МОДЕЛЬ УЗЛА ДОСТУПА VPN КАК ОБЪЕКТА СЕТЕВОЙ И ПОТОКОВОЙ КОМПЬЮТЕРНЫХ РАЗВЕДОК И DDOS-АТАК

Гречишников Е.В.[1], Добрышин М.М.[2], Закалкин П.В.[3]

Увеличение количества сетевых атак и мощности деструктивных воздействий на виртуальные частные сети требует от должностных лиц своевременной оценки степени нанесенного ущерба и принятия мер по ее минимизации. Имеющиеся научно–технические решения по оценке ущерба сетевыми атаками не в полной мере учитывают ресурсы злоумышленника по вскрытию сети связи и деструктивному воздействию на нее. Злоумышленник не всегда способен достоверно вскрыть структуру сети связи, так как обладает ограниченными ресурсами воздействия. При оценке возможностей противника по вскрытию сети не учитываются или учитываются не в полной мере способы снижения контрастности признаков сети связи в признаковом пространстве Единой сети электросвязи РФ. Использование предложенной модели позволяет на основании вероятностного подхода предсказать и оценить ущерб, нанесенный DDoS–атаками узлам доступа виртуальной частной сет, определить его способность выполнять свои задачи по предназначению в условиях ведения DDoS–атак. В работе используются статистические данные о возможностях злоумышленника по ведению компьютерной разведки и DDoS–атак. На основании оценки ущерба должностные лица принимают решение о реконфигурации сети связи. С помощью разработанной модели могут решаться следующие задачи: оценки защищенности структурных элементов и сети связи за счет оценки возможности злоумышленника по вскрытию и воздействию на сеть связи, оценки эффективности использования ресурсов, имеющихся у злоумышленника, планирования сетей связи в условиях ведения сетевой и потоковой разведок и деструктивных воздействий.

***Ключевые слова**: виртуальная частная сеть, мониторинг, защищенность сети связи, вероятность вскрытия, контрастность, вероятность подавления.*

Введение

Развитие информационных технологий является одним из важнейших факторов, способствующих решению ключевых задач государственной политики Российской Федерации [1].

В целях достижения взаимных интересов различных государств в процессе интернационализации глобального информационного пространства Российской Федерацией широко используются зарубежные информационные и коммуникационные технологии, в том числе технологии виртуальных частных сетей (Virtual Private Network – VPN).

Применение технологии VPN для организации процесса обмена данными между территориально разнесенными подразделениями компаний на некоторое время позволило минимизировать угрозы, вызванные ведением злоумышленниками компьютерной разведки и информационно-технических воздействий. Однако они разработали средства ведения компьютерной разведки, способные вскрывать виртуальную сеть связи и совершенствовали методы информационно-технических воздействий на эти сети. Эффективными способами ведения компьютерной разведки являются сетевая и потоковая компьютерные разведки (СиП КР) [2].

Учитывая тот факт, что передаваемая в VPN информация надежно защищена с криптографической точки зрения, а взаимодействие осуществляется только с «доверенными» абонентами, наиболее эффективными являются воздействия, направленные на срыв процесса передачи данных [2–4]. В настоящее время злоумышленник активно использует ряд атак, которые приводят к срыву передачи данных. Наиболее эффективными из них являются DDoS-атаки [4,5]. Таким образом, в отношении VPN наиболее вероятно ведение СиП КР и DDoS-атак.

Для обеспечения требуемой защищенности узлов доступа VPN, интегрированных в ЕСЭ РФ, от СиП КР и DDoS-атак разработана модель узла коммутации VPN как объекта сетевой и потоковой компьютерных разведок и сетевых компьютерных атак типа «распределенный отказ в обслуживании».

1 Гречишников Евгений Владимирович, доктор технических наук, доцент, Академия ФСО России, г. Орёл
2 Добрышин Михаил Михайлович, Академия ФСО России, г. Орёл, dobrithin@ya.ru
3 Закалкин Павел Владимирович, кандидат технических наук, Академия ФСО России, г. Орёл

Исходя из основных задач, сформирована последовательность действий элементов СиП КР по обнаружению и вскрытию элементов VPN, а также DDoS-атак по частичному затруднению или полному блокированию доступа к ресурсам информационной системы, содержащая поиск и обнаружение демаскирующих признаков (ДМП) элементов VPN; наблюдение ДМП элементов VPN в заданное время, необходимое для фиксации ДМП; фиксация необходимого числа ДМП элементов VPN, достаточного для распознавания и идентификации элемента VPN; вскрытие числа элементов VPN, необходимого для того, чтобы сделать вывод о вскрытии VPN в целом; формирование «электронного» или другого «портрета объекта»; воздействие атакующей компьютерной сети с целью создания условий, препятствующих доступу к ресурсам информационной системы (может быть осуществлено по времени доступа, функциям по обработке информации, видам доступа и (или) доступным информационным ресурсам); восстановление работоспособности элемента VPN по окончании DDoS-атаки.

С учетом выявленных особенностей функционирования СиП КР, DDoS-атак и элементов VPN разработана комплексная аналитико-имитационная модель. Задача моделирования заключается в разработке научно-методического обеспечения по оценке защищенности элементов VPN от СиП КР и DDoS-атак.

Постановка задачи на исследование

Целью моделирования является получение функциональных зависимостей времени вскрытия элемента VPN от контрастности его параметров в признаковом пространстве, времени DDoS-атаки на элемент VPN от параметров атакующей распределенной бот-сети, времени подавления элемента VPN от значений параметров DDoS-атаки, а также зависимостей группы показателей функционирования элемента VPN от групп показателей ведения СиК КР и параметров подавления с использованием DDoS-атак.

Промежуточными выходными результатами являются зависимости коэффициентов контраста элемента VPN от параметров элементов VPN и элементов ЕСЭ РФ в указанном сегменте ($K_{\text{Эл}VPN} = f(R_{\text{Эл}VPN}; R_{\text{ЭлЕСЭ}})$); вероятности вскрытия элемента VPN средствами СиП КР ($P_{\text{вскр.}ij} = f(t_{\text{кcc}})$) и вероятности подавления элемента VPN DDoS-атакой ($P_{\text{подавл.}ij} = f(t_{\text{кcc}})$) от времени квазистационарного состояния элемента VPN.

Основными исходными данными модели являются время квазистационарного состояния элемента VPN ($t_{\text{кcc}}$); среднее время вскрытия j-м злоумышленником элемента VPN ($\overline{T}_{\text{вскр.}j}$); среднее время атаки (подавления) j-м злоумышленником элемента VPN ($\overline{T}_{\text{атак}j}$); среднее количество средств вскрытия, имеющихся у j-го злоумышленника_($\overline{N}_{\text{вскр.}j}$); количество сторонних однотипных узлов связи ЕСЭ, функционирующих в указанном сегменте ЕСЭ РФ ($N_{\text{ЕСЭ}\ k}$); количество однотипных элементов VPN, функционирующих в указанном сегменте ЕСЭ РФ ($N_{\text{э}VPN}$); значение x-го параметра, e-го однотипного узла связи ЕСЭ, функционирующего в указанном сегменте ЕСЭ РФ ($R_{\text{ЕСЭ}\ ex}$); значение i-го параметра элемента VPN, функционирующего в указанном сегменте ЕСЭ РФ ($R_{\text{э}VPN}$); значение сетевого ресурса, используемого абонентами k-й категории, элемента VPN ($R_{\text{аб.}k}$); количество абонентов k-й категории, элемента VPN ($N_{\text{абонент}\ k}$); значение сетевого ресурса, предоставляемого элементу VPN доверенным оператором связи РФ ($R_{\text{э}VPN\ z}$); средняя максимальная мощность атаки, проводимой j-м злоумышленником на элемент VPN ($\overline{R}_{\text{атак}\ j}$); быстродействие s-й бот-сети, используемой j-м злоумышленником ($R_{\text{бот-сеть}\ sj}$); быстродействие системы противодействия атакам элемента VPN ($R_{\text{СЗ}}$).

Основными допущениями считают следующие: элемент VPN получает сетевой ресурс у доверенного оператора связи РФ; доверенный оператор связи РФ обеспечивает требуемые значения параметров качества сетевых соединений; в районе развертывания и функционирования элемента VPN функционируют другие элементы ЕСЭ РФ.

Основные ограничения: ограниченный временной ресурс действий СиП КР и DDoS-атаки; ресурс сил и средств СиП КР и DDoS-атаки ограничен; время квазистационарного состояния (КСС) элемента VPN больше времени вскрытия этого элемента злоумышленником; рассматриваются ДМП, характеризующие параметры элемента VPN на сетевом уровне; время, необходимое для вскрытия элемента VPN силами и средствами видовой разведки, значительной превышает время вскрытия элемента VPN СиП КР; среднее время и средняя мощность проведения DDoS-атак соизмеримы со среднестатистическими значениями.

Модель включает в себя два этапа: вскрытие средствами СиП КР злоумышленника элементов VPN и подавление DDoS-атакой вскрытых элементов VPN.

В ходе предоставления абонентам услуг специальной связи происходит проявление групповых

и индивидуальных ДМП элементов VPN. Учитывая интеграцию ЕСЭ РФ в мировое информационное пространство, ДМП элементов VPN становятся доступны СиП КР, а элементы VPN становятся вероятными объектами DDoS-атак. Исходя из этого схема алгоритма модели элемента VPN как объекта СиП КР и DDoS-атак состоит из двух частей: первая часть заключается в оценке способности злоумышленника вскрыть элемент VPN и VPN в целом; вторая часть алгоритма состоит в моделировании DDoS-атак на элемент VPN и VPN в целом.

Модель элемента VPN как объекта сетевой и потоковой компьютерных разведок

Первая часть моделирующего алгоритма VPN как объекта СиП КР представлена на рисунке 1 и заключается в следующей последовательности действий.

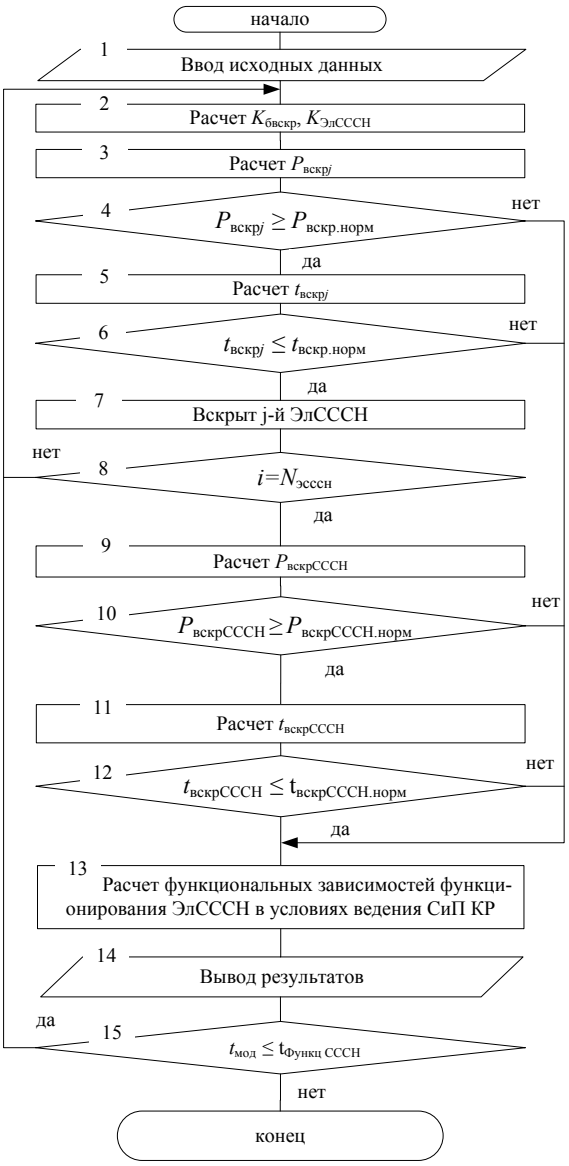

***Рис. 1**. Схема моделирующего алгоритма VPN как объекта СиП КР*

В блоке 1 осуществляют ввод исходных данных, в котором задают количество средств вскрытия, имеющихся у злоумышленника ($N_{\text{вскр. }j}$); количество элементов VPN ($N_{\text{эсссн}}$); количество элементов ЕСЭ РФ, функционирующих в рассматриваемом сегменте ЕСЭ ($N_{\text{ЕСЭ}}$); значение параметров однотипного элемента ЕСЭ, функционирующего в рассматриваемом сегменте ЕСЭ ($R_{\text{ЕСЭ }ex}$); значение параметров элемента VPN, функционирующего в указанном районе ($R_{\text{эсссн }i}$); время квазистационарного состояния элемента VPN ($t_{\text{ксс}}$); среднее время вскрытия злоумышленником элемента VPN средствами СиП КР ($\overline{T}_{\text{вскр. }j}$).

В блоке 2 осуществляют расчет коэффициента вскрытия *j*-м злоумышленником элемента VPN, коэффициента контраста *i*-й характеристики элемента VPN и коэффициента контраста элемента VPN согласно формулам (1–3):

Коэффициент быстродействия системы вскрытия злоумышленника рассчитывается по формуле

$$K_1 = \frac{N_{\text{вскр. }j}}{N_{\text{ЕСЭ}} + N_{\text{эсссн}}}, \quad (1)$$

где $N_{\text{вскр. }j}$ – количество средств вскрытия, имеющихся у *j*-го злоумышленника; $N_{\text{ЕСЭ}}$ – количество сторонних однотипных узлов связи ЕСЭ, функционирующих в указанном районе; $N_{\text{эсссн}}$ – количество однотипных элементов VPN, функционирующих в указанном районе.

Коэффициент контраста (K_2) элемента VPN рассчитывается по формуле

$$K_2 = K_{2i} \cdot k_i, \quad (2)$$

где K_{2i} – коэффициент контраста *i*-й характеристики элемента VPN; k_i – весовой коэффициент *i*-й характеристики элемента VPN, определяется на основании экспертной оценки.

Коэффициент контраста *i*-й характеристики элемента VPN рассчитывается по формуле

$$K_{2i} = \left| \frac{R_{\text{ЕСЭ }ik} - R_{\text{эсссн }i}}{R_{\text{ЕСЭ}ik}} \right|, \quad (3)$$

где $R_{\text{ЕСЭ }ik}$ – значение *k*-го однотипного узла связи ЕСЭ, функционирующего в указанном районе; $R_{\text{эсссн }i}$ – значение *i*-й характеристики элемента VPN, функционирующего в указанном районе.

В блоке 3 осуществляют расчет вероятности вскрытия элемента VPN ($P_{\text{вскр }j}(t_{\text{ксс}})$) [5]:

$$P_{\text{вскр. }ji}(t_{\text{ксс}}) = 1 - e^{-\frac{t_{\text{ксс}} \cdot K_1 \cdot K_2}{\overline{T}_{\text{вскр. }j}}}, \quad (4)$$

где $t_{\text{ксс}}$ – время квазистационарного состояния элемента VPN; K_1 – коэффициент вскрытия *j*-м

злоумышленником элемента VPN; K_2 – коэффициент контраста z-го элемента VPN; $\overline{T}_{\text{вскр. }j}$ – среднее время вскрытия элемента VPN средствами СиП

В блоке 4 сравнивают значения вероятности вскрытия элемента VPN с нормированным значением и принимают решение о его вскрытии. Если элемент сети связи не вскрыт, полученное значение вероятности вскрытия элемента VPN сохраняют в базе данных для последующего вывода результатов расчета.

В блоке 5 рассчитывают фактическое время вскрытия элемента VPN ($t_{\text{вскр. }j}$) по формуле

$$t_{\text{вскр}|P_{\text{вскр}}} = \frac{-t_{\text{кcc}} \cdot K_1 \cdot K_2}{\ln(1-P_{\text{вскр}})}. \quad (5)$$

В блоке 6 сравнивают значения времени вскрытия элемента VPN с нормированным значением и принимают решение о его вскрытии. Если элемент сети связи не вскрыт, полученное значение времени вскрытия элемента VPN сохраняют в базе данных для последующего вывода результатов расчета.

Если элемент VPN вскрыт, то в блоке 7 значение количества вскрытых элементов VPN ($N_{\text{вскр эл}}$) увеличивается на 1.

В блоке 8 осуществляется цикл по расчету вероятности вскрытия всех элементов VPN, после чего в блоке 9 осуществляется расчет статистической оценки вероятности вскрытия VPN в целом:

$$\widehat{P}_{\text{вскрССCН}}(t_{\text{кcc}^*}) = \frac{N_{\text{вскр. эл}}}{N_{\text{эсссн}}}, \quad (6)$$

где $N_{\text{вскр. эл}}$ – количество вскрытых элементов VPN; $N_{\text{эсссн}}$ – общее число элементов VPN; $t_{\text{кcc}^*}$ – время квазистационарного состояния VPN.

В блоке 10 сравнивают значения вероятности вскрытия VPN с нормированным значением и принимают решение о его вскрытии, после чего в блоке 11 рассчитывают фактическое время вскрытия VPN ($t_{\text{вскрСС}}$).

Далее в блоке 12 сравнивают значения времени вскрытия VPN с нормированным значением и принимают решение о вскрытии VPN.

В блоке 13 рассчитывают зависимости группы показателей функционирования элемента VPN от групп показателей параметров вскрытия средствами СиП КР злоумышленника и определяют зависимость между количеством средств вскрытия СиП КР злоумышленника ($N_{\text{вскр}j}$) и временем квазистационарного состояния элемента VPN ($t_{\text{кcc}}$) по формуле

$$N_{\text{вскр. }j} = \frac{\overline{T}_{\text{вскр. }j} \cdot (1-P_{\text{вскр}}) \cdot (N_{\text{эсссн}} + N_{\text{ЕСЭ}})}{t_{\text{кcc}} \cdot K_2}, \quad (7)$$

где K_2 – коэффициент контраста параметров элемента VPN-переменной; $\overline{T}_{\text{вскр. }j}$; $N_{\text{эсссн}}$; $N_{\text{ЕСЭ}}$; $t_{\text{кcc}}$ – постоянное значение. По усмотрению пользователя возможны определение иных функциональных зависимостей с использованием имеющихся исходных данных и промежуточных результатов и их расчет.

В блоке 14 выводятся результаты расчета выбранных показателей. На рисунках 2–3 представлены некоторые из промежуточных и выходных результатов моделирования процесса вскрытия элемента VPN средствами СиП КР. В блоке 15 осуществляется контроль времени моделирования.

Модель элемента VPN как объекта DDoS-атак

Вторая часть моделирующего алгоритма VPN как объекта СиП КР представлена на рисунке 4 и заключается в следующей последовательности действий.

В блоке 1 осуществляют ввод исходных данных, в котором задают среднее время DDoS-атаки j-го злоумышленника на элемент VPN ($\overline{T}_{\text{атак }j}$); сетевой ресурс, используемый абонентами элемента VPN ($R_{\text{аб }j}$); мощность атаки злоумышленника на элемент VPN ($R_{\text{атак }j}$); имеющийся сетевой ресурс элемента VPN, получае-

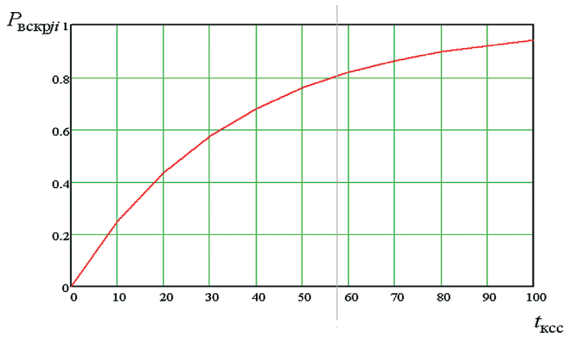

***Рис. 2**. Зависимость вероятности вскрытия элемента VPN от времени квазистационарного состояния элемента VPN*

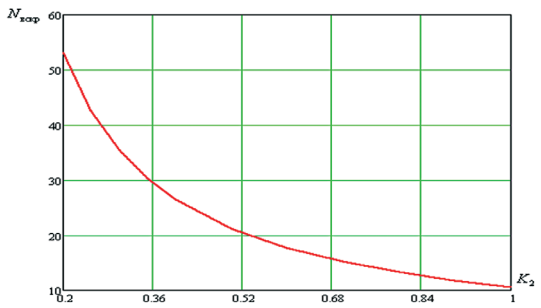

***Рис. 3**. Зависимость количества средств вскрытия СиП КР от коэффициента контраста элемента VPN*

мый у доверенного оператора связи РФ ($R_{эсс\ i}$); быстродействие бот-сети, используемой злоумышленником ($R_{бот\text{-}сеть\ zj}$); быстродействие системы защиты элемента VPN ($R_{СЗ}$); время квазистационарного состояния элемента VPN ($t_{ксс}$); среднее время вскрытия злоумышленником элемента VPN средствами СиП КР ($\overline{T}_{вскр.\ j}$); количество элементов VPN ($N_{эсссн}$).

В блоке 2 формируют имитационную модель элемента VPN как объекта DDoS-атак, в которой на основе потребностей системы управления определяют количество абонентов, категории абонен-

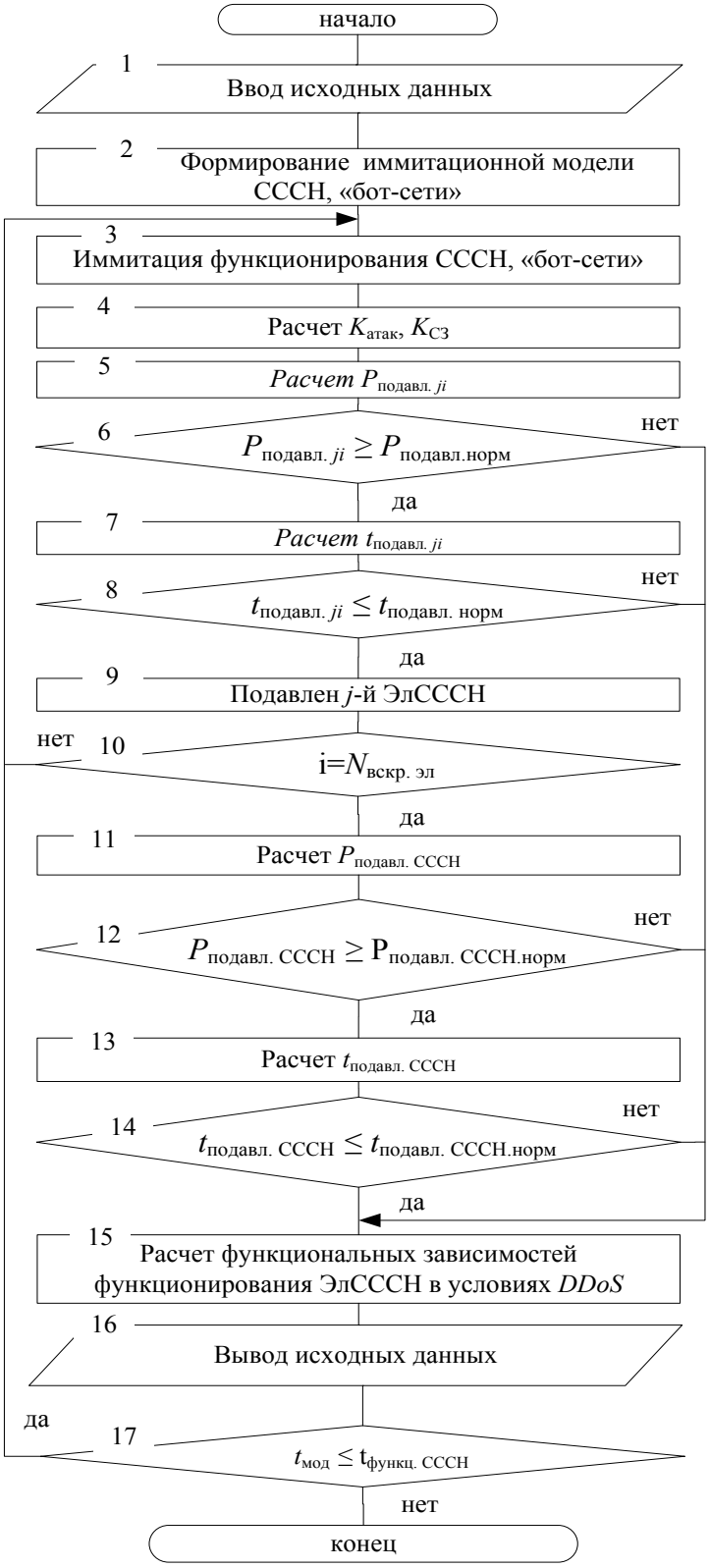

Рис. 4. *Схема моделирующего алгоритма VPN как объекта DDoS-атаки*

тов, предоставляемые услуги связи различным категориям абонентов и значения параметров предоставляемых услуг. С учетом потребностей различных абонентов элемента VPN, топологии VPN и требуемых услуг связи определяют количество рабочих направлений и значения передаваемых информационных потоков. Далее формируют структуру бот-сети и работы обслуживающего устройства элемента VPN.

В блоке 3 имитируют функционирование элемента VPN в условиях предоставления услуг связи различным абонентам как объекта DDoS-атак. При этом осуществляется генерация пакетов передаваемой информации по заданным законам распределения с заданной длиной пакета от различных категорий абонентов элемента VPN; производится объединение информационных потоков различных категорий абонентов элемента VPN в единый исходящий информационный поток элемента VPN; генерируются информационные потоки от элементов VPN по заданному закону распределения информационных потоков и объему передаваемой информации; производится объединение информационных потоков различных элементов VPN в единый входящий информационный поток элемента VPN; генерируется информационный поток от бот-сети по заданному закону распределения и объему информации, передаваемой элементу VPN. Далее имитируется работа обслуживающего устройства с заданной производительностью.

В блоке 4 осуществляют расчет коэффициента эффективной мощности атаки j-го злоумышленника на элемент VPN, коэффициента способности системы защиты элемента VPN противодействовать DDoS-атаке.

Коэффициент эффективной мощности атаки j-го злоумышленника на элемент VPN рассчитывается по формуле

$$K_3 = \frac{R_{\text{аб.}i} + \overline{R}_{\text{атак}\,i}}{R_{\text{эсс}i}}, \qquad (8)$$

где $R_{\text{аб. }j}$ – значения параметра используемого сетевого ресурса абонентами элемента VPN; $\overline{R}_{\text{атак. }j}$ – значения средней максимальной мощности атаки j-го злоумышленника на элемент VPN; $R_{\text{эсс. }i}$ – имеющийся сетевой ресурс элемента VPN, получаемый у доверенного оператора связи РФ.

Коэффициент способности системы защиты элемента VPN противодействовать DDoS-атаке рассчитывается по формуле

$$K_4 = \frac{R_{\text{бот-сеть }sj}}{R_{\text{СЗ}}}, \qquad (9)$$

где $R_{\text{бот-сеть }sj}$ – быстродействие s-й бот-сети, используемой j-м злоумышленником; $R_{\text{СЗ}}$ – быстродействие системы защиты элемента VPN.

В блоке 5 осуществляют расчет вероятности подавления DDoS-атакой j-го злоумышленника i-го элемента VPN ($P_{\text{подавл}ji}(t_{\text{ксс}})$) по формуле

$$P_{\text{подавл. }ji}(t_{\text{ксс}}) = 1 - e^{-\frac{(t_{\text{ксс}} - \overline{T}_{\text{вскр. }j}) \cdot K_3 \cdot K_4}{\overline{T}_{\text{атак }j}}}, \qquad (10)$$

где K_3 – коэффициент эффективной мощности атаки j-го злоумышленника на элемент VPN; K_4 – коэффициент способности системы защиты элемента VPN противодействовать DDoS-атаке, $\overline{T}_{\text{атак }j}$ – среднее время DDoS-атаки j-го злоумышленника на элемент VPN.

В блоке 6 сравнивают значения вероятности подавления элемента VPN с нормированным значением и принимают решение о его подавлении. Если элемент сети связи не подавлен, полученное значение вероятности подавления элемента VPN сохраняют в базе данных для последующего вывода результатов расчета.

В блоке 7 рассчитывается фактическое время подавления элемента VPN DDoS-атакой по формуле

$$t_{\text{подавл}} = \frac{-(t_{\text{ксс}} - t_{\text{вскр}}) \cdot K_3 \cdot K_4}{\ln(1 - P_{\text{подавл}})}. \qquad (11)$$

В блоке 8 сравнивают значения времени подавления элемента VPN с нормированным значением и принимают решение о его подавлении. Если элемент сети связи не подавлен, полученное значение времени подавления элемента VPN сохраняют в базе данных для последующего вывода результатов расчета.

Если элемент VPN вскрыт, то в блоке 9 значение количества подавленных элементов VPN ($N_{\text{подав.эл}}$) увеличивается на 1. В блоке 10 осуществляется цикл по расчету вероят-ности подавления всех элементов VPN.

В блоке 11 производится расчет статистической оценки вероятности подавления VPN в целом по формуле

$$\widehat{P}_{\text{подавл ССС Н}}(t_{\text{КСС}^*}) = \frac{N_{\text{подавл. эл}}}{N_{\text{эсссн}}}, \qquad (12)$$

где $N_{\text{подавл. эл}}$ – количество подавленных элементов VPN; $N_{\text{эсссн}}$ – общее число элементов VPN, $t_{\text{ксс}^*}$ – фактическое время квазистационарного состояния VPN.

В блоке 12 сравнивают значения вероятности подавления VPN с нормированным значением и принимают решение о подавлении VPN в целом.

В блоке 13 рассчитывается фактическое время подавления VPN в целом ($t_{\text{подав СС}}$).

В блоке 14 сравнивают значения времени подавления VPN с нормированным значением и принимают решение о подавлении VPN. Если сеть связи не подавлена, полученное значение времени подавления VPN сохраняют в базу данных для последующего вывода результатов расчета.

В блоке 15 производят расчет зависимостей группы показателей функционирования элемента VPN от групп показателей параметров подавления с использованием DDoS-атак.

Определяют зависимость между временем подавления элемента DDoS-атакой злоумышленника и быстродействием системы защиты элемента VPN:

$$T_{\text{атак}} = \frac{-(t_{\text{кcc}} - t_{\text{вскр.}}) \cdot K_3 \cdot (\frac{R_{\text{бот-сет}}}{R_{\text{СЗ}}})}{\ln(1 - P_{\text{подавл.}})}, \quad (13)$$

где $R_{\text{СЗ}}$ – переменная; $t_{\text{кcc}}$; $t_{\text{вскр}}$; K_3; $R_{\text{бот-сет}}$ – постоянные значения.

Зависимость между временем подавления элемента DDoS-атакой злоумышленника и временем квазистационарного состояния элемента VPN $t_{\text{кcc}}$ для различных K_3:

$$T_{\text{атак}} = \frac{-(t_{\text{кcc}} - t_{\text{вскр.}}) \cdot K_3 \cdot K_4}{\ln(1 - P_{\text{подавл.}})}, \quad (14)$$

где $t_{\text{кcc}}$ – переменная; $t_{\text{вскр.}}$; K_4 – постоянные значения.

Зависимость мощности DDoS-атаки от времени атаки на элемент VPN:

$$R_{\text{атак}} = \frac{-\ln(1 - P_{\text{подавл.}}) \cdot t_{\text{подавл.}} \cdot (R_{\text{эссс}})}{(t_{\text{кcc}} - t_{\text{вскр.}}) \cdot K_4} - R_{\text{аб}}, \quad (15)$$

где $t_{\text{подавл.}}$ – переменная; $t_{\text{кcc}}$; $t_{\text{вскр.}}$; K_3; $R_{\text{эссс}}$; $R_{\text{аб}\ j}$ – постоянные значения.

Зависимость быстродействия бот-сети злоумышленника от времени атаки на элемент VPN:

$$R_{\text{бот-сет}} = \frac{t_{\text{атак}} \cdot R_{\text{СЗ}} \cdot \ln(1 - P_{\text{подавл}})}{-(t_{\text{кcc}} - t_{\text{вскр}})K_3}, \quad (16)$$

где $t_{\text{атак}}$ – переменная; $t_{\text{кcc}}$; $t_{\text{вскр}}$; K_3; $R_{\text{СЗ}}$ – постоянные значения.

Помимо этого по усмотрению пользователя возможно определение иных функциональных зависимостей с использованием имеющихся исходных данных и промежуточных результатов и их расчет.

В блоке 16 выводятся результаты моделирования. На рисунках 5, 6 представлены некоторые из промежуточных выходных результатов моделирования процесса подавления элемента VPN DDoS-атакой. В блоке 17 осуществляется контроль времени моделирования.

Моделирующие алгоритмы процессов ведения СиП КР и подавления элемента DDoS-атакой реализованы в программных средах GPSS World, «C++». Результаты оценки качества разработанной модели удовлетворяют общепринятым требованиям.

Таким образом, в рамках содержательного описания модели элементов VPN как объекта СиП КР и DDoS-атак злоумышленника разработаны: структура элемента VPN как объекта ведения злоумышленником СиП КР, структура элемента VPN как объекта DDoS-атаки.

Выводы

Научная новизна разработанной модели заключается в учете многообразия параметров (ДМП) элементов VPN, позволяет имитировать динамику функционирования элемента VPN, интегрированного с ЕСЭ РФ в условиях ведения

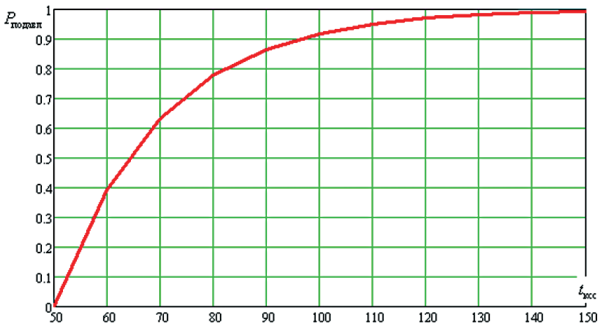

***Рис. 5**. Зависимость вероятности подавления элемента VPN от времени его функционирования*

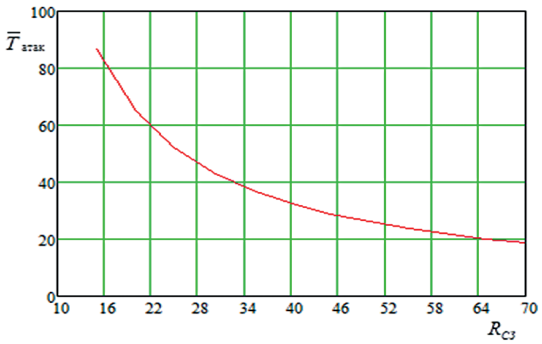

***Рис. 6**. Зависимость среднего времени подавления элемента VPN от быстродействия системы защиты*

СиП КР, DDoS-атак и получать на этой основе вероятностно-временные зависимости основных показателей функционирования элементов VPN во времени в условиях ведения СиП КР и DDoS-атак, а также определять значения времени квазистационарного состояния элементов VPN (времени подключения элемента VPN к точке доступа ЕСЭ РФ), необходимого для обеспечения своевременного предоставления услуг специальной связи абонентам.

Разработанное научно-методическое обеспечение предназначено для научно-исследовательских организаций с целью обоснования и разработки руководящих документов, регламентирующих порядок планирования, развертывания и функционирования VPN, интегрированной с ЕСЭ РФ в условиях ведения СиП КР и DDoS-атак.

Представленное в разделе научно-методическое обеспечение является основой и определяет наиболее перспективные направления для разработки подходов и научно-технических предложений по оценке степени защищенности элементов VPN от СиП КР и DDoS-атак.

Последовательность действий, представленная в модели элементов VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак, реализована в патенте РФ на изобретение № 2541205, 10.02.2015, также разработаны две программы для ЭВМ. Модель повышает достоверность прогнозирования развития атак, вследствие чего повышается защищенность элементов VPN за счет своевременного принятия мер по противодействию сетевым атакам [10].

Научная новизна разработанной модели заключается в том, что с ее помощью можно учитывать ресурсы злоумышленника по вскрытию элементов VPN, подавлению элемента VPN с применением DDoS-атак, а также оценивать возможности злоумышленника по подавлению элементов VPN с учетом успешности ведения СиП КР. В модели учитываются особенности ДМП элемента VPN, которые влияют на правильность и своевременность ведения разведки.

***Рецензент**: Бухарин В.В., доктор технических наук, сотрудник Академии ФСО России, г. Орел, bobah_buch@mail.ru.*

Литература:

1. Путин В.В. Заседание Совета Безопасности, посвященное вопросам противодействия угрозам национальной безопасности в информационной сфере, 2014. URL: http://kremlin.ru/news (дата обращения 01.10.2014).
2. Стародубцев Ю.И., Бухарин В.В., Кирьянов А.В., Баленко О.А. Метод оценки защищенности информационно-телекоммуникационной сети от деструктивных программных воздействий // Вестник компьютерных и информационных технологий. 2013. № 4 (106). С. 37-42.
3. Бухарин В.В., Караечев С.Ю. Метод защиты информационного обмена сегментов распределенной мультисервисной сети // Технологии техносферной безопасности. 2015. № 4 (62). С. 306-312.
4. Добрышин М.М., Диденко П.М. Оценка защищенности беспроводных сетей связи. В сборнике: Радиотехника, электроника и связь («РЭиС-2013») Сборник докладов II Международной научно-технической конференции. ОАО «ОНИИП». 2013. С. 155-160.
5. Макаренко С.И., Михайлов Р.Л. Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4 (12). С. 69-79.
6. DDoS-атаки в третьем квартале 2015 года. URL: http://www.comss.info/page.php?al= DDoS_ataki_v_tretem_ kvartale_2015_ goda (дата обращения: 24.04.16).
7. Qrator Labs: В 2015 году в Рунете возросло количество DDoS-атак. URL: http://www.securitylab.ru/.
8. Гречишников Е. В., Добрышин М. М. Оценка защищенности элементов сети связи при информационно-технических воздействиях. Сборник трудов XXXIV Всероссийской научно-технической конференции / Проблемы эффективности и безопасности функционирования сложных технических и информационных систем // Ч. 6. Военная академия ракетных войск стратегического назначения им. Петра Великого. Серпухов, Московская область, 2015. С.11–14.
9. Гречишников Е. В., Горелик С. П., Добрышин М. М. Способ обеспечения требуемой защищенности сети связи от внешних деструктивных воздействий // Телекоммуникации. 2015. № 6. С. 32-37.
10. 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.

 УДК 004.942

A MODEL OF A VPN ACCESS POINT AS OF AN OBJECT OF NETWORK AND STREAMING COMPUTER INTELLIGENCE AND DDOS ATTACKS

Grecihnikov E.V.[4], Dobrusin M.M.[5], Suchalkin P.V.[6]

The increase in the number of network attacks and the power of destructive impacts on virtual private networks, requires officials to timely assess the extent of damage and measures for its minimization. Available scientific and technical solutions, damage assessment, network attacks do not fully account for the resources of the attacker by opening a network connection and the destructive impact on it. The attacker is not always able to reliably reveal the structure of the communication network and has limited resources impact. When assessing the capabilities of the enemy to open up the network are not taken into account or not fully considered ways to reduce the contrast of the characteristics of the communication network in a feature space Unified telecommunication network of the Russian Federation. The use of the proposed model allows on the basis of a probabilistic approach to predict and estimate the damage caused by DDoS-attacks to the access nodes of the virtual private network and its ability to perform its tasks as intended in terms of doing DDoS attacks. The paper uses statistical data about the capabilities of the attacker on the management of computer intelligence and DDoS attacks. On the basis of the damage assessment, officials make a decision about reconfiguring the network connection. When using the developed model can perform the following tasks: security assessment of the structural elements and communication network by evaluating the capabilities of the attacker on opening and the impact on network communication, performance assessment use of resources available to the attacker, the planning of communication networks in terms of maintenance of the network and streaming of the intelligence and destructive impacts.

***Keywords**: virtual private network, monitoring, secure network communication, the probability of opening, contrast, the probability of suppression.*

References:

1. Putin V. V. Zasedanie Soveta Bezopasnosti, posvyashchennoe voprosam protivodeystviya ugrozam natsional'noy bezopasnosti v informatsionnoy sfere, 2014. URL: http://kremlin.ru/news.
2. Starodubtsev Yu.I., Bukharin V.V., Kir'yanov A.V., Balenko O.A. Metod otsenki zashchishchennosti informatsionno-telekommunikatsionnoy seti ot destruktivnykh programmnykh vozdeystviy, Vestnik komp'yuternykh i informatsionnykh tekhnologiy. 2013. No 4 (106), pp. 37-42.
3. Bukharin V. V., Karaechev S. Yu. Metod zashchity informatsionnogo obmena segmentov raspredelennoy mul'tiservisnoy seti, Tekhnologii tekhnosfernoy bezopasnosti. 2015. No 4 (62), pp. 306-312.
4. Dobryshin M. M., Didenko P. M. Otsenka zashchishchennosti besprovodnykh setey svyazi. V sbornike: Radiotekhnika, elektronika i svyaz' («REiS-2013») Sbornik dokladov II Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. OAO «ONIIP». 2013, pp. 155-160.
5. Makarenko S. I., Mikhaylov R. L. Otsenka ustoychivosti seti svyazi v usloviyakh vozdeystviya na nee destabiliziruyushchikh faktorov, Radiotekhnicheskie i telekommunikatsionnye sistemy. 2013. No 4 (12), pp. 69-79.
6. DDoS-ataki v tret'yem kvartale 2015 goda. URL: http://www.comss.info/page.php?al= DDoS_ataki_v_tretem_ kvartale_ 2015_goda.
7. Qrator Labs: V 2015 godu v Runete vozroslo kolichestvo DDoS-atak. URL: http://www.securitylab.ru/.
8. Grechishnikov E. V., Dobryshin M. M. Otsenka zashchishchennosti elementov seti svyazi pri informatsionno-tekhnicheskikh vozdeystviyakh. Sbornik trudov XXXIV Vserossiyskoy nauchno-tekhnicheskoy konferentsii, Problemy effektivnosti i bezopasnosti funktsionirovaniya slozhnykh tekhnicheskikh i informatsionnykh system, Ch. 6. Voennaya akademiya raketnykh voysk strategicheskogo naznacheniya im. Petra Velikogo. Serpukhov, Moskovskaya oblast', 2015, pp.11–14.
9. Grechishnikov E. V., Gorelik S. P., Dobryshin M. M. Sposob obespecheniya trebuemoy zashchishchennosti seti svyazi ot vneshnikh destruktivnykh vozdeystviy, Telekommunikatsii. 2015. No 6, pp. 32-37.
10. Grechishnikov E. V., Dobryshin M. M., Belov A. S., Kuz'mich A. A. Sposob otsenki effektivnosti informatsionno-tekhnicheskikh vozdeystviy na seti svyazi, Patent na izobretenie No 2541205, 24.12.2014.

4 Evgeny Grecihnikov, D.Sc., Associate Professor, The Academy of Federal Security Guard Service of the Russian Federation, Orel
5 Mikhail Dobrushin, The Academy of Federal Security Guard Service of the Russian Federation, Orel, dobrithin@ya.ru
6 Pavel Suchalkin, Ph.D., The Academy of Federal Security Guard Service of the Russian Federation, Orel