УДК: 681.5.015.24

В.В. Баранов[2], А.М. Крибель[1], О.С. Лаута[1], А.П. Нечепуренко[1]

[1]Россия, г. Санкт-Петербург, Военная академия связи им. С.М. Буденного
[2]Россия, г. Новочеркасск, Южно-Российский государственный политехнический университет имени М.И. Платова

ПРИМЕНЕНИЕ МЕТОДА ТОПОЛОГИЧЕСКОГО ПРЕОБРАЗОВАНИЯ СТОХАСТИЧЕСКИХ СЕТЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ

В докладе рассматривается топологическое преобразование стохастической сети средств защиты, используемых в ИТКС. Существующий подход к нейтрализации КА сводится к использованию разнородных средств защиты без учета их эффективности и взаимосвязи. Таким образом, требуется обосновать структуру системы защиты, устраняющую указанные недостатки.

Ключевые слова: компьютерная атака, информационно-телекоммуникационная сеть, вероятностно-временные характеристики, топологическое преобразование стохастической сети.

Требуемая защищенность информационных и программных ресурсов в настоящее время обеспечивается реализацией достаточного количества средств защиты, предотвращения их преодоления противником, выбором относительно стойких к вскрытию средств и алгоритмов защиты информации и рациональной сменой параметров защиты для каждой из преград

Процесс преодоления системы защиты будем моделировать как последовательность преодоления средств защиты противником. Средство защиты преодолено, если время его преодоления меньше времени между соседними изменениями параметров, тогда вероятность защищенности ИТКС от воздействия КА определим так [1]

$$P_{\text{защ}} = 1 - \prod_{m=1}^{k} P_{\text{преод}_m}, \qquad (1)$$

где k – количество средств защиты, которые необходимо преодолеть противнику;

$P_{\text{преод}_m}$ – вероятность преодоления противником m-ого средства защиты.

Для экспоненциальной аппроксимации распределений исходных характеристик и при их независимости [18]:

$$P_{\text{преод}_m} = \frac{\overline{t}_{fm}}{\overline{t}_{fm} + \overline{t}_{um}}, \quad (2)$$

где $\overline{t}_{fm}$ – среднее время между соседними изменениями параметров *m*-ого средства системы защиты;

$\overline{t}_{um}$ – среднее время преодоления *m*-ого средства системы защиты [1, 2].

Таким образом, с целью определения защищенности ИТКС первоначально необходимо определить среднее время между соседними изменениями параметров *m*-ого средства системы защиты и среднее время ($\overline{t}_{um}$) преодоления каждого средства системы защиты, т.е. ВВХ.

Для этого предлагается использовать профильные модели процесса преодоления противником средств защиты и метод топологического преобразования стохастических сетей.

Рассмотрим профильную модель преодоления КА вида «Вредоносные коды» антивирусной системы. Первоначально построим профильные модели всех способов реализации КА вида «Вредоносные коды». В качестве примера рассмотрим профильную модель КА «*Ransomware*».

2. Профильная модель КА вида «Вредоносные коды» при реализации способом «*Ransomware*», воздействующая на ПЭВМ (сервер), с установленной на них антивирусной системой:

– получение на порт ПЭВМ (сервера) пакета сообщения, зараженной вредоносным кодом «*Ransomware*» за среднее время $\overline{t}_{\text{нек.зап}}$ с функцией распределения *W(t);*

– дефрагментация сетевой картой ПЭВМ (сервера) указанного пакета за среднее время $\overline{t}_{\text{дефр}}$ с функцией распределения *M(t);*

– запуск сканера антивирусной системы и проверка антивирусной системой в оперативной памяти ПЭВМ (сервера) указанного пакета за среднее время $\overline{t}_{\text{пров}}$ с функцией распределения *L(t);*

– с вероятностью P_{I} преодоления антивирусной системы вредоносным кодом «*Ransomware*» за среднее время $\overline{t}_{\text{обнар}}$ с функцией распределения *B(t);*

– заражение ПЭВМ за среднее время $\overline{t}_{\text{блок}}$ с функцией распределения *O(t).*

Если пакет заблокирован, то с вероятностью (1-P_I) противник повторно направляет запрос за среднее время $\overline{t}_{повт}$ с функцией распределения *Z(t)*.

Требуется определить интегральную функцию распределения вероятности $F(t)$ и среднее время $\overline{t}_{um}$ преодоления антивирусной системы вредоносным кодом «*Ransomware*».

Математическая модель. Описанный выше процесс представим в виде стохастической сети (рисунок 1).

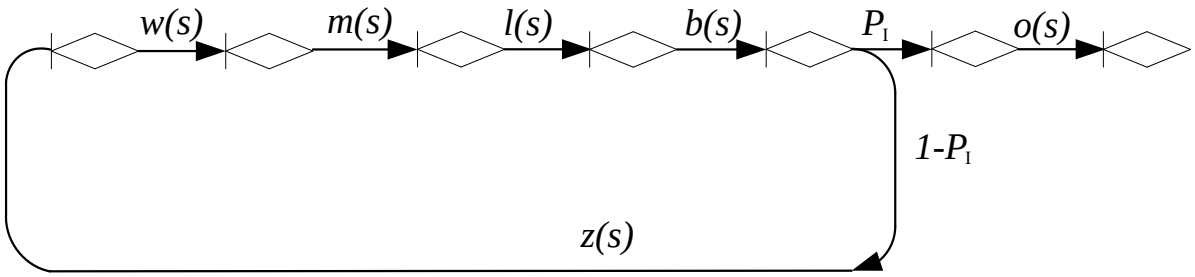

Рисунок 1 – Стохастическая сеть КА вида «Вредоносные коды» при реализации способом «*Ransomware*», воздействующая на ПЭВМ, с установленной антивирусной системой

Используя правила преобразования профильных моделей по правилам ТПСС, расчетные выражения для интегральной функции распределения вероятности и среднего времени реализации КА:

$$F(t) = \sum_{k=1}^{6} \frac{w \cdot m \cdot l \cdot b \cdot P_I \cdot o \cdot (z + s_k)}{\varphi'(s_k)} \cdot \frac{1 - \exp[s_k t]}{s_k}, \quad (3)$$

$$\overline{t}_{um} = \sum_{k=1}^{6} \frac{w \cdot m \cdot l \cdot b \cdot P_I \cdot o \cdot (z + s_k)}{\varphi'(s_k)} \cdot \frac{1}{(s_k)^2}. \quad (4)$$

Результаты расчетов ВВХ представлены на рисунке 2. В качестве исходных данных используются следующие значения:

$$\overline{t_{получ}} = 0{,}1 \text{ мин}; \overline{t_{дефр}} = 0{,}1 \text{ мин}; \overline{t_{пров}} = 1 \text{ мин}; \overline{t_{скан}} = 0{,}1 \text{ мин};$$
$$\overline{t_{блок}} = 0{,}1 \text{ мин}; \overline{t_{повт}} = 1 \text{ мин}; P_I = 0{,}1...0{,}9.$$

На втором этапе разрабатывается профильная модель работы ПЭВМ, с установленной антивирусной системой и при реализации КА вида «Вредоносные коды» при комплексном воздействии КА.

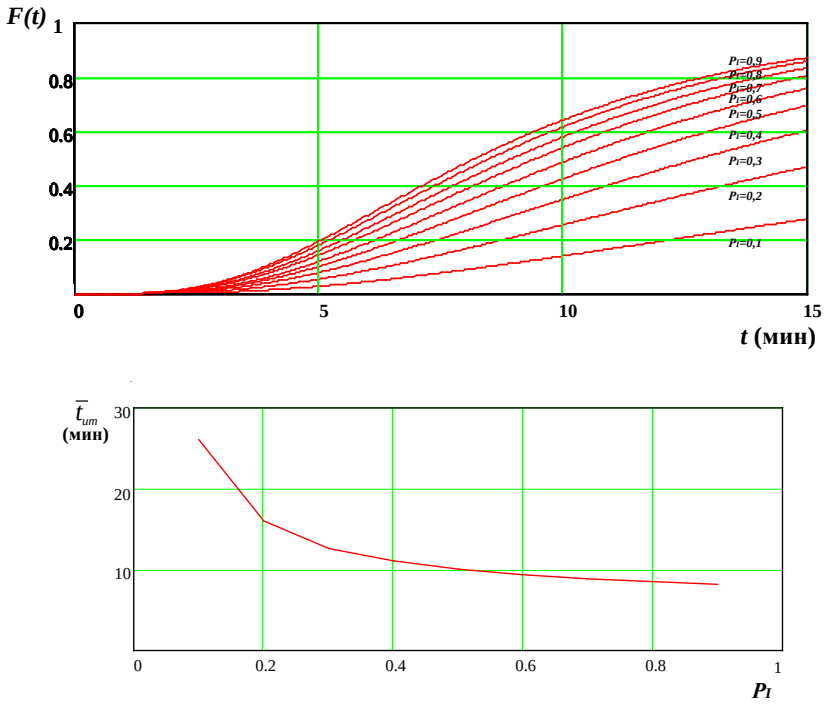

Рисунок 2 – Вероятностно-временные характеристики преодоления антивирусной системы КА вида «Вредоносные коды» при реализации способом «Ransomware»: а) зависимость интегральной функции распределения вероятности от времени преодоления антивирусной системы; б) зависимость среднего времени от вероятности преодоления антивирусной системы

2. Профильная модель при комплексном воздействии КА вида «Вредоносные коды»:

– с вероятностью P_{I} осуществляется преодоление антивирусной системы вредоносным кодом «*Ransomware*» за среднее время $\overline{t}_{RAM}$ с функцией распределения *B(t)*;

– с вероятностью P_{II} осуществляется преодоление антивирусной системы вредоносным кодом «Троянский конь» за среднее время $\overline{t}_{\text{ТК}}$ с функцией распределения *N(t)*;

– с вероятностью P_{III} осуществляется преодоление антивирусной системы вредоносным кодом *«Spyware»* за среднее время $\overline{t}_{SP}$ с функцией распределения *C(t)*;

– с вероятностью P_{IV} осуществляется преодоление антивирусной системы вредоносным кодом *«Knobe»* за среднее время $\overline{t}_{KN}$ с функцией распределения *P(t)*;

– с вероятностью P_{V} осуществляется преодоление антивирусной системы вредоносным кодом «Атака нулевого дня» за среднее время $\overline{t}_{\text{АНД}}$ с функцией распределения *M(t)*.

С обратной вероятностью компьютерная атака вида «Вредоносные коды» прекращает воздействие на каждом этапе, если вероятность преодоления на этом этапе больше 0,8 или изменены значения параметров антивирусной системы за среднее время $\overline{t}_{\text{повт}}$ с функцией распределения *Z(t)*.

Требуется определить интегральную функцию распределения вероятности $F(t)$ и среднее время $\overline{t}_{um}$ преодоления антивирусной системы.

Математическая модель. Описанный выше процесс представим в виде стохастической сети (рисунок 3)

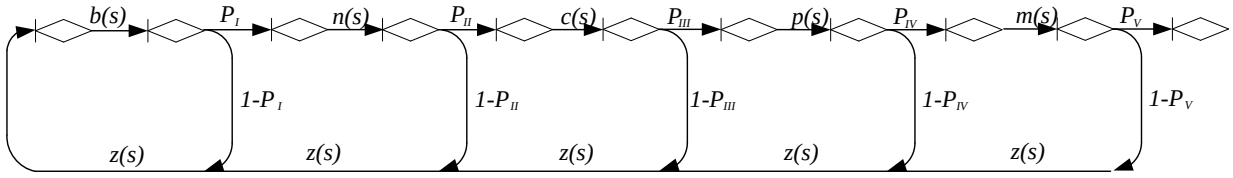

Рисунок 3 – Стохастическая сеть воздействия КА вида «Вредоносные коды» на ПЭВМ, с установленной антивирусной системой

Используя правила преобразования профильных моделей по правилам ТПСС (78), получены расчетные выражения для интегральной функции распределения вероятности и среднего времени реализации КА:

$$F(t)=\sum_{k=1}^{9}\frac{b\cdot P_{\text{I}}\cdot n\cdot P_{\text{II}}\cdot c\cdot P_{\text{III}}\cdot p\cdot P_{\text{IV}}\cdot m\cdot P_{\text{V}}\cdot(z+s_k)^5}{\varphi'(s_k)}\cdot\frac{1-\exp[s_k t]}{s_k}, \qquad (5)$$

$$\overline{t}_{um}=\sum_{k=1}^{9}\frac{b\cdot P_{\text{I}}\cdot n\cdot P_{\text{II}}\cdot c\cdot P_{\text{III}}\cdot p\cdot P_{\text{IV}}\cdot m\cdot P_{\text{V}}\cdot(z+s_k)^5}{\varphi'(s_k)}\cdot\frac{1}{(s_k)^2}. \qquad (6)$$

Результаты расчетов ВВХ представлены на рисунке 4. В качестве исходных данных используются следующие значения:

$\overline{t_{RAM}}=8$ мин; $\overline{t_{\text{ТК}}}=8$ мин; $\overline{t_{SP}}=8$ мин; $\overline{t_{KN}}=8$ мин; $\overline{t_{\text{АНД}}}=8$ мин; $\overline{t_{\text{повт}}}=1$ мин;

$P=0{,}1...0{,}9$; $P_{\text{II}}=0{,}1...0{,}9$; $P_{\text{III}}=0{,}1...0{,}9$; $P_{\text{IV}}=0{,}1...0{,}9$; $P_{\text{V}}=0{,}1...0{,}9$.

Полученные результаты показывают, что используемые в ИТКС средства защиты малоэффективны при противодействии комплексным КА. Это связано с тем, что существующий подход к нейтрализации КА сводится к использованию разнородных средств защиты без учета их эффективности и взаимосвязи.

Таким образом, требуется обосновать структуру системы защиты, устраняющую указанные недостатки.

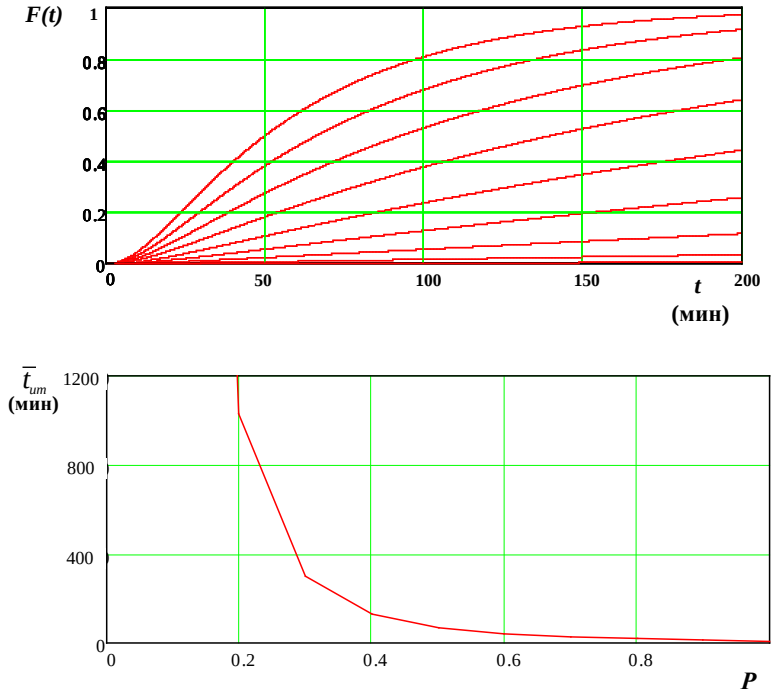

Рисунок 4 – Вероятностно-временные характеристики преодоления антивирусной системы КА вида «Вредоносные коды»:
а) зависимость интегральной функции распределения вероятности от времени преодоления антивирусной системы;
б) зависимость среднего времени от вероятности преодоления антивирусной системы

Литература

1. Берзин Е.А. Оптимальное распределение ресурсов и элементы синтеза систем. – М.: Советское радио, 1974. – 304 с.

2. Коцыняк М.А., Лаута О.С., Нечепуренко А.П., Штеренберг И.Г. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Труды учебных заведений связи. 2016. Т.2. № 4 С. 82-87.

3. Коцыняк М.А., Карганов В.В., Лаута О.С., Нечепуренко А.П. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия. Вопросы оборонной техники. Серия 1: Технические средства противодействия терроризму. 2016. № 9-10 (99-100). С. 54-57.