УДК 004.72

Оценка эффективности деструктивных программных воздействий на сети связи

Гречишников Е. В., Добрышин М. М.

Постановка проблемы: *увеличение количества деструктивных программных воздействий на сети связи интегрированных в мировое информационное пространство, требует от должностных лиц своевременной оценки уровня защищенности. Имеющиеся научно-технические решения по оценке уровня защищенности сети связи от деструктивных программах воздействий не учитывают ресурсы злоумышленника по вскрытию сети связи и деструктивному воздействию на неё. На основании статистических данных злоумышленник не всегда способен достоверно вскрыть структуру сети связи, а также обладает ограниченными ресурсами воздействия.* ***Методы:*** *моделирование функционирование элементов сети связи средств вскрытия и деструктивного воздействия, имеющихся у злоумышленника.* ***Результаты:*** *использование предложенного способа оценки эффективности деструктивных программных воздействий на сети связи позволяет на основании статистических данных о возможностях злоумышленника, определить уровень защищенности сети связи. На основании уровня защищенности сети связи, должностные лица принимают решение о ее реконфигурации. Сравнительный анализ существующих способов и предлагаемого способа показал, что защищённость элементов сети связи увеличивается от 5 до 9 %. Улучшение защищённости элементов сети связи подверженных внешним деструктивным воздействиям обусловлено повышением достоверности оценки возможностей злоумышленника по вскрытию сети связи и эффективности использования ресурсов воздействий имеющихся у злоумышленника, а так же своевременной реконфигурации сети связи. Кроме того повышение защищённости достигается, за счет маскировки сети под сети связи функционирующие в указанном районе.* ***Практическая значимость:*** *результаты исследований могут быть использованы для защиты сетей связи интегрированных в мировое информационное пространство от внешних деструктивных воздействий. При использовании представленного предложения обеспечивается: требуемая защищённость структурных элементов и сети связи в целом за счёт оценки возможности злоумышленника по вскрытию сети связи, оценки эффективности использования ресурсов воздействий имеющихся у злоумышленника.*

Ключевые слова*: сеть связи, уровень защищённости, вскрытие, воздействие, мониторинг.*

Актуальность

В настоящее время для дезорганизации систем управления различных объектов и организаций, злоумышленниками все чаще используются средства деструктивных программных воздействий (ДПВ) на сети связи. Под информационно-техническими воздействиями понимаются применение способов и средств воздействия на информационно-технические объекты, на технику и т.п. в интересах достижения поставленных целей. Интеграция сетей связи во все сферы деятельности современного общества способствовала появлению различных групп и организаций (например киберсообщество Anonymous), способных своими действиями существенно влиять на эффективность функционирования различных организаций и объектов.

Устойчивое функционирование информационных ресурсов и сетей связи имеет исключительное значение для динамического развития экономики и социальной сферы, а так же для защиты суверенитета государства [1].

Для обеспечения безопасности в информационной сфере в настоящее время разработаны и используются ряд научно-технических решений по защите сетей связи от внешних деструктивных воздействий, однако они имеют ряд системных противоречий [2-6]. В большинстве из этих решений количественный и качественный состав ресурсов злоумышленника по вскрытию и деструктивному воздействию не учитывается или считается, что злоумышленник заведомо обладает возможностью максимально точно вскрыть топологию сети связи и располагает необходимым количеством сил и средств, а свои деструктивные воздействия осуществляет слаженно и организованно. При этом не учитываются или учитываются не в полной мере возможности системы защиты по затруднению вскрытия сети связи и воздействию. Исходя из проведенного анализа [2-8] злоумышленник не всегда способен полностью и достоверно вскрыть структуру сети связи. Кроме того, у злоумышленника могут быть ограничены ресурсы и он не всегда слаженно воздействует на сети связи или не успевает своевременно воздействовать на них. Этим вопросам и посвящена настоящая статья.

Оценка эффективности деструктивных программных воздействий на сети связи

Для решения указанных противоречий разработаны варианты по оценке эффективности деструктивных программных воздействий на сети связи. Разработанные предложения заключаются в том, что на основании анализа данных о значениях параметров развернутых в указанном районе сетей связи и значений параметров злоумышленника по вскрытию сети связи и воздействию на нее создают модель планируемой к развертыванию сети связи. На основе разработанной модели имитируют действия злоумышленника, а так же оценивают эффективность этих действий [9].

Предложения поясняются структурно-логической последовательностью (рис. 1), где (блок 1 на рис. 1) на этапе планирования сети связи измеряют основные технические параметры элементов функционирующих в указанном районе сетей связи ($D_{nip}^{эсс}$). Осуществляют создание базы данных измеренных параметров. Ранжируют измеренные параметры существующих сетей связи. Производят выбор из перечня параметров наиболее значимых, исходя из критерия максимальной информативности демаскирующих признаков для злоумышленника.

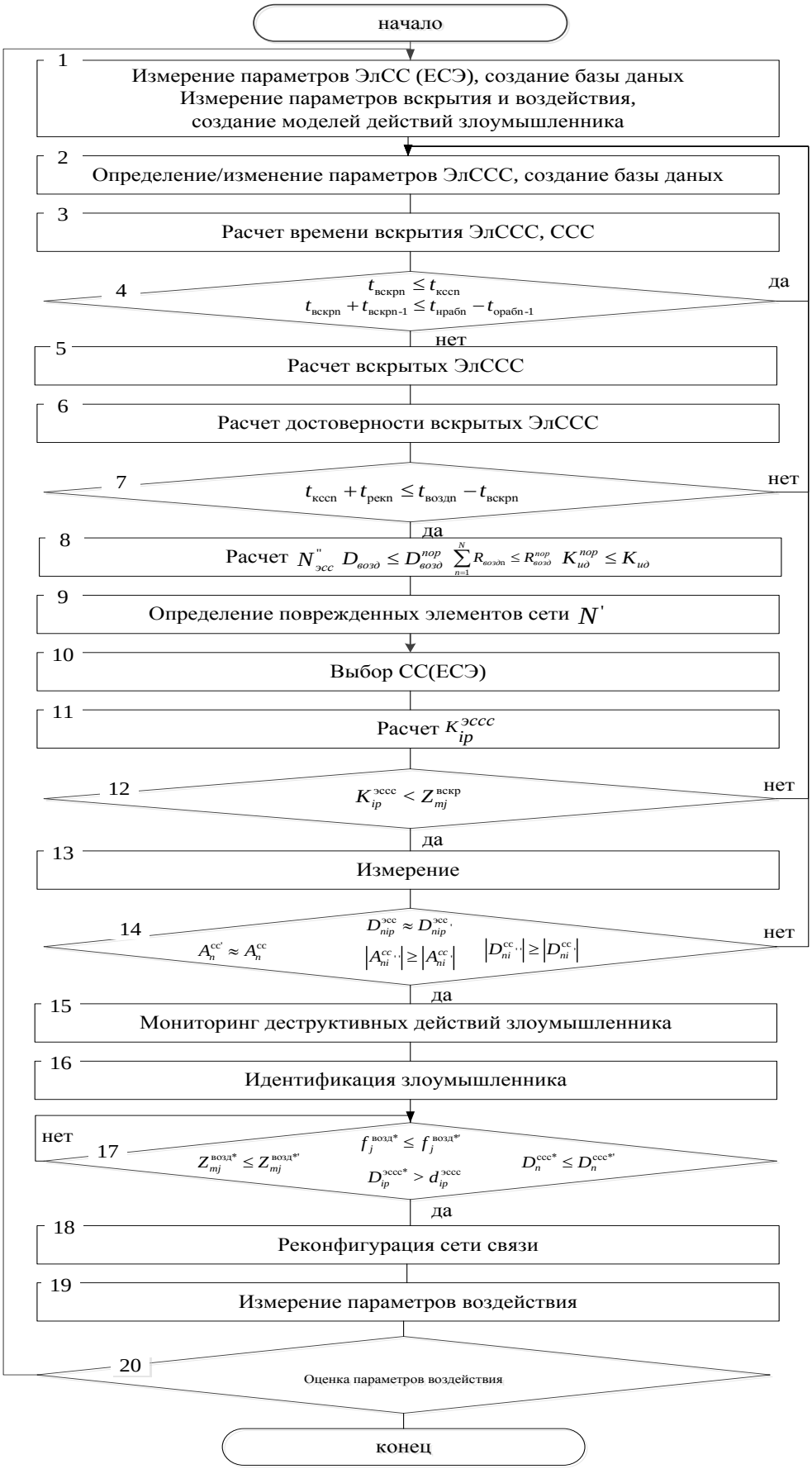

Рис. 1. Структурно-логическая последовательность оценки эффективности деструктивных программных воздействий на сети связи

Измеряют параметры вскрытия сети связи злоумышленником ($Z_{mj}^{\text{вскр}}$) и воздействия ($Z_{mj}^{\text{возд}}$) на сеть связи, где m - значение параметра вскрытия (воздействия) сети связи, а j - идентификационный признак злоумышленника. Идентифицируют оборудование и создают модели действий j-го злоумышленника по вскрытию ($f_j^{\text{вскр}}$) и воздействию ($f_j^{\text{возд}}$) на сеть связи. Создают базу данных измеренных параметров и моделей.

Далее (блок 2 на рис. 1) задают технические параметры, определяющие топологию ($A^{\text{ссс}}$) и технические параметры ($D_p^{\text{эссс}}$) элементов создаваемой сети связи.

На основании измеренных значений (блок 3 на рис. 1) и анализа демаскирующих признаков аппаратуры связи, рассчитывается: время необходимое злоумышленнику для поиска n-го элемента сети связи ($t_{\text{поиск}n}$), время, необходимое злоумышленнику для распознавания элемента сети связи ($t_{\text{распn}}$), время необходимое для вскрытия n-ого элемента сети связи ($t_{\text{вскр}n}$). Так же определяют время реконфигурации сети связи ($t_{\text{рекn}}$) и квазистационарного состояния n-ого элемента сети связи ($t_{\text{кссn}}$). Под временем квазистационарного состояния n-ого элемента сети связи понимается период времени от первого вхождения в связь с абонентом до окончания последнего сеанса связи этого элемента.

Возможности злоумышленника по вскрытию элемента сети связи предлагается оценивать по критерию (блок 4 на рис. 1):

$$t_{\text{вскр}n} \le t_{\text{кссn}}, \quad (1)$$

При не выполнении условия (1) делается вывод о том, что злоумышленник не успевает вскрыть элемент сети связи.

Если условие (1) выполняется, то возможности злоумышленника по вскрытию сети связи в целом оцениваются по следующему критерию:

$$\sum_{n=1}^{N} t_{\text{вскр}n} \le \sum_{n=1}^{N} t_{\text{кссn}}, \quad (2)$$

где $\sum_{n=1}^{N} t_{\text{вскр}n}$ – время вскрытия сети связи, $\sum_{n=1}^{N} t_{\text{кссn}}$ – время квазистационарного состояния сети связи, N – количество элементов сети связи.

При не выполнении условия (2) делается вывод о том, что злоумышленник не успевает вскрыть сеть связи.

При выполнении указанных условий (1, 2) считают элемент сети связи вскрытым, если одно из условий не выполняется (1, 2) элемент не вскрыт.

Возможности злоумышленника по вскрытию элементов сети связи и сети связи в целом (рис. 2) оцениваются по следующим критериям:

$$t_{\text{вскр}n} \le t_{\text{кссn}}, \quad (3)$$

$$t_{\text{вскр}n} + t_{\text{вскр}n\text{-}1} \le t_{\text{нрабn}} - t_{\text{орабn-1}}, \quad (4)$$

где $t_{вскрn-1}$ – время вскрытия $(n-1)$-ого элемента сети связи, $t_{нрабn}$ – время начала функционирования n- ого элемента сети связи, $t_{орабn-1}$ – время окончания функционирования $(n-1)$ -ого элемента сети связи.

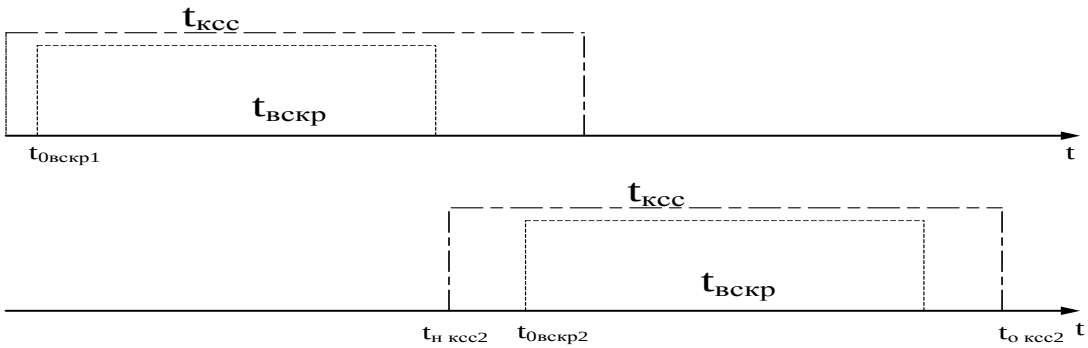

Рис. 2. Соотношения времени вскрытия элементов сети связи и их квазистационарного состояния

При не выполнении условий (3, 4) делается вывод о том, что злоумышленник не имеет средств для вскрытия сети связи.

В блоке 5 рис. 1 рассчитывают значения весовых коэффициентов вскрытых элементов сети ($R_{вскрn}$), а так же определяют число вскрытых элементов сети связи ($N_{эсс}^{'вскр}$). Далее осуществляется расчёт достоверности вскрытия сети связи.

$$D_{вск} = \frac{N_{эсс}^{'вскр}}{N_{эсс}}, \quad (5)$$

где $D_{вск}$ – достоверность вскрытия сети связи.

В блоке 6 рис. 1 осуществляется оценка достоверности вскрытия сети связи согласно критериям:

$$D_{вск} \le D_{вскр}^{пор}, \quad (6)$$

где $D_{вскр}^{пор}$ – пороговая достоверность вскрытия сети связи.

$$\sum_{n=1}^{N} R_{вскрn} \le R_{вскр}^{пор}. \quad (7)$$

где $\sum_{n=1}^{N} R_{вскрn}$ – сумма весовых коэффициентов вскрытых элементов сети связи;

Если достоверность вскрытия сети связи ($D_{вск}$) или сумма весовых коэффициентов вскрытых элементов сети ($\sum_{n=1}^{N} R_{вскрn}$) не соответствуют критериям (6, 7), то производят реконфигурацию сети связи.

Если условия (6, 7) выполнены в блоке 6 производят расчёт времени, требуемого злоумышленнику для принятия решения о воздействии на n-ый элемент сети связи ($t_{воздn}$).

В блоке 7 рис. 1 осуществляется оценка возможностей злоумышленника по воздействию на элементы сети связи по формуле:

$$t_{\text{кссп}} + t_{\text{рекп}} \le t_{\text{воздп}} - t_{\text{вскрп}}\ , \qquad (8)$$

где $t_{\text{ðåên}}$ – время реконфигурации сети связи; $t_{\text{âîçä}\,n}$ – время, необходимое средствам воздействия злоумышленника для воздействий на элемент сети связи (рис 3).

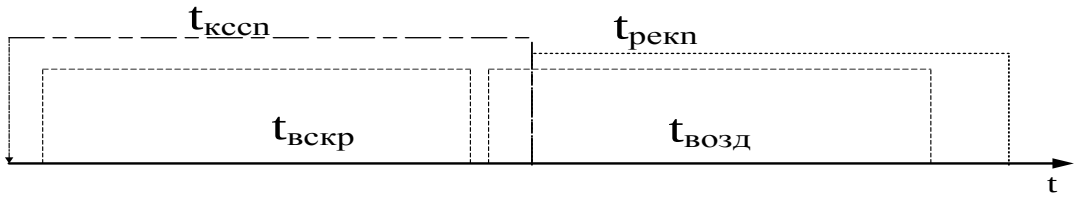

Рис. 3. Соотношение времен функционирования элемента сети связи, вскрытия и воздействия на него злоумышленником

В блоке 8 рис. 1 осуществляется расчёт количества элементов сети связи подвергшихся воздействию ($N''_{эсс}$) и достоверности воздействия злоумышленником на сеть связи.

Оценка достоверности воздействия на сеть связи злоумышленником осуществляется согласно формулам:

$$D_{\text{возд}} \le D^{\text{пор}}_{\text{возд}}, \qquad (9)$$

где $D^{пор}_{возд}$ – пороговая достоверность воздействия на сеть связи.

$$\sum_{n=1}^{N} R_{\text{воздп}} \le R^{\text{пор}}_{\text{возд}}. \qquad (10)$$

где $\sum_{n=1}^{N} R_{\text{воздп}}$ – сумма весовых коэффициентов элементов сети связи подвергшихся воздействию, $R^{\text{пор}}_{\text{возд}}$ – сумма пороговых значений весовых коэффициентов подвергшихся воздействию элементов сети связи.

Расчёт и сравнение коэффициента исправного действия сети связи с пороговым значением осуществляется согласно неравенства:

$$K^{\text{пор}}_{\text{ид}} \le K_{\text{ид}}, \qquad (11)$$

Если достоверность воздействия на сети связи ($D_{\text{возд}}$) или сумма весовых коэффициентов подвергшихся воздействию элементов сети связи ($\sum_{n=1}^{N} R_{\text{воздп}}$) или коэффициент исправного действия ($K_{\text{ид}}$) не отвечают условиям (9-11), то производится реконфигурация модели сети связи.

При выполнении указанных условий (9-11) логическому коэффициенту ($i_n^{\text{повр}}$) присваивается 1, если условие не выполнено присваивается 0.

В блоке 9 рис. 1 определяют сети связи (N') на которые осуществлялась наименьшее количество деструктивных воздействий.

На основании анализа технических параметров ($A_n^{cc}, D_{nip}^{эсс}$) выбранных функционирующих сетей связи (N') (блок 10 рис. 1) выбирают сети связи, удовлетворяющие требованиям, предъявляемым к техническим параметрам ($A^{ссс}, D_{ip}^{эссс}$) создаваемой сети связи.

Коэффициенты контраста (блок 11 рис. 1), технических параметров элементов создаваемой сети связи($K_{ip}^{эссс}$) рассчитывают по следующей формуле:

$$K_{ip}^{эссс} = \frac{D_{ip}^{эссс} - D_{nip}^{эсс}}{D_{ip}^{эссс}}, \quad (12)$$

где $K_{ip}^{эссс}$ – коэффициент контраста технического параметра элемента создаваемой сети связи, $D_{ip}^{эссс}$ – значение технических параметров элементов создаваемой сети связи, $D_{nip}^{эсс}$ – значение технических параметров элементов сетей связи наиболее точно удовлетворяющей техническим требованиям, i – номер элемента сети связи, p – параметр элемента функционирующей сети связи.

Далее (блок 12 рис. 1) сравнивают коэффициенты контраста технических параметров элементов создаваемой сети связи ($K_{ip}^{эссс}$) со значениями и технических параметров средств вскрытия сети связи ($Z_{mj}^{вскр}$):

$$K_{ip}^{эссс} < Z_{mj}^{вскр}, \quad (13)$$

Если условие (13) не выполняется, то принимается решение о подстройке технических параметров ($D_{ip}^{эссс}$) элементов сети связи.

На основании мониторинга технических параметров функционирующих сети связи ($A_n^{cc}{}', D_{nip}^{эсс}{}'$) (блок 13 рис. 1), осуществляется поиск впервые введенных в эксплуатацию сетей связи, а так же оцениваются параметры других функционирующих сетей связи ($A_n^{cc}{}', D_{nip}^{ýcñ}{}''$). Измеренные параметры ($A_n^{cc}, D_{nip}^{эсс}$) оцениваются согласно следующих соотношений:

$$A_n^{cc'} \approx A_n^{cc}, \quad (14)$$

$$D_{nip}^{эсс} \approx D_{nip}^{эсс}{}', \quad (15)$$

$$\left|A_{ni}^{cc}{}''\right| \geq \left|A_{ni}^{cc}{}'\right|, \quad (16)$$

$$\left|D_{ni}^{cc}{}''\right| \geq \left|D_{ni}^{cc}{}'\right|, \quad (17)$$

Если одно из соотношений (14-17) не выполняется, то (блок 14 рис. 1) принимается решение о перестройке p-х параметров созданной сети.

Во время функционирования сети связи (блок 15 рис. 1) осуществляют мониторинг признаков и действий злоумышленника по воздействию на созданную сеть связи. На основании выбранных критериев осуществляют фиксацию факта начала деструктивного воздействия на созданную сеть связи [9].

На основании статистических данных индивидуальных особенностей принимают решение о идентификации принадлежности аппаратуры определённому злоумышленнику (блок 16 рис. 1).

На основании имеющихся моделей действий злоумышленника по информационно-техническим воздействиям, (блок 17 рис. 1) осуществляют сравнение прогнозируемых параметров воздействия ($Z_n^{\text{возд}*'}$, $f_j^{\text{возд}*'}$, $D_n^{\text{cccc}*}$), с фактическим значениями ($Z_n^{\text{возд}*'}$, $f_j^{\text{возд}*'}$, $D_n^{\text{cccc}*}$), а так же осуществляют сравнение фактических параметров созданной сети связи подверженной воздействию ($D_n^{\text{сñи}*}$) и минимальных параметров сетей связи подвергшихся деструктивному воздействию, при которых созданная сеть связи будет выполнять функциональные задачи ($d_n^{\text{ссс}}$). Сравнение осуществляется согласно следующих неравенств:

$$Z_{mj}^{\text{возд}*} \le Z_{mj}^{\text{возд}*'}, \quad (18)$$

$$f_j^{\text{возд}*} \le f_j^{\text{возд}*'}, \quad (19)$$

$$D_n^{\text{ссс}*} \le D_n^{\text{cccc}*}, \quad (20)$$

$$D_{ip}^{\text{эссс}*} > d_{ip}^{\text{эссс}}. \quad (21)$$

Если одно из неравенств (18-21) не выполняется, то принимают решение о реконфигурации сети связи.

В блоке 18 рис. 1 измеряют параметры воздействия на созданную сеть связи и на основании выбранных критериев принимают решение об окончании деструктивного воздействия [9].

В блоке 19 рис. 1 оценивают результаты воздействия на сеть связи. Оценка наличия у злоумышленника средств воздействия осуществляется согласно неравенства:

$$N_{\text{возд}}^{'} > N_{\text{эсс}}^{''}, \quad (22)$$

где $N_{\text{возд}}^{'}$ – фактическое количество средств воздействия на сеть связи имеющиеся у злоумышленника; $N_{\text{эсс}}^{''}$ – предполагаемое количество повреждённых элементов сети связи.

На основании неравенства (22) осуществляется вывод о наличии средств воздействия ($N_{\text{возд}}$) у злоумышленника.

Оценка возможностей злоумышленника по вскрытию элементов сети связи осуществляется согласно неравенства:

$$N_{\text{возд}}^{'} \le N_{\text{возд}}, \quad (23)$$

где $N_{\text{возд}}$ – предполагаемое количество средств воздействия.

$$N_{\text{эсс}}^{''} < z_{mj}^{\text{вскр}}, \quad (24)$$

где $N_{\text{эсс}}^{''}$ – фактическое количество повреждённых элементов сети связи.

На основании неравенств (23, 24) делается вывод о способности злоумышленника своевременно вскрыть ($t_{вскрп}$) сеть связи.

Если значения параметров деструктивного воздействия на созданную сеть связи не соответствуют имеющимся в базе данных, или параметры сети связи подвергшейся воздействию не соответствуют заданным значениям, то (блок 20

рис. 1) на основе имеющихся параметров деструктивного воздействия осуществляют оценку возможностей злоумышленника по вскрытию созданной сети связи и деструктивному воздействию на неё. Определяют количество средств вскрытия и средств деструктивного воздействия имеющихся у злоумышленника.

На основании произведённой оценки осуществляется дополнение статистических данных о возможностях вскрытия сети связи и воздействия на сеть связи злоумышленником.

Выводы

Сравнительный анализ значений показателей защищённости некоторых существующих способов защиты сетей связи от внешних деструктивных воздействий [9, 10] и предлагаемого способа показал, что защищённость элементов сети связи увеличивается от 5 до 9 % [11]. Расчёт производился в GPSS World.

Улучшение защищённости элементов сети связи подверженных внешним деструктивным воздействиям обусловлена повышением оценки достоверности вскрытия злоумышленником топологии сети связи, оценки эффективности использования ресурсов воздействий имеющихся у злоумышленника, а так же своевременной реконфигурации сети связи исходя из анализа возможностей злоумышленника. Кроме того, повышение защищённости достигается за счет маскировки сети под сети связи, функционирующие в указанном районе. Проведение мониторинга признаков или действий злоумышленника по вскрытию сети связи и воздействию на нее повышает оперативность принятия решения на реконфигурацию сети связи в рамках обеспечения ее защищенности.

Предлагаемое техническое решение может быть использовано при проектировании мультисервисных сетей для обеспечения требуемой защищённости технических разведок и внешних информационно-технических воздействий.

Предлагаемый способ подтвержден патентом на изобретение.

Литература

1. Путин В. В. Заседание Совета Безопасности, посвящённое вопросам противодействия угрозам национальной безопасности в информационной сфере 2014. URL: http://kremlin.ru/news (дата обращения 01.10.2014).

2. Гречишников Е. В., Белов А. С. Способ обеспечения устойчивости сетей связи в условиях внешних деструктивных воздействий // Патент на изобретение № 2379753, 20.01.2010.

3. Гречишников Е. В., Белов А. С. Способ обеспечения устойчивого функционирования системы связи // Патент на изобретение № 240518427.11.2010.

4. Гречишников Е. В., Белов А. С. Способ (варианты) защиты системы связи от внешних деструктивных воздействий // Патент на изобретение № 2451416, 20.05.2012.

5. Макаренко С. И., Михайлов Р. Л. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69-79.

6. Макаренко С. И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2-2. URL: http://jre.cplire.ru/jre/sep11/4/text.pdf

7. Гречишников Е. В., Добрышин М. М. Способ обеспечения защищённости сетей связи от технической компьютерной разведки. // Сборник Проблемы теории и практики развития войск ПВО СВ в современных условиях. Смоленск: ВА ВПВО ВС РФ. 2013. С. 43–46.

8. Гречишников Е. В., Горелик С. П., Белов А. С. Способ управления защищенностью сетей связи в условиях деструктивных программных воздействий // Телекоммуникации. 2014. № 3. С. 18-22.

9. Гудов Н. В. Система и способ уменьшения ложных срабатываний при определении сетевой атаки // Патент на изобретение № 2480937, 27.04.2013.

10. Добрышин М. М., Диденко П. М. Оценка защищённости беспроводных сетей связи // Радиотехника, электроника и связь. II Международная научно-техническая конференция. Омск: 2013. С. 155-159.

11. Гречишников Е. В., Горелик С. П. Способ (варианты) мониторинга и обеспечения требуемого качества обслуживания абонентов в мультисервисных сетях // Патент на изобретение № 2517327, 28.03.2014.

12. Гречишников Е. В., Добрышин М. М., Белов А. С., Кузьмич А. А. Способ оценки эффективности информационно-технических воздействий на сети связи // Патент на изобретение № 2541205, 24.12.2014.

References

1. Putin V. V. Zasedaniye Soveta Bezopasnosti, posvyashchonnoye voprosam protivodeystviya ugrozam natsional'noy bezopasnosti v informatsionnoy sfere 2014 [Meeting of the Security Council on questions of counteraction to threats to national security in the information sphere 2014] Available at: http:/kremlin.ru/news (accessed 01.10.2014) (in Russia).

2. Grecihnikov E. V., Belov A. S. *Sposob obespecheniya ustoychivosti setey svyazi v usloviyakh vneshnikh destruktivnykh vozdeystviy* [Method to ensure the stability of networks under external destructive influences]. Patent Russia, no. 2379753, 2010 (in Russia).

3. Grecihnikov E. V., Belov A. S. *Sposob obespecheniya ustoychivogo funktsionirovaniya sistemy svyazi* [Method to ensure sustainable operation of the communication system]. Patent Russia, no. 2405184, 2010 (in Russia).

4. Grecihnikov E. V., Belov A. S. *Sposob (varianty) zashchity sistemy svyazi ot vneshnikh destruktivnykh vozdeystviy* [Method (versions) protect communication systems from external destructive influences]. Patent Russia, no. 2451416, 2012 (in Russia).

5. Mikhailov R. L., Makarenko S. I. Estimating Communication Network Stability under the Conditions of Destabilizing Factors Affecting it. *Radio and telecommunication systems*, 2013, no. 4, pp. 69–79 (in Russian).

6. Makarenko S. I. *Podavlenie paketnux radiosetey so slyhainum mnogestvennum dostypom za shet destabilizacii ix sostoijnij* [The countermeasures of the radio networks with the random multiple access by changing the radionet state to non-stable]. *Radio electronics journal*, 2011, no. 9. Available at: http://jre.cplire.ru/jre/sep11/4/text.pdf (in Russian).

7. Grecihnikov E. V., Dobrithin M. M. *Podavleniye paketnykh radiosetey so sluchaynym mnozhestvennym dostupom za schet destabilizatsii ikh sostoyaniya* [Method of facilitating secure communication networks from technical computer intelligence. Collection of problems of the theory and practice of development of air defense troops of PVO SV in modern conditions]. Smolensk, Military Academy of army air defence of the Armed Forces of the Russian Federation Pabl., 2013, pp. 43–46 (in Russia).

8. Grecihnikov E. V., Gorelik S. P., Belov A. S. *Sposob upravleniya zashchishchennost'yu setey svyazi v usloviyakh destruktivnykh programmnykh vozdeystviy* [A method of controlling the security of communication networks in terms of destructive program influences]. *Telecommunications*, 2014, no. 3, pp. 18-22 (in Russia).

9. Goodov N. V. *Sistema i sposob umen'sheniya lozhnykh srabatyvaniy pri opredelenii setevoy ataki* [System and a method of reducing false positives when identifying network attacks]. Patent Russia, no. 2480937, 2013 (in Russia).

10. Dobrushin M. M., Didenko P. M. Otsenka zashchishchonnosti besprovodnykh setey svyazi [Evaluate the security of wireless networks communication]. *Radio engineering, electronics and communication. II international scientific and technical conference*, Omsk, 2013, pp. 155-159 (in Russia).

11. Grecihnikov E. V., Gorelik S. P. *Sposob (varianty) monitoringa i obespecheniya trebuyemogo kachestva obsluzhivaniya abonentov v mul'tiservisnykh setyakh* [Method monitor and ensure the required quality of customer service in multiservice networks]. Patent Russia, no. 2517327, 2014 (in Russia).

12. Grecihnikov E. V., Dobrithin M. M. *Sposob otsenki effektivnosti informatsionno-tekhnicheskikh vozdeystviy na seti svyazi* [Method of evaluating the effectiveness of ICT impacts on the communication network]. Patent Russia, no. 2541205, 2014 (in Russia).

Статья поступила 19 июня 2015 г.

Информация об авторах

Гречишников Евгений Владимирович – доктор технических наук, доцент. Сотрудник Академии ФСО России. Область научных интересов: информационное противоборство.

Добрышин Михаил Михайлович – соискатель ученой степени кандидата технических наук. Сотрудник Академии ФСО России. Область научных интересов: мониторинг защищенности элементов сети связи от информационно-технических воздействий. E–mail: dobrithin@ya.ru

Адрес: 302028, Россия, г. Орел, Приборостроительная 35а.

Performance Evaluation of Destructive Effects Software in the Communications Network

Grecihnikov E. V., Dobrushin M. M.

***Purpose**: increasing the number of destructive software effects on network integrated into the global information space, requires officials timely assessment of the level of security. Existing scientific and technical solutions to assess the security level of the communications network of the destructive impact of the programs do not take into account the resources of the attacker by autopsy a communication network and destructive impact on her. Based on statistics the attacker is not always able to reliably reveal the structure of the network, as well as has the impact of limited resources. **Methods**: A simulation of the elements of the communication network means autopsy and destructive impacts available to the attacker. **Results**: The use of the proposed method of assessing the effectiveness of the destructive impacts of the program on the network allows on the basis of statistical data on the possibilities of an attacker to determine the level of security of the communication network. Based on the level of security of communication networks, officials decide on its reconfiguration. Comparative analysis of existing methods and the proposed method shows that The security elements of the communication network is increased from 5 to 9%. Improving the security of network elements susceptible to external disruptive impact due to increased reliability of the assessment as deterrents for autopsy network and effective use of resources available to the attacker's actions, as well as timely communication network reconfiguration. Further increase of security is achieved by masking the network under the network autopsy in that area. **Practical significance**: The results can be used to protect the networks integrated into the global information space from external destructive impact. By using of the proposal is provided by: The security required structural elements and networks in general due to assess the possibility of an attacker by autopsy a communication network, evaluate the effectiveness of the use of resources available to the attacker's actions.*

Keywords: communications network, level of security, autopsy, impact.

Information about Authors

Grecihnikov Evgeny Vladimirovich - Dr. habil. of Engineering Sciences, Associate Professor. The Academy of Federal Security Guard Service of the Russian Federation. Research interests: information warfare.

Dobrushin Mikhail Mikhailovich - Doctoral Student. The Academy of Federal Security Guard Service of the Russian Federation. Research interests: monitoring security elements of the communication network from the information technology influences. E-mail: dobrithin@ya.ru

Address: Russia, 302028, Orel, Priborostroitelnay 35A.