УДК 004.942

ПРЕДЛОЖЕНИЕ ПО ОЦЕНКЕ СПОСОБНОСТИ УЗЛА КОМПЬЮТЕРНОЙ СЕТИ ФУНКЦИОНИРОВАТЬ В УСЛОВИЯХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

Бегаев А.Н.[1], Гречишников Е.В.[2], Добрышин М.М.[3], Закалкин П.В.[4]

***Целью статьи** является разработка предложений, позволяющих повысить достоверность предсказания и оценки ущерба, наносимого информационно-техническими воздействиями узлам коммутации сети.*

***Метод исследования:** вероятностный подход оценки способности узла компьютерной сети предоставлять разное количество различных услуг связи заданному количеству абонентов, исходя из параметров информационно-технических воздействий.*

***Полученный результат:** создан инструментарий для инженерно-технического персонала для принятия решений о заблоговременной реконфигурации сети, что обеспечивает повышение защищенности узла от информационно-технических воздействий.*

***Ключевые слова:** сетевая компьютерная разведка, интеграция, статистические данные, прогнозирование ущерба, услуги связи.*

DOI: 10.21681/2311-3456-2018-3-02-08

Введение

Интеграция частных сетей связи различных компаний с Единой Сетью Электросвязи Российской Федерации (ЕСЭ РФ), наряду со значительными удобствами и удешевлением процесса организации связи (нет затрат на строительство и обслуживание линий связи), способствует тому, что злоумышленники активно применяют различные средства информационно-технических воздействий.

Статистические данные, фиксируемые ведущими организациями в сфере информационной безопасности [1, 2], исследования [3-13] и практический опыт защиты узлов компьютерной сети от различных компьютерных атак[5], показывают увеличение рейтингового и финансового ущерба [14]. Анализ существующих решений выявил ряд факторов [15], влияющих на низкую защищенность узла компьютерной сети от информационно-технических воздействий (ИТВ), вызванных, в том числе отсутствием оценки способности узла предоставлять различное количество услуг связи, различному количеству абонентов в условиях информационно-технических воздействий [16-18].

Постановка задачи на исследование

Разработанное предложение относится к области диагностирования и контроля технического состояния компьютерных сетей в условиях информационно-технических воздействий.

Задачей разработанного предложения является повышение достоверности предсказания и оценки ущерба, наносимого информационно-техническими воздействиями узлам коммутации сети в условиях ИТВ.

Низкая достоверность оценки наносимого ущерба, вызвана отсутствием учета способности злоумышленника своевременно вскрыть УзКС, своевременно воздействовать на него, а также учета влияния информационно-технических воздействий на предоставление различных услуг связи (в работе рассматриваются следующие услуги связи: видеоконференция, телефония и передача данных).

Порядок оценки способности узла компьютерной сети функционировать в условиях информационно-технических воздействий

Разработанная последовательность поясняется структурно–логической последовательностью представленной на рисунке 1, где в блоке 1 измеряют значения параметров однотипных сетей связи, интегрированных с ЕСЭ в условиях предоставления различных услуг связи различному количеству абонентов ($R_{iay}^{\text{укс}}$), где i –я однотипная сеть связи ($i = 1...I$, где I –количество однотипных сетей связи), a – количество абонентов узла КС, y – услуга связи; время начала работы $t_{\text{н.сеан.св}}$ и окончания работы $t_{\text{о.сеан.св}}$ каждого узла КС, время квазистационарного состояния $t_{\text{кссn}}$ каждого узла КС, значения параметров сетевой компьютерной разведки (СКР) ($P_{ij}^{\text{СР}}$) и ИТВ ($P_{ij}^{\text{ИТВ}}$) на однотипные функционирующие сети связи и где i –я однотипная сеть связи, $j - \text{é}$ злоумышленник ($j = 1,2,...J$, где J – количество злоумышленников) включающие максимальное $t_{\text{поискn}}^{\max}$ и минимальное значение $t_{\text{поискn}}^{\min}$ времени поиска злоумышленником каждого узла компьютерной сети, максимальное $t_{\text{распn}}^{\max}$ и минимальное значения времени распознавания $t_{\text{распn}}^{\min}$ злоумышленником каждого узла КС, время принятия решения необходимое злоумышленнику на $t_{\text{прn}}^{\text{вскр}}$ вскрытие и $t_{\text{прn}}^{\text{возд}}$ воздействие на каждый УзКС, времени вскрытия $t_{\text{вскрn}}$ узла КС, время воздействия $t_{\text{воздn}}$ злоумышленником на каждый узел КС, объём I_n – используемого $n-\text{м}$

1 Бегаев Алексей Николаевич, кандидат технических наук, генеральный директор, АО «Эшелон-СЗ», г. Санкт-Петербург, Россия. E-mail: a.begaev@nwechelon.ru.

2 Гречишников Евгений Владимирович, доктор технических наук, профессор, Академия ФСО России, г. Орел, Россия.

3 Добрышин Михаил Михайлович, кандидат технических наук, Академия ФСО России, г. Орел, Россия. E -mail: Dobrithin@ya.ru.

4 Закалкин Павел Владимирович, кандидат технических наук, Академия ФСО России, г. Орел. Россия.

5 www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf

Способ оценки способности узла компьютерной сети функционировать в условиях информационно-технических воздействий

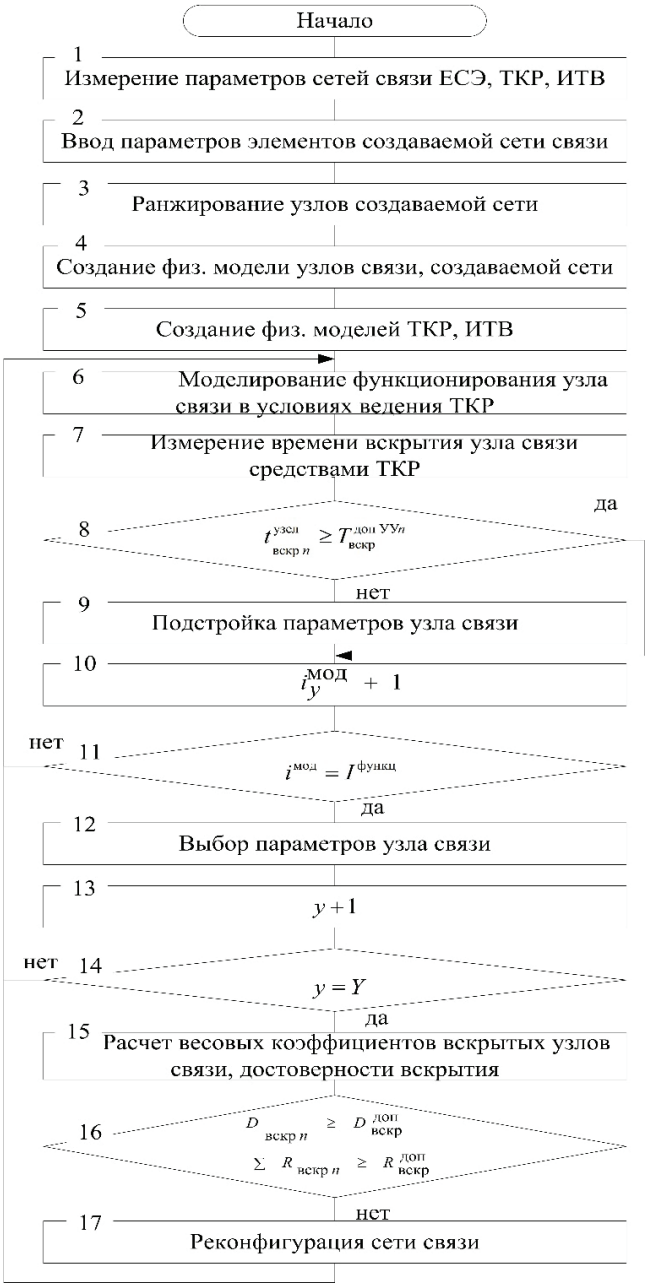

Рис.1. (начало)

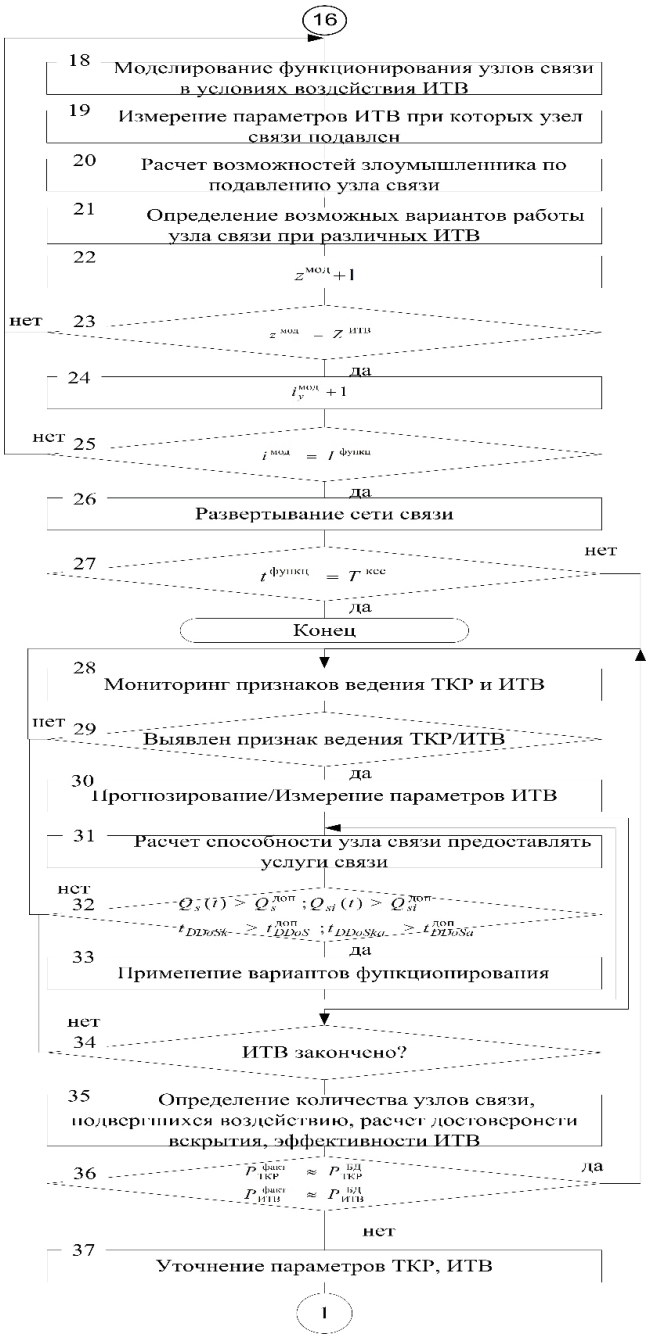

Рис.1. (окончание)

УзКС цифрового потока информации, количество связей (направлений) S_n – n – го УзКС. Присваивают каждой функционирующей УзКС в сегменте ЕСЭ номер.

В блоке 2 задают значения параметров, характеризующие узлы создаваемой сети.

В блоке 3 ранжируют УзКС, исходя из важности передаваемой информации, определяют весовые коэффициенты согласно [15]:

$$R_n = \left(\frac{I_n}{\sum_{n=1}^{N} I_n} + \frac{S_n}{\sum_{n=1}^{N} S_n} \right) \cdot \frac{1}{2} \qquad (1)$$

где I_n – используемый n–м УзКС цифровой поток информации; S_n – количество связей (направлений) n–го УзКС.

В блоке 4 формируют модель УзКС в условиях предоставления различных услуг связи различному количеству абонентов. Созданной модели задают требуемые параметры P^{cc}_{sr}, где s – номер УзКС, r – номер технического параметра.

В блоке 5 формируют модели СКР и ИТВ различных злоумышленников учитывающие параметры средств СКР (P^{CP}_{ij}) и ИТВ ($P^{ИТВ}_{ij}$).

В блоке 6 моделируют совместное функционирование узла связи с учетом предоставления различных услуг связи различному количеству абонентов и проведение злоумышленником СКР.

В блоке 7 измеряют время вскрытия СКР УзКС.

В блоке 8 сравнивают измеренные значения времени вскрытия УзКС с допустимыми:

$$t^{\text{узел}}_{\text{вскр}\,n} \geq T^{\text{доп УУ}n}_{\text{вскр}}, \quad (2)$$

где $t^{\text{узел}}_{\text{вскр}\,n}$ – измеренное время вскрытия n–го УзКС, $T^{\text{доп УУ}n}_{\text{вскр}}$ – допустимое время вскрытия УзКС.

Если значения времени вскрытия узла КС не удовлетворяют выражению 2, в блоке 9 осуществляют подстройку параметров УзКС под параметры выбранной функционирующей КС в сегменте ЕСЭ. Повторно моделируют процесс совместного функционирования УзКС и СКР.

В блоке 10 прибавляется 1 к количеству итераций, и осуществляют повторное моделирование до тех пор, пока не будет выполнено условие в выражении 1,2 или не будут перебраны все КС, функционирующие в сегменте ЕСЭ (блок 11).

$$i^{\text{мод}} = I^{\text{функц}}, \quad (3)$$

где $i^{\text{мод}}$ – количество итераций, $I^{\text{функц}}$ – количество КС, функционирующие в сегменте ЕСЭ.

Если условие выражения 2 не было выполнено, а условие выражения 3 выполнено, в блоке 12 выбирают значения параметров КС, при которых время вскрытия больше чем у остальных вариантов. При наличии нескольких одинаковых максимальных значений оператор выбирает значения параметров самостоятельно.

В блоке 13 прибавляется 1 к количеству итераций и повторно осуществляют процесс моделирования до тех пор, пока не будет выполнено условие в выражении 1, 2 или не будут перебраны все КС, функционирующие в сегменте ЕСЭ (блок 14).

В блоке 15 рассчитывают значения весовых коэффициентов вскрытых ($R_{\text{вскр}}$) УзКС согласно выражения:

$$R_{\text{вскр}} = \sum_{n=1}^{N} i_n^{\text{вскр}} R_n, \quad (4)$$

где $i_n^{\text{вскр}}$ – логический коэффициент вскрытия $n-$го узла, R_n – весовой коэффициент $n-$го узла КС.

Расчёт вскрытых узла КС осуществляется согласно выражения:

$$N'_{\text{эсс}\,n} = \sum_{n=1}^{N} i_n^{\text{вскр}} R_{\text{эсс}\,n}, \quad (5)$$

где $N'_{\text{эсс}\,n}$ – предполагаемое количество вскрытых УзКС; $N_{\text{эсс}\,n}$ – $n-$й УзКС.

Расчёт достоверности вскрытия КС ($D_{\text{вскр}}$) осуществляется согласно выражения:

$$D_{\text{вскр}} = \frac{N'^{\text{вскр}}_{\text{эсс}}}{N_{\text{эсс}}}, \quad (6)$$

В блоке 16 осуществляется оценка достоверности вскрытия КС злоумышленником согласно критериям:

$$D_{\text{вскр}} \leq D_{\text{пор.вскр}}, \quad (7)$$

где $D_{\text{пор.вскр}}$ – пороговая достоверность вскрытия КС.

$$\sum_{n=1}^{N} R_{\text{вскр}\,n} \leq R_{\text{пор.вскр}}, \quad (8)$$

где $\sum_{n=1}^{N} R_{\text{вскр}\,n}$ – сумма весовых коэффициентов вскрытых УзКС, допустимое значение суммы весовых коэффициентов вскрытых УзКС.

Если достоверность вскрытия КС ($D_{\text{вскр}}$) или сумма весовых коэффициентов вскрытых УзКС ($\sum_{n=1}^{N} R_{\text{вскр}\,n}$) не удовлетворяют (7,8), то в блоке 17 производят реконфигурацию структуры и топологии КС до выполнения указанных условий.

Если условия 7, 8 выполнены, то в блоке 18 осуществляют совместное функционирование моделей узла КС и ИТВ.

В блоке 19 измеряют время подавления и значения параметров средств ИТВ.

В блоке 20 оценивают возможности злоумышленника по подавлению УзКС и своевременности подавления УзКС.

В блоке 21 определяют режимы работы, количество абонентов и предоставляемых услуг связи при различных значениях параметров ИТВ, при которых УзКС способен выполнять свои функциональные задачи.

В блоке 22 прибавляется 1 к количеству итераций различных параметров ИТВ.

В блоке 23 сравнивают количество итераций различных параметров ИТВ и заданного количества параметров ИТВ.

В блоке 24 прибавляется 1 к количеству итераций, после чего в блоке 25 сравнивают количество итераций и количества КС функционирующих в сегменте ЕСЭ.

В блоке 26 осуществляют развертывание и функционирование КС, а в блоке 27 определяют окончание функционирование сети связи.

В блоке 28 во время функционирования КС проводят непрерывный мониторинг состояния КС. На основании выбранных критериев фиксируют факт ведения СКР и ИТВ в отношении УзКС.

В блоке 29 при отсутствии признаков ведения СКР или ИТВ, продолжают мониторинг состояния КС. Если выявлен признак (признаки) ведения СКР или ИТВ, в блоке 30 измеряют параметры ИТВ.

В блоке 31 на основании данных полученных о параметрах ИТВ прогнозируют способность узла КС выполнять свои функциональные задачи:

Рассчитывают вероятность предоставления у–й услуги связи ($Q_y(t)$) и вероятность предоставления ($Q_{ay}(t)$) группы услуг связи (в качестве примера представлен расчет вероятности предоставления услуг связи в условиях DDoS–атак [19]:

$$Q_y(t_{\text{ксс}}) = e^{-\frac{\left(\frac{R_{botnet}(t_{\text{ксс}})}{R_{\text{СЗ}}}\right)\cdot\left(\frac{R_y}{R_{\text{кан}}-R_{\text{атак}}(t_{\text{ксс}})}\right)\cdot t_{\text{ксс}}}{\overline{T}_{\text{атак}}}}, \quad (9)$$

$$Q_{ay}(t_{\text{ксс}}) = e^{-\frac{\left(\frac{R_{botnet}(t_{\text{ксс}})}{R_{\text{СЗ}}}\right)\cdot\left(\frac{\sum_{a=1}^{A}\sum_{y=1}^{Y} R_y}{R_{\text{кан}}-R_{\text{атак}}(t_{\text{ксс}})}\right)\cdot t_{\text{ксс}}}{\overline{T}_{\text{атак}}}}, \quad (10)$$

где $R_{botnet}(t_{\text{ксс}})$ – быстродействие атакующей сети злоумышленника; $R_{\text{СЗ}}$ – способность средств противодействия ИТВ, минимизировать деструктивное воздействие на узел КС; R_y – сетевой ресурс, необходимый для обеспечения у–й услуги связи;

$\sum_{a=1}^{A}\sum_{y=1}^{Y} R_y(t)$ – сетевой ресурс, необходимый для обеспечения группы услуги связи, абонентам а–категории; $R_{\text{кан}}$ – имеющийся сетевой ресурс; $R_{\text{атак}\,(t_{\text{кcc}})}$ – фактическая мощность атаки сети злоумышленника, $t_{\text{кcc}}$ – время квазистационарного состояния узла КС, $T_{\text{атак}}$ – среднее время атаки злоумышленником на узел КС.

Определяют время отказа в обслуживании у–й услуги связи и группы услуг связи для абонентов [19]:

$$t_{DDoS\,y} = \frac{\left(R_y + R_{\text{атак}}(t_{\text{кcc}})\right)\cdot R_{botnet}(t_{\text{кcc}})\cdot t_{\text{кcc}}}{R_{\text{кан}}\cdot R_{\text{СЗ}}\cdot \ln\left(1-P_{\text{подавл}\,y}\right)}, \quad (11)$$

$$t_{DDoS\,ay} = \frac{\left(\sum_{a=1}^{A}\sum_{y=1}^{Y} R_y + R_{\text{атак}}(t_{\text{кcc}})\right)\cdot R_{botnet}(t_{\text{кcc}})\cdot t_{\text{кcc}}}{R_{\text{кан}}\cdot R_{\text{СЗ}}\cdot \ln\left(1-P_{\text{подавл}\,y}\right)}. \quad (12)$$

где $P_{\text{подавл}\,y}$ – вероятность подавления у–й услуги связи (определяется экспериментально).

При проведении практических экспериментов по подавлению отдельных услуг связи средствами DDoS–атак, выявлено, что отказ в обслуживании видеоконференции наступает при вероятности подавления равной 0,85; телефонии – 0,95, а передачи данных при вероятности подавления превышающей 0,999.

В блоке 32 сравнивают вероятность предоставления у–й услуги связи ($Q_y(t)$), вероятность предоставления нескольких услуг связи ($Q_{ay}(t_{\text{кcc}})$) а–ой категории абонентов и время отказа в обслуживании услуги связи ($t_{DDoS\,y}$) и время отказа в обслуживании группы услуг связи ($t_{DDoS\,ay}$) с допустимыми значениями:

$$Q_y(t_{\text{кcc}}) > Q_y^{\text{доп}}, \quad (13)$$

$$Q_{yi}(t_{\text{кcc}}) > Q_{yi}^{\text{доп}}, \quad (14)$$

$$t_{DDoS\,y} > t_{DDoS}^{\text{доп}}, \quad (15)$$

$$t_{DDoS\,ay} > t_{DDoS}^{\text{доп}}. \quad (16)$$

Если выражения 13 – 16 выполняются, продолжают мониторинг (блок 28). Если выражения 13 – 16 не выполняются, в блоке 33 применяют варианты функционирования при различных ИТВ, используя базу данных полученных в блоке 21.

Если деструктивное воздействие злоумышленника на КС окончено (блок 34), то в блоке 35 измеряют количество УзКС подвергшихся деструктивному воздействию и УзКС, подавленные средствами ИТВ. Определяют достоверность вскрытия УзКС средствами СКР. Определяют эффективность ведения ИТВ злоумышленником.

В блоке 36 сравнивают фактические значения параметров деструктивного воздействия на УзКС с аналогичными параметрами, имеющимися в базе данных.

$$P_{\text{СКР}}^{\text{факт}} \approx P_{\text{ТКР}}^{\text{БД}}, \quad (17)$$

$$P_{\text{ИТВ}}^{\text{факт}} \approx P_{\text{ИТВ}}^{\text{БД}}, \quad (18)$$

где $P_{\text{СКР}}^{\text{факт}}$, $P_{\text{ИТВ}}^{\text{факт}}$ – значения фактических параметров, характеризующих ведение СКР и ИТВ соответственно, $P_{\text{СКР}}^{\text{БД}}$, $P_{\text{ИТВ}}^{\text{БД}}$ – значения параметров, характеризующих ведение СКР и ИТВ соответственно имеющиеся в базе данных.

В том случае, если указанные значения параметров деструктивного воздействия соответствуют имеющимся значениям в базе данных, продолжают мониторинг состояния КС. Если указанные значения параметров деструктивного воздействия на КС не соответствуют имеющимся значениям, или параметры КС, подвергшейся воздействию, не соответствуют заданным значениям, то в блоке 37 уточняют значения параметров СКР и ИТВ и дополняют базу данных (блок 1).

Выводы

Использование разработанного предложения позволяет на основании вероятностного подхода предсказать и оценить ущерб, наносимый информационно-техническими воздействиями узлам коммутации сети. На основании оценки ущерба, инженерно-технический персонал принимает решение о заблаговременной реконфигурации компьютерной сети.

Оценка эффективности предлагаемого предложения проводилась на основании сравнения достоверности результатов моделирования КС и ИТВ с одним из известных решений [20, 21]. Одним из определяющих параметров достоверности результатов моделирования является вероятность ошибки. Оценка вероятности ошибки $P(|\,p^*_{\partial\,в} - p_{\partial\,в}\,| < \varepsilon)$ [22] проводилась согласно выражению:

$$P(|\,p^*_{\partial.в} - p_{\partial.в}\,| < \varepsilon) = 2\Phi\left[\frac{\varepsilon\sqrt{N}}{\sqrt{p^*_{\partial.в}\cdot(1-p^*_{\partial.в})}}\right], \quad (19)$$

где: Φ – функция Лапласа; ε – величина доверительного интервала; N – количество имитируемых услуг связи; $p^*_{\partial.в}$ – средняя статистическая вероятность моделирования; $p_{\partial.в}$ – минимальная вероятность моделирования.

Расчет достоверности оценки моделирования проводился при следующих исходных значениях, $\varepsilon = 0,02$; $N = 1$ (для известного решения); $\varepsilon = 0,02$; $N = 6$ (в качестве примера взяты 3 услуги связи: передача данных, IP–телефония, видеоконференцсвязь. В качестве примера выбраны 2 категории абонентов. Таким образом $N = 3\times 2 = 6$); $p^*_{\partial.в} = 0,99$.

Исходя из сравнения основных показателей способа прототипа и заявленного способа следует вывод, что заявленный способ повышает достоверность результатов моделирования путем оценки способности узла КС предоставлять различное количество услуг КС, различному количеству абонентов в условиях противодействия ИТВ, на 4,4 %.

Таким образом, поставленная задача по разработке предложения обеспечивающего повышение защищенности узла компьютерной сети от информационно-технических воздействий, за счет повышения достоверности результатов оценки способности узла предоставлять различное количество услуг связи, различному количеству абонентов в условиях ИТВ.

Повышение достоверности оценки наносимого ущерба, осуществляется за счет учета способности злоумышленника своевременно вскрыть УзКС, сво-

евременно воздействовать на него, а также за счет учета влияния информационно-технических воздействий на предоставление различных услуг связи (в работе рассматриваются следующие услуги связи: видеоконференция, телефония и передача данных).

Научная новизна разработанного предложения заключается в том, что оно позволяет: учесть новые параметры, характеризующие процесс подавления узла компьютерной сети, получить временное представление и новые зависимости характеризующие данный процесс. Элементы разработанного предложения частично реализованы в патенте РФ на изобретение [23] и 2 программах для ЭВМ [24, 25].

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. Гарнаева М.А., Макрушин Д.Н., Иванов А.М., Наместников Ю.В., Ван дер Вил Йорнт. Kaspersky Security Bulletin: цифры года и прогнозы-2016 // Защита информации. Инсайд. 2016. № 1 (67). С. 47-53.
2. Гарнаева М.А., Функ К. Kaspersky Security Bulletin 2013 // Вопросы кибербезопасности. 2014. № 3 (4). С. 65-68.
3. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. СПб.: Изд-во «Наукоемкие технологии», 2017. 120 с.
4. Еремеев М.А., Аллакин В.В., Будко Н.П. Модель наступления критического события информационной безопасности в информационно-коммуникационной системе // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 6. С. 52-60.
5. Калашников А.О., Бурса М.В., Остапенко Г.А. Мультисервисные сети: дискретная риск-модель HTTP-флуда // Вопросы кибербезопасности. 2015. № 1 (9). С. 49-54.
6. Косенко М.Ю., Мельников А.В. Вопросы обеспечения защиты информационных систем от ботнет атак // Вопросы кибербезопасности. 2016. № 4 (17). С. 20-28.
7. Новиков С.В., Зима В.М., Андрушкевич Д.В. Организация защиты информации в гетерогенных вычислительных сетях // Защита информации. Инсайд. 2014. № 3 (57). С. 50-55.
8. Паршуткин А.В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.
9. Слесарчик К.Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1 (25). С. 19-27.
10. Стародубцев П.Е., Смирнов Д.В. Построение многоуровневой защиты корпоративных информационных систем с применением обманных технологий // Известия Института инженерной физики. 2017. Т. 1. № 43. С. 68-71.
11. Тарасов Я.В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5 (24). С. 23-29.
12. Begaev A., Chesnakov M., Starodubtsev Yu. Method of Mixed Traffic Model Formation. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 1-5.
13. Starodubtsev Yu.I., Grechishnikov E.V., Komolov D.V. Use of neural networks to ensure stability of communication networks in conditions of external impacts. Telecommunications and Radio Engineering. 2011. V. 70. N 14. P. 1263-1275.
14. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. СПб.: Изд-во Политехн. ун-та, 2017. 454 с.
15. Добрышин М.М., Диденко П.М. Оценка защищённости беспроводных сетей связи // II Международная научно–техническая конференция «Радиотехника, электроника и связь» – Омск. – 2013. – С. 155–159.
16. Анисимов В.В., Бегаев А.Н., Стародубцев Ю.И. Модель функционирования сети связи с неизвестным уровнем доверия и оценки её возможностей по предоставлению услуги VPN с заданным качеством // Вопросы кибербезопасности. 2017. № 1 (19). С. 6-15. DOI: 10.21681/2311-3456-2017-1-6-15.
17. Бегаев А.Н., Стародубцев Ю.И., Фёдоров В.Г. Методика оценки управляемости фрагмента сети связи общего пользования с учетом влияния множественности центров управления и деструктивных программных воздействий. Вопросы кибербезопасности. 2017. № 4 (22). С. 32-39. DOI: 10.21681/2311-3456-2017-4-32-39.
18. Гречишников Е.В., Добрышин М.М., Закалкин П.В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4-12.
19. Гречишников Е.В. и др. Оценка способности узла виртуальной частной сети предоставлять услуги связи в условиях противодействия и DDoS–атакам // Сборник трудов научно–практической конференции «Проблемы технического обеспечения войск в современных условиях» Военная академия связи им. С.М. Буденного, Санкт–Петербург, – 2016. – С.48–51.
20. Пат. 22405184 РФ, МПК G05B 23/00, G06F 17/50 (2006.01) Способ обеспечения устойчивого функционирования системы связи / Гречишников Е.В., Дыбко Л.К., Ерышов В.Г., Жуков А.В., Стародубцев Ю.И. – 2009117902/08, заявл. 12.05.2009; опубл. 27.11.2010. – 17 с.
21. Пат. 2541205 РФ, МПК G05B 23/00, G06F 21/55 (2013.01) Способ оценки эффективности информационно – технических воздействий на сети связи / Гречишников Е.В., Белов А.С., Добрышин М.М., Исаченко В.Г., Кузмич А.А. – 2013134627/8, заявл. 23.07.2013; опубл. 10.02.2015. – 21 с.
22. Вентцель Е.С. Теория вероятности и ее инженерное приложение. М.:Наука, 1988, 463 с.
23. Пат. 2648508 РФ, МПК G05B 23/00 (2006.01), G06F 21/00 (2013.01), G06N 5/00 (2006.01) Способ оценки способности узла компьютерной сети функционировать в условиях информационно-технических воздействий / Гречишников Е.В., Добрышин М.М., Закалкин П.В., Горелик С.П., Белов А.С., Скубьев А.В. – 2016151502, заявл. 26.12.2016; опубл. 26.03.2018 – 33 с.
24. Свидетельство о государственной регистрации программы для ЭВМ № 2017616948. Расчет возможностей узла компьютерной сети предоставлять услуги связи в условиях DDoS–атак с учетом различных способов минимизации деструктивного воздействия / М. М. Добрышин и др. – опубл. 26.04.2017.
25. Свидетельство о государственной регистрации программы для ЭВМ № 2018610012. Расчет времени наступления отказа в обслуживании группы услуг (услуги) связи в условиях DDoS–атак с учетом возможности перераспределения предоставляемых услуг связи. / М. М. Добрышин, Р. В. Гуцын, А. Н. Реформат. – опубл. 09.01.2018.

Рецензент: *Марков Алексей Сергеевич, доктор технических наук, профессор кафедры ИУ-8 МГТУ им.Н.Э.Баумана, г.Москва, **a.markov@bmstu.ru***

THE OFFER ON ASSESSMENT OF ABILITY OF COMPUTER NETWORK NODE TO FUNCTION WITHIN THE CONDITIONS OF INFORMATION AND TECHNICAL INFLUENCES

Begaev A.N.[6], Grechishnikov E.V.[7], Dobryshin M.M.[8], Zakalkin P.V.[9]

The purpose of article is development of the offers allowing to increase reliability of a prediction and assessment of the damage caused by information and technical influences to knots of switching of a network. A research method probabilistic approach of an assessment of ability of knot of a computer network to provide different quantity of various communication services to the set number of subscribers proceeding from parameters of information and technical influences. The received result is created tools for technical personnel for making decisions on preliminary reconfiguration of a network that provides increase of security of knot from information and technical influences.

Keywords: information and technical influences, network computer investigation, prediction of damage, communication service.

References:

1. Garnaeva M.A., Makrushin D.N., Ivanov A.M., Namestnikov Yu.V., van der Vil J. Kaspersky Security Bulletin: cifry goda i prognozy-2016, Zashchita informacii. Insajd. 2016. No 1 (67), pp. 47-53.
2. Garnaeva M.A., Funk K. Kaspersky Security Bulletin 2013, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. No 3 (4), pp. 65-68.
3. Drobotun E.B. Teoreticheskie osnovy postroeniya sistem zashchity ot komp›yuternyh atak dlya avtomatizirovannyh sistem upravleniya. SPb.: Izd-vo «Naukoemkie tekhnologii», 2017. 120 p.
4. Eremeev M.A., Allakin V.V., Budko N.P. Model› nastupleniya kriticheskogo sobytiya informacionnoj bezopasnosti v informacionno-kommunikacionnoj sisteme, Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2017. T. 9. No 6, pp. 52-60.
5. Kalashnikov A.O., Bursa M.V., Ostapenko G.A. Mul›tiservisnye seti: diskretnaya risk-model› HTTP-fluda, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. No 1 (9), pp. 49-54.
6. Kosenko M.YU., Mel›nikov A.V. Voprosy obespecheniya zashchity informacionnyh sistem ot botnet atak, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2016. No 4 (17), pp. 20-28.
7. Novikov S.V., Zima V.M., Andrushkevich D.V. Organizaciya zashchity informacii v geterogennyh vychislitel›nyh setyah, Zashchita informacii. Insajd. 2014. No 3 (57), pp. 50-55.
8. Parshutkin A.V. Konceptual›naya model› vzaimodejstviya konfliktuyushchih informacionnyh i telekommunikacionnyh sistem, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. No 5 (8), pp. 2-6.
9. Slesarchik K.F. Metod obnaruzheniya nizkointensivnyh raspredelennyh atak otkaza v obsluzhivanii so sluchajnoj dinamikoj harakteristik fragmentacii i periodichnosti, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2018. No 1 (25). C. 19-27.
10. Starodubcev P.E., Smirnov D.V. Postroenie mnogourovnevoj zashchity korporativnyh informacionnyh sistem s primeneniem obmannyh tekhnologij, Izvestiya Instituta inzhenernoj fiziki. 2017. T. 1. No 43, pp. 68-71.
11. Tarasov Ya.V. Issledovanie primeneniya nejronnyh setej dlya obnaruzheniya nizkointensivnyh DDoS-atak prikladnogo urovnya, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. No 5 (24), pp. 23-29.
12. Begaev A., Chesnakov M., Starodubtsev Yu. Method of Mixed Traffic Model Formation. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 1-5.
13. Starodubtsev Yu.I., Grechishnikov E.V., Komolov D.V. Use of neural networks to ensure stability of communication networks in conditions of external impacts. Telecommunications and Radio Engineering. 2011. V. 70. N 14. P. 1263-1275.
14. Starodubcev YU.I., Begaev A.N., Davlyatova M.A. Upravlenie kachestvom informacionnyh uslug. SPb.: Izd-vo Politekhn. Un-ta, 2017. 454 p.
15. Dobryshin M.M., Didenko P.M. Ocenka zashchishchyonnosti besprovodnyh setej svyazi, II Mezhdunarodnaya nauchno–tekhnicheskaya konferenciya «Radiotekhnika, ehlektronika i svyaz›» – Omsk. – 2013. – P. 155–159.
16. Anisimov V.V., Begaev A.N., Starodubcev Yu.I. Model› funkcionirovaniya seti svyazi s neizvestnym urovnem doveriya i ocenki eyo vozmozhnostej po predostavleniyu uslugi VPN s zadannym kachestvom, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. No 1 (19), pp. 6-15. DOI: 10.21681/2311-3456-2017-1-6-15.
17. Begaev A.N., Starodubcev YU.I., Fyodorov V.G. Metodika ocenki upravlyaemosti fragmenta seti svyazi obshchego pol›zovaniya s uchetom vliyaniya mnozhestvennosti centrov upravleniya i destruktivnyh programmnyh vozdejstvij. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. No 4 (22), pp. 32-39. DOI: 10.21681/2311-3456-2017-4-32-39.
18. Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. Model› uzla dostupa VPN kak ob»ekta setevoj i potokovoj komp›yuternyh razvedok i DDoS-atak, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2016. No 3 (16), pp. 4-12.
19. Grechishnikov E.V. i dr. Ocenka sposobnosti uzla virtual›noj chastnoj seti predostavlyat› uslugi svyazi v usloviyah protivodejstviya i DDoS–atakam, Sbornik trudov nauchno–prakticheskoj konferencii «Problemy tekhnicheskogo obespecheniya vojsk v sovremennyh usloviyah» Voennaya akademiya svyazi im, pp.M. Budennogo, Sankt–Peterburg, – 2016. – S.48–51.
20. Pat. 22405184 RF, MPK G05B 23/00, G06F 17/50 (2006.01) Sposob obespecheniya ustojchivogo funkcionirovaniya sistemy svyazi / Grechishnikov E.V., Dybko L.K., Eryshov V.G., ZHukov A.V., Starodubcev YU.I. – 2009117902/08, zayavl. 12.05.2009; opubl. 27.11.2010. – 17 s.

6. Alexey Begaev, Ph.D., CEO, JSC "NW-Echelon", St. Petersburg, a.begaev@nwechelon.ru
7. Evgenii Grechishnikov, Dr.Sc., Professor, Academy of Federal Guard Service of the Russian Federation, Orel.
8. Mihail Dobryshin, Academy of Federal Guard Service of the Russian Federation, Orel, Dobrithin@ya.ru
9. Pavel Zakalkin, Ph.D., Academy of Federal Guard Service of the Russian Federation, Orel.

21. Pat. 2541205 RF, MPK G05B 23/00, G06F 21/55 (2013.01) Sposob ocenki ehffektivnosti informacionno – tekhnicheskih vozdejstvij na seti svyazi / Grechishnikov E.V., Belov A.S., Dobryshin M.M., Isachenko V.G., Kuzmich A.A. – 2013134627/8, zayavl. 23.07.2013; opubl. 10.02.2015. – 21 s.
22. Ventcel› E.S. Teoriya veroyatnostej i ee inzhenernoe prilozhenie. M.: Nauka, 1988, pp. 463.
23. Pat. 2648508 RF, MPK G05B 23/00 (2006.01), G06F 21/00 (2013.01), G06N 5/00 (2006.01) Sposob ocenki sposobnosti uzla komp›yuternoj seti funkcionirovat› v usloviyah informacionno-tekhnicheskih vozdejstvij / Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V., Gorelik S.P., Belov A.S., Skub›ev A.V. – 2016151502, zayavl. 26.12.2016; opubl. 26.03.2018 – 33 s.
24. Svidetel›stvo o gosudarstvennoj registracii programmy dlya EHVM No 2017616948. Raschet vozmozhnostej uzla komp›yuternoj seti predostavlyat› uslugi svyazi v usloviyah DDoS–atak s uchetom razlichnyh sposobov minimizacii destruktivnogo vozdejstviya / M. M. Dobryshin i dr. – opubl. 26.04.2017.
25. Svidetel›stvo o gosudarstvennoj registracii programmy dlya EHVM No 2018610012. Raschet vremeni nastupleniya otkaza v obsluzhivanii gruppy uslug (uslugi) svyazi v usloviyah DDoS–atak s uchetom vozmozhnosti pererаspredeleniya predostavlyaemyh uslug svyazi. / M. M. Dobryshin R. V. Gutcin, A. N. Reformat. – opubl. 09.01.2018.