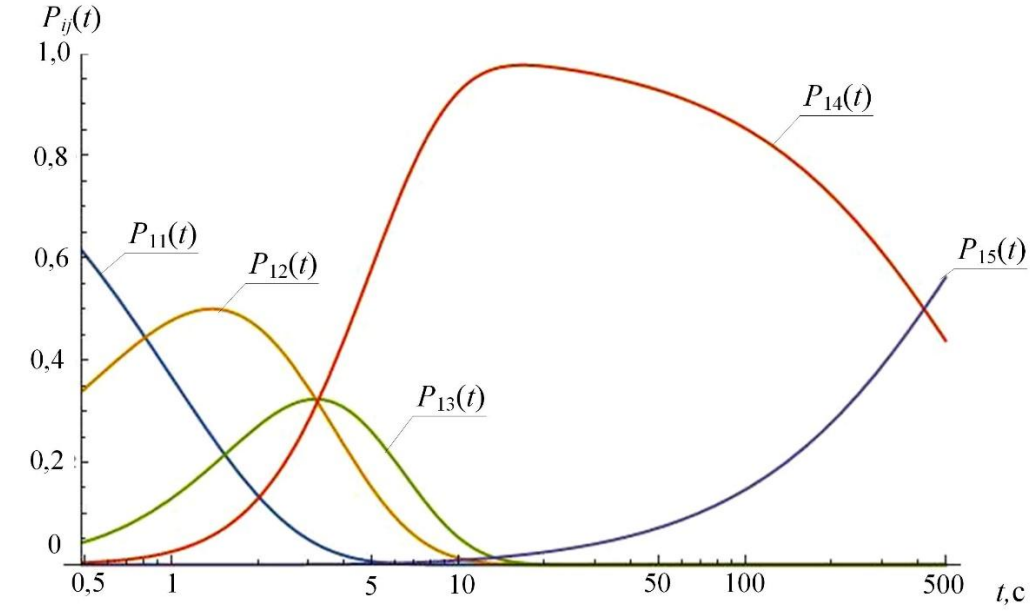
В общем случае, при реализации целенаправленных информационно-технических воздействий (*APT*-атак) на целевой узел ИС ВН, злоумышленник в перспективе достигнет своей цели по обходу системы защиты и эксплуатации выявленных уязвимостей. Проведенный анализ [19 - 21] показал, что злоумышленнику с высоким потенциалом для взлома целевой системы может потребоваться от нескольких часов до нескольких минут.

На рис. 2 представлены результаты расчетов с учетом неблагоприятных условий, когда злоумышленнику требуется в среднем 10 минут на преодоление средств защиты и вскрытие СФХ ИС ВН, то есть, интенсивность потока событий $\lambda_{45} = (600)^{-1}$ с$^{-1}$.

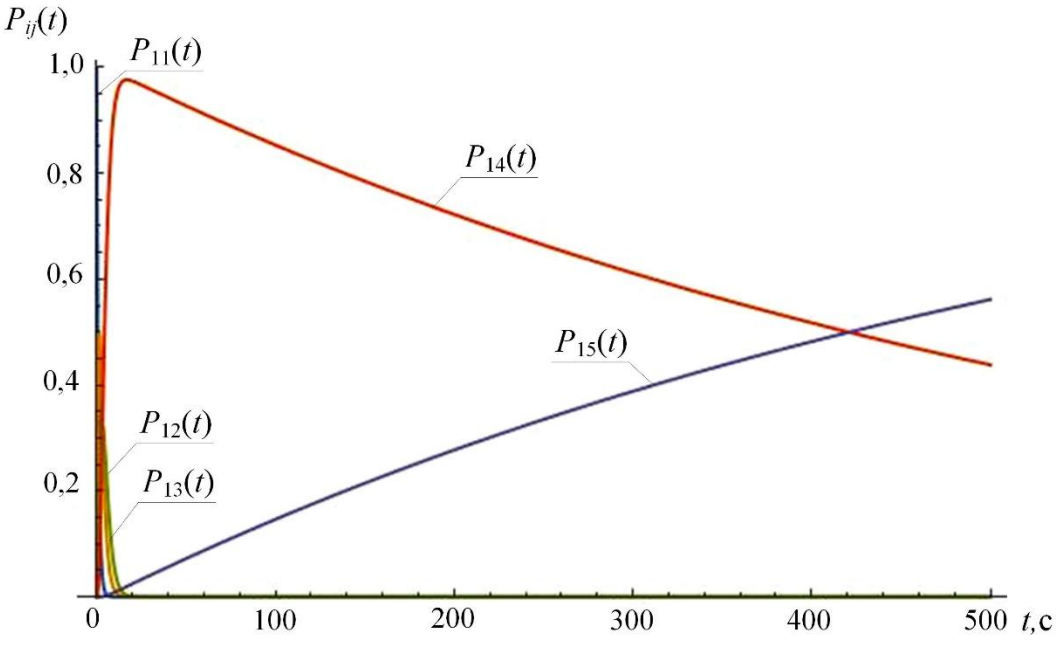
Расчет интервально-переходных вероятностей пребывания ИС ВН в состояниях моделируемого процесса показал, что, начиная с момента времени $t = 2$ по 400 с, целевая система преимущественно находится в благоприятном для злоумышленника состоянии S_4, в котором им идентифицированы все необходимые СФХ ИС ВН (*IP*-адреса и маски подсетей, средства защиты, открытые порты, типы и версии операционных систем, сервисы и службы) в связи с их статичностью, а злоумышленник, обладая неограниченным временным ресурсом, осуществляет поиск способа начала эксплуатации уязвимостей целевой системы.

С момента времени $t = 100$ с наблюдается монотонный рост вероятности достижения злоумышленником цели по началу эксплуатации уязвимостей с учетом принятых условий и ограничений. Так как состояние S_5 является поглощающим, то финальная вероятность данного состояния $p_5 = 1$, то есть злоумышленник обязательно достигнет своей цели, а расчет вероятностно-временных характеристик позволяет определить какой

временной ресурс для этого может потребоваться и при каких параметрах конфигурирования СФХ ИС ВН.



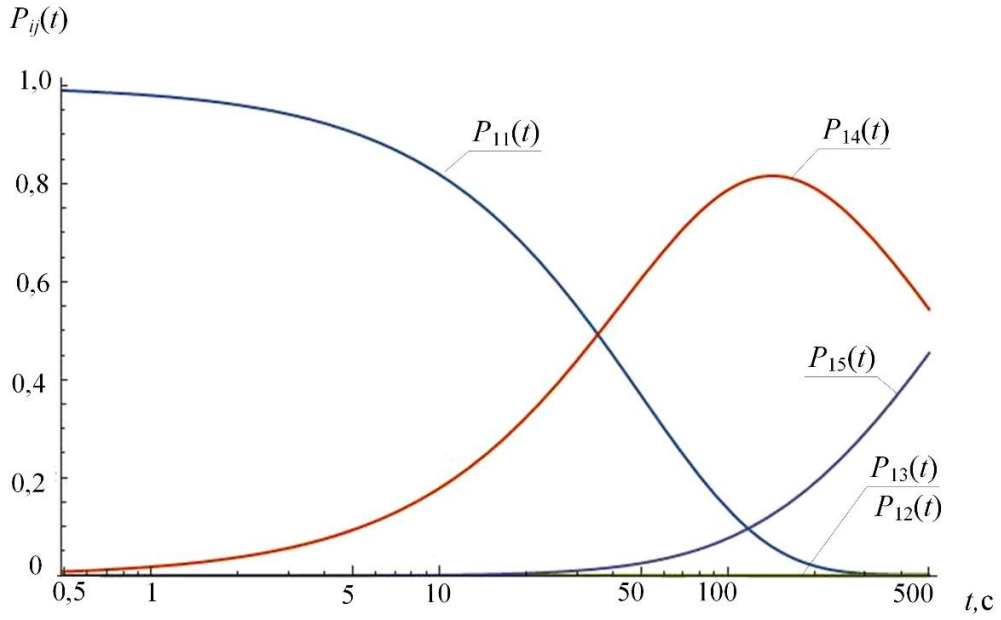
а)



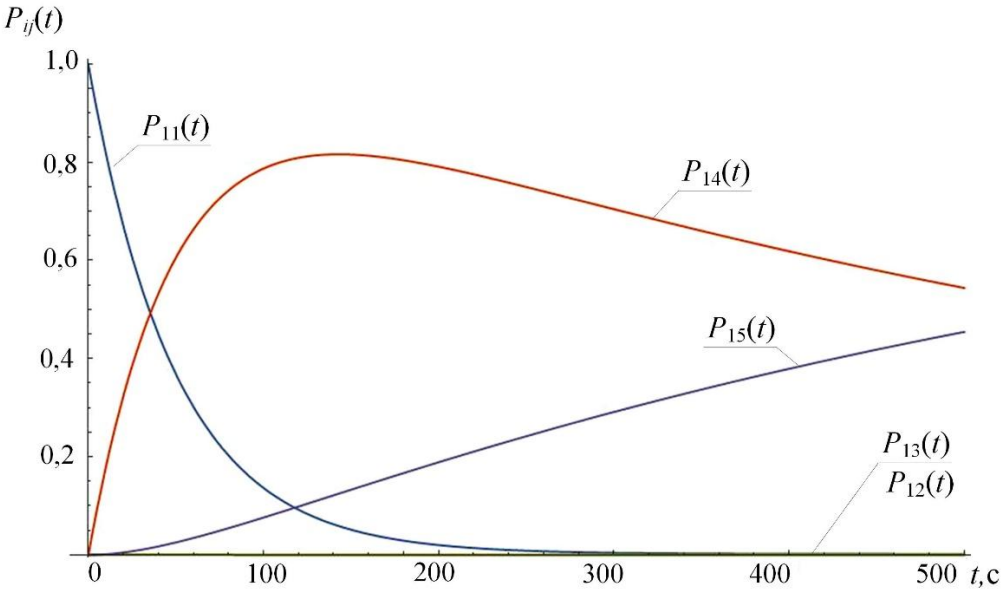
б)

Рис. 2. - Зависимость интервально-переходных вероятностей $P_{ij}(t)$ от времени без конфигурирования СФХ (рисунки а) и б) в логарифмической и линейной шкалах времени) при условиях: $P_{11}(0) = 1$, $\lambda_{45} = (600)^{-1}$ с$^{-1}$; $\lambda_{12} = 1$ с$^{-1}$

На рис. 3 представлены расчеты интервально-переходных вероятностей в условиях конфигурирования СФХ ИС ВН, применяющей ЛСИО.



а)



б)

Рис. 3 - Зависимость интервально-переходных вероятностей $P_{ij}(t)$ от времени при конфигурировании СФХ (рисунки а) и б) в логарифмической и линейной шкалах времени) в условиях: $z = 50$; $P_{11}(0) = 1$, $\lambda_{45} = (600)^{-1}$ с$^{-1}$; $\lambda_{12} = 1$ с$^{-1}$; $\lambda_{21} = (300)^{-1}$ с$^{-1}$; $\lambda_{31} = (300)^{-1}$ с$^{-1}$; $\lambda_{41} = (3600)^{-1}$ с$^{-1}$

При условии, что в подсети развернуто $z = 50$ ЛСИО, конфигурирование *IP*-адресов и сетевых портов осуществляется с частотой 1 раз в 5 минут ($\lambda_{21} = \lambda_{31} = (300)^{-1}$ с$^{-1}$), конфигурирование доменных имен осуществляется с частотой 1 раз в 1 час ($\lambda_{41} = (3600)^{-1}$ с$^{-1}$), в промежутке времени от 0 до 30 с, система преимущественно находится в начальном состоянии, в котором отсутствуют актуальные сведения и предпосылки для реализации угроз безопасности информации. Также произошло перераспределение вероятностей пребывания системы в неблагоприятных состояниях S_4 и S_5, имеет место тенденция к снижению вероятности достижения целей злоумышленника при фиксированных временных границах, приведенных на рис. 3.

С целью оценки влияния интенсивности активной СР, проводимой посредством сканирования (направления *ICMP*- и *DNS*-запросов) на рис. 4 приведены расчеты зависимостей интервально-переходных вероятностей от времени и интенсивности потока событий $P_{ij}(t, \lambda_{12})$.

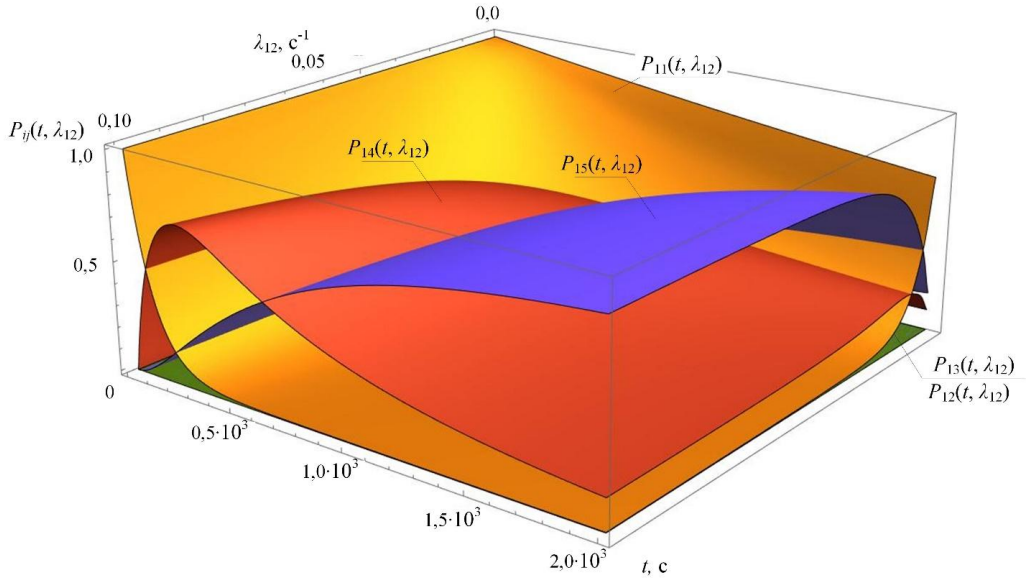


Рис. 4 - Зависимость интервально-переходных вероятностей $P_{ij}(t, \lambda_{12})$ от времени и интенсивности активной СР при конфигурировании СФХ в условиях: $z = 10$; $P_{11}(0, \lambda_{12}) = 1$, $\lambda_{45} = (600)^{-1}$ с$^{-1}$; $\lambda_{21} = (300)^{-1}$ с$^{-1}$; $\lambda_{31} = (300)^{-1}$ с$^{-1}$; $\lambda_{41} = (3600)^{-1}$ с$^{-1}$

Полученные результаты показали, что наибольшее влияние на характер вероятностно-временных характеристик, в частности, на вероятность перехода в поглощающее состояние, вызывает интенсивность активной СР, при которой воздействия средств разведки осуществляются чаще, чем 1 раз в минуту в условиях принятых ограничений и допущений.

Полученные результаты позволяют сделать вывод, что разработанная модель отражает взаимосвязь параметров конфигурирования СФХ ИС ВН и выходных характеристик, позволяющих определить режим настройки разработанных мер защиты и осуществить оценку защищенности ИС ВН при различных условиях ее функционирования.

Адекватность модели. Рассчитанные по модели вероятностно-временные характеристики соответствуют реальным свойствам процесса, так как структура модели соответствует последовательности действий, реализуемым при осуществлении различных воздействий средств СР (реализации компьютерных атак): корректного извлечения признаков инициирующих событий из реализации (дампа) трафика, стационарности в узком смысле и эргодичности случайного процесса, корректного использования методов математической статистики при обработке исходных данных и параметрической идентификации модели, корректного использования методов преобразования Лапласа.

Научная новизна модели заключается в применении математического аппарата теории полумарковских случайных процессов с дискретным пространством состояний и непрерывным временем для исследования процесса функционирования ИС ВН, применяющей ЛСИО.

Практическая значимость модели заключается в нахождении вероятностно-временных характеристик, описывающих состояния процесса функционирования ИС ВН, применяющей ЛСИО, при конфигурировании ее СФХ в условиях СР.

Литература

1. Cho J., Sharma D.P. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Commun. Surv. Tutor. 2020, 22, pp. 709-745.

2. Соколовский С.П., Орехов Д.Н. Концептуализация проблемы проактивной защиты интегрированных информационных систем // Научные чтения имени профессора Н.Е. Жуковского: сб. научн. стат. VIII Междунар. науч. метод. – Краснодар: КВВУ, 2018. С. 47-52.

3. Починок В.В., Шерстобитов Р.С., Теленьга А.П., Лебедкина Т.В., Кучуров В.В. Модель процесса мониторинга корректности фрагментации пакетов в ведомственной сети передачи данных //Инженерный вестник Дона, 2020, №5. URL: ivdon.ru/ru/magazine/archive/n5y2020/6493.

4. Лыков Н.Ю. Методика управления ресурсами маскираторов информационных направлений распределенных интегрированных инфокоммуникационных систем ведомственного назначения // Инженерный вестник Дона, 2018, №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5377.

5. Иванов И.И., Максимов Р.В. Этюды технологии маскирования функционально-логической структуры информационных систем // Инновационная деятельность в Вооруженных Силах Российской Федерации: сб. тр. участников всеармейской научно-практической конференции. – Санкт-Петербург, 2017. С. 147-154.

6. Keong Ch., Pan L., Xiang Y. Honeypot Frameworks and Their Applications: A New Framework // In SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore, 2018. – 81 p.

7. Andres S., Kenyon B., Birkolz E. Security Sage's Guide to Hardening the Network Infrastructure. – Sungress Publ., 2004. – 608 p.

8. Provos N., Holz T. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. – Addison Wesley, 2007. – 480 p.

9. Request for Comments: RFC 2131. Dynamic Host Configuration Protocol, 1997. URL: tools.ietf.org/html/rfc2131.

10. Request for Comments: 1034. Domain Names – Concepts and Facilities, 1987. URL: tools.ietf.org/html/rfc1034.

11. Request for Comments: 1035. Domain Names – Implementation and Specification, 1987. URL: tools.ietf.org/html/rfc1035.

12. Соколовский С.П., Максимов Р.В., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация. – 2020. – Т. 19. – №5. – С. 1018-1049.

13. Горбачев А.А. Модель и параметрическая оптимизация проактивной защиты сервиса электронной почты от сетевой разведки // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 69-81.

14. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. Москва: Наука. Гл. ред. физ.-мат. лит., 1991. – 384 с.

15. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. Москва: Наука, 1966. – 431 с.

16. Каплин М.А., Соколовский С.П., Горбачев А.А. Определение оптимальных параметров конфигурирования информационных систем в условиях сетевой разведки // Вопросы кибербезопасности. – 2022. – №4(50). – С. 80-90.

17. Соколовский С.П. Параметрическая оптимизация информационных систем при решении задачи управления сетевыми соединениями со средствами сетевой разведки // Информационные технологии. – 2022. – Т. 28. – №6. – С. 302-308.

18. Соколовский С.П. Параметрическая оптимизация информационных систем при решении задачи проактивной защиты сервиса передачи данных от

сетевой разведки //Вестник компьютерных и информационных технологий. – Т. 19 – №5(215). – 2022. – С. 49-57.

19. Бурховецкий А.С., Бухарин В.В., Казачкин А.В., Карайчев С.Ю. Метод защиты распределенных вычислительных сетей за счет формирования ложного информационного обмена // Информационные системы и технологии. – 2019. – №1(111). – С. 96-101.

20. Привалов А.А., Скуднева Е.В., Вандич А.П., Яичкин М.А. Метод повышения структурной скрытности сетей передачи данных оперативно технологического назначения ОАО «РЖД» // ТРУДЫ ЦНИИС. – 2016. – Т. 2(3) – С. 65-74.

21. Крылов В.В., Кравцов К.Н. Защита IP-подсетей от DDoS-атак и несанкционированного доступа методом псевдослучайной смены сетевых адресов // Вопросы защиты информации. – 2014. – №3. – С. 24-31.

References

1. Cho J., Sharma D.P. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Commun. Surv. Tutor. 2020, 22, pp. 709-745.

2. Sokolovskiy S. P., Orekhov D.N. Nauchnye chteniya imeni professora N.E. Zhukovskogo: sb. nauchn. stat. VIII Mezhdunar. nauch. metod. Krasnodar: KVVU, 2018. pp. 47-52.

3. Pochinok V.V., Sherstobitov R.S., Telen'ga A.P., Lebedkina T.V., Kuchurov V.V. Inzhenernyj vestnik Dona, 2020, №5. URL: ivdon.ru/ru/magazine/archive/n5y2020/6493.

4. Lykov N. Yu. Inzhenernyj vestnik Dona, 2018, №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5377.

5. Ivanov I.I., Maksimov R.V. Innovatsionnaya deyatel'nost' v Vooruzhennykh Silakh Rossiyskoy Federatsii: sb. tr. uchastnikov vsearmeyskoy nauchno-prakticheskoy konferentsii. Saint Petersburg, 2017. pp. 147-154.

6. Keong Ch., Pan L., Xiang Y. In SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore, 2018. 81 p.

7. Andres S., Kenyon B., Birkolz E. Security Sage's Guide to Hardening the Network Infrastructure. Sungress Publ., 2004. 608 p.

8. Provos N., Holz T. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison Wesley, 2007. 480 p.

9. Request for Comments: RFC 2131. Dynamic Host Configuration Protocol, 1997. URL: tools.ietf.org/html/rfc2131.

10. Request for Comments: 1034. Domain Names – Concepts and Facilities, 1987. URL: tools.ietf.org/html/rfc1034.

11. Request for Comments: 1035. Domain Names – Implementation and Specification, 1987. URL: tools.ietf.org/html/rfc1035.

12. Sokolovskiy S.P., Maksimov R.V., Voronchikhin I.S. Informatika i avtomatizatsiya. 2020. T. 19. №5. pp. 1018-1049.

13. Gorbachev A.A. Voprosy kiberbezopasnosti. 2022. №3(49). pp. 69-81.

14. Venttsel' E.S., Ovcharov L.A. Teoriya sluchaynykh protsessov i ee inzhenernye prilozheniya [Theory of random processes and its engineering applications]. Moskva: Nauka. Gl. red. fiz.-mat. lit., 1991. 384 p.

15. Gnedenko B.V., Kovalenko I.N. Vvedenie v teoriyu massovogo obsluzhivaniya [Introduction to mass service theory]. Moskva: Nauka, 1966. 431 p.

16. Kaplin M.A., Sokolovskiy S.P., Gorbachev A.A. Voprosy kiberbezopasnosti. 2022. №4(50). pp. 80-90.

17. Sokolovskiy S.P. Informatsionnye tekhnologii. 2022. T. 28. № 6. pp. 302-308.

18. Sokolovskiy S.P. Vestnik komp'yuternykh i informatsionnykh tekhnologiy. T. 19. №5(215). 2022. pp. 49-57.

19. Burkhovetskiy A.S., Bukharin V.V., Kazachkin A.V., Karaychev S.Yu. Informatsionnye sistemy i tekhnologii. 2019. №1(111). pp. 96-101.

20. Privalov A.A., Skudneva E.V., Vandich A.P., Yaichkin M.A. TRUDY TsNIIS. 2016. T. 2(3) pp. 65-74.

21. Krylov V.V., Kravtsov K.N. Voprosy zashchity informatsii. 2014. №3. pp. 24-31.