Модель реализации компьютерной атаки «Отказ в обслуживании» на сеть пакетной радиосвязи

Implementation model of Denial-of-Service cyber attack on packet radio network

Присяжнюк / Prisyazhnyuk S.
Сергей Прокофьевич
(office@itain.ru)
доктор технических наук, профессор,
заслуженный деятель науки РФ,
действительный член Академии инженерных наук им. А. М. Прохорова.
ЗАО «Институт телекоммуникаций»,
генеральный директор.
г. Санкт-Петербург

Канаев / Kanaev A.
Андрей Константинович
(kanaev@pgups.ru)
доктор технических наук, профессор.
ФГБОУ ВО "Петербургский государственный университет путей сообщения Императора Александра I" (ПГУПС), заведующий кафедрой «Электрическая связь».
г. Санкт-Петербург

Сахарова / Sakharova M.
Мария Александровна
(saharova@itain.ru, zuvakamariya@mail.ru)
кандидат технических наук.
ПГУПС, доцент кафедры «Электрическая связь».
г. Санкт-Петербург

Сорокин / Sorokin R.
Роман Павлович
(123roman456@mail.ru)
ПГУПС, аспирант кафедры «Электрическая связь».
г. Санкт-Петербург

Ключевые слова: пакетная радиосвязь – packet radio; информационная безопасность – information security; угроза «Отказ в обслуживании» – Denial-of-Service threat; имитационное моделирование – simulation.

В статье приведена оценка возможности создания угрозы информационной безопасности пакетной радиосети за счет разработки имитационной модели действий злоумышленника при реализации атаки типа «Отказ в облуживании», а также получены вероятностно-временные характеристики исследуемого процесса.

The article provides assessment of information security threat for the packet radio network by using the developed simulation model of hacker's actions during Denial-of-Service attack, as well as probabilistic temporal characteristics of the studied process.

Введение

Пакетная радиосеть отличается своей универсальностью для различного круга пользователей за счет формирования выделенных каналов связи для передачи радиопакетов малого размера (по сравнению с классическими IP-сетями), что позволяет передавать данные удаленным объектам управления [1, 2]. Угрозы несанкционированного воздействия в пакетной радиосети реализуются путем создания нештатных режимов работы программно-аппаратных и аппаратных средств, в результате которых осуществляется нарушение конфиденциальности, целостности и доступности информации [3].

Причинами возникновения возможных угроз информационной безопасности пакетной радиосети являются преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения; несанкционированное внедрение и использование неразрешенных к применению программ, создающих уязвимости в программном и программно-аппаратном обеспечении; сбои в работе аппаратного и программного обеспечения, в том числе средств защиты информации (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.) [4].

Указанные причины были учтены при разработке имитационной модели реализации угрозы «Отказ в обслуживании» на сеть пакетной радиосвязи, которая позволяет оценить вероятность успешного совершения атаки при наличии различных уязвимостей. Модель может быть использована на этапах проектирования и разработки средств защиты передачи информации как в сетях радиосвязи, так и в сетях проводной связи

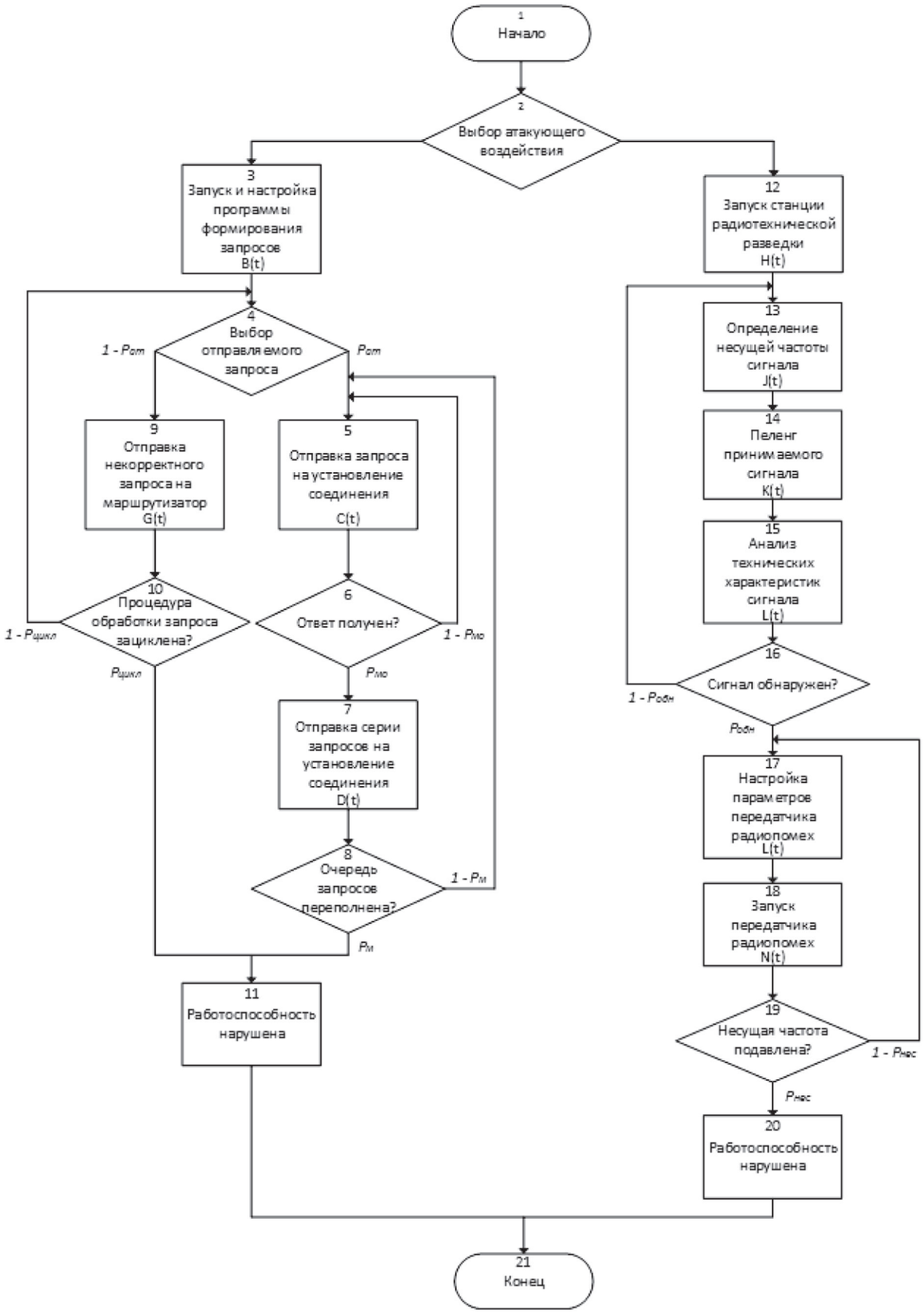

Рис. 1. Укрупненный алгоритм реализации атаки типа «Отказ в обслуживании»

в виду своей универсальности и быстрого изменения параметров.

Принцип реализации атаки типа «Отказ в обслуживании»

Общий анализ возможных атак показывает, что наиболее эффективным способом воздействия на пакетную радиосеть с целью изменения состояния её защищенности [5] является атака типа «Отказ в обслуживании». В настоящее время не существует эффективных и универсальных средств и методов защиты от данного типа атак.

При реализации данной атаки злоумышленник задействует большую часть ресурсов атакуемого объекта путем отправки ложных запросов на обслуживание, на каждый из которых атакуемый объект отвечает пакетом-подтверждением. В результате при постоянном потоке запросов буфер ожидания полуоткрытых соединений будет заполнен и не сможет обрабатывать запросы от настоящих пользователей.

Выделяют несколько способов реализации атаки: от довольно простых взаимодействий путем преднамеренного создания помех до сложных методов дезинформации атакуемого устройства [6].

Данная атака в отличие от остальных не нацелена на получение доступа к сети или на получение из этой сети какой-либо информации. Одним из ключевых элементов проектируемой пакетной радиосети является маршрутизатор, на который может быть реализована атака типа «Отказ в обслуживании», способная сделать сеть недоступной для использования путём превышения допустимых пределов функционирования сети, операционной системы или приложения. Алгоритм реализации атаки представлен на рис. 1.

Рассмотрено два варианта реализации атаки:

1. Злоумышленник осуществляет запуск и настройку программы, осуществляющей формирование и направление запросов за среднее время $\overline{t}_{\text{прог}}$ с функцией распределения $B(t_b) = 1 - \exp(-\lambda_b \times t_b)$. Затем с вероятностью $P_{\text{ат}}$ направляется запрос на маршрутизатор для установления соединения за среднее время $\overline{t}_{\text{зап}}$ с функцией распределения $C(t_c) = 1 - \exp(-\lambda_c \times t_c)$. После получения ответа от маршрутизатора за среднее время $\overline{t}_{\text{шт}}$ с функцией распределения $D(t_d) = 1 - \exp(-\lambda_d \times t_d)$ производится отправка большого количества («шторма») анонимных запросов на подключение от имени других объектов. Из-за переполнения очереди запросов с вероятностью $P_{\text{м}}$ маршрутизатор не в состоянии обрабатывать запросы и нарушается его работоспособность.

Кроме того, с вероятностью $(1 - P_{\text{ат}})$ на атакуемый маршрутизатор может быть отправлен некорректный, специально подобранный запрос за среднее время $\overline{t}_{\text{изап}}$ с функцией распределения $G(t_g) = 1 - \exp(-\lambda_g \times t_g)$. В этом случае при наличии ошибок в удаленной системе с вероятностью $P_{\text{цикл}}$ возможно зацикливание процедуры обработки запроса, что приведет к переполнению буфера с последующим отказом в обработке входящих запросов [6–8].

2. Радиоэлектронная атака, при которой происходит нарушение работы и снижение эффективности радиосредств, путем постановки помех радиоэлектронным системам и средствам [9]. При ее реализации злоумышленник за среднее время $\overline{t}_{\text{разв}}$ с функцией

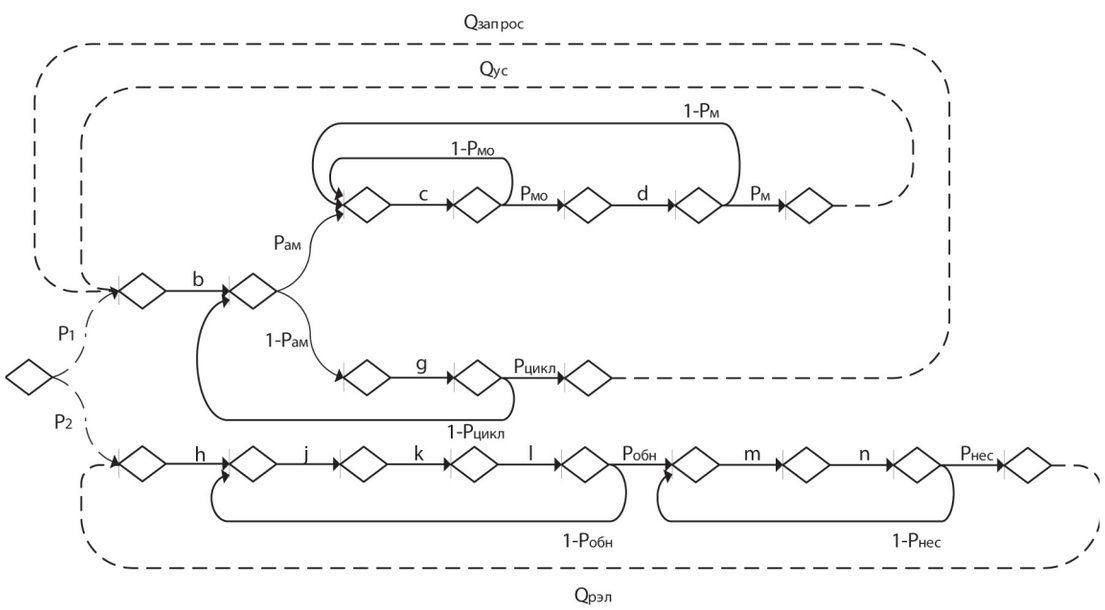

Рис. 2. Стохастическая GERT-сеть реализации атаки «Отказ в обслуживании»

распределения $H(t_h)=1-\exp(-\lambda_h \times t_h)$ запускает станцию радиотехнической разведки для определения радиочастотных характеристик сигнала. Далее он определяет несущую частоту сигнала за среднее время $\overline{t}_{\text{нес}}$ с функцией распределения $J(t_j)=1-\exp(-\lambda_j \times t_j)$, проводит пеленг принимаемого сигнала за среднее время $\overline{t}_{\text{пел}}$ с функцией распределения $K(t_k)=1-\exp(-\lambda_k \times t_k)$ и проводит анализ полученных характеристик сигнала за среднее время $\overline{t}_{\text{анализ}}$ с функцией распределения $L(t_l)=1-\exp(-\lambda_l \times t_l)$. С вероятностью $P_{\text{обн}}$ радиосигнал будет обнаружен, и будут определены все его технические характеристики.

После успешного обнаружения сигнала злоумышленник настраивает передатчик радиопомех за среднее время $\overline{t}_{\text{рпмх}}$ с функцией распределения $M(t_m)=1-\exp(-\lambda_m \times t_m)$ и производит запуск передатчика прицельной радиопомехи за среднее время $\overline{t}_{\text{перрпмх}}$ с функцией распределения $N(t_n)=1-\exp(-\lambda_n \times t_n)$. С вероятностью $P_{\textbf{нес}}$ несущая частота передаваемого сигнала будет подавлена, что нарушит работоспособность устройств.

Эквивалентная функция стохастической GERT-сети реализации атаки «Отказ в обслуживании» определяется из топологического уравнения. В общем виде эквивалентная функция $Q(s)$ для стохастической GERT-сети произвольной структуры имеет вид:

$$Q(s)=\frac{\prod_{j=1}^{k} f_j(s)}{1+\sum_{l=1}^{M}(-1)^l W_l(s)},$$

где k – количество функций $f_i(s)$ в прямой цепи стохастической GERT-сети процесса мониторинга узла сети.

Для каждой ветви, взвешенной двумя параметрами: функцией распределения времени выполнения ветви и вероятностью ее выполнения, определяются изображения функции распределения времени с помощью интегрального преобразования Лапласа. Например, для выполнения операции определения злоумышленником несущей частоты сигнала плотность распределения вероятности имеет вид: $J(t)=\lambda_j \times \exp(-\lambda_j \times t_j)$, а изображение будет $J(s)=\int_0^{\infty}\lambda_j \times \exp(-\lambda_j \times t_j)\times \exp(-s \times t_j)=\frac{j}{s+j}$. Аналогично будут выполнены процессы преобразования Лапласа для всех подпроцессов алгоритма (рис. 2).

Определим вероятностно-временные характеристики (ВВХ) СС процесса мониторинга узла сети при помощи метода двухмоментной аппроксимации.

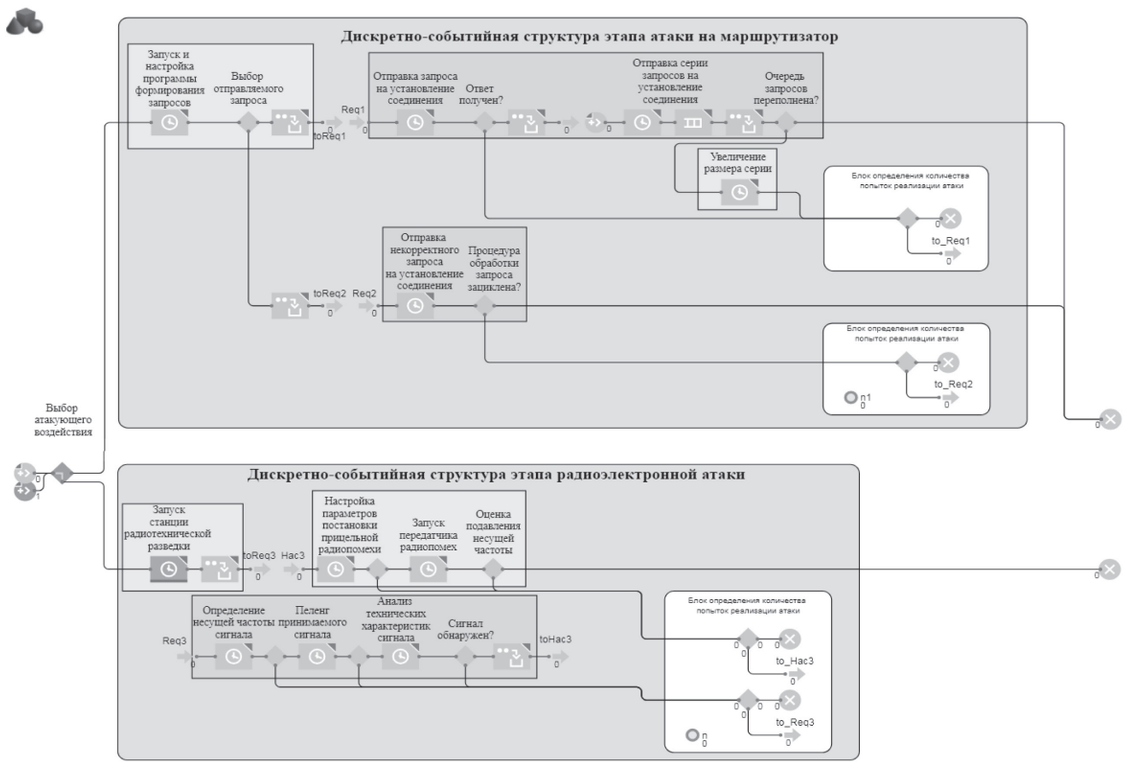

Рис. 3. Имитационная модель действий нарушителя при реализации атаки «Отказ в обслуживании»

Таблица 1

Вероятностно-временные характеристики реализации атаки

№	Характеристика действий нарушителя	Условное обозначение	Значение
1	Запуск и настройка программы формирования запросов	$\overline{t}_{\text{прог}}$	20 секунд
2	Функция распределения времени $t_{\text{прог}}$	$B(t)$	normal (10,30)
3	Вероятность отправки запроса на установление соединения	$P_{\text{ат}}$	0,5
4	Отправка запроса на установление соединения	$\overline{t}_{\text{зап}}$	2 секунды
5	Функция распределения времени $t_{\text{зап}}$	$C(t)$	normal (1,3)
6	Вероятность получения ответа от маршрутизатора	$P_{мо}$	normal (0.4,0.99)
7	Отправка серии запросов на установление соединения	$\overline{t}_{\text{шт}}$	5 минут
8	Функция распределения времени $t_{\text{шт}}$	$D(t)$	normal (1,10)
9	Вероятность переполнения очереди запросов	$P_{м}$	normal (0.4,0.99)
10	Вероятность отправки некорректного запроса на маршрутизатор	$(1 - P_{\text{ат}})$	0,5
11	Отправка некорректного запроса	$\overline{t}_{\text{изап}}$	3 секунды
12	Функция распределения времени $t_{\text{изап}}$	$G(t)$	normal (1,5)
13	Вероятность зацикливания процедуры обработки запросов	$P_{\text{цикл}}$	normal (0.4,0.99)
14	Запуск станции радиотехнической разведки	$\overline{t}_{\text{разв}}$	8 минут
15	Функция распределения времени $t_{\text{разв}}$	$H(t)$	normal (5,10)
16	Определение несущей частоты	$\overline{t}_{\text{нес}}$	3 минуты
17	Функция распределения времени $t_{\text{нес}}$	$J(t)$	normal (2,5)
18	Пеленг принимаемого сигнала	$\overline{t}_{\text{пел}}$	3 минуты
19	Функция распределения времени $t_{\text{пел}}$	$K(t)$	normal (2,5)
20	Анализ технических характеристик сигнала	$\overline{t}_{\text{анализ}}$	12 минут
21	Функция распределения времени $t_{\text{анализ}}$	$L(t)$	normal (5,20)
22	Вероятность обнаружения сигнала	$P_{\text{обн}}$	normal (0.5,0.99)
23	Настройка параметров передатчика радиопомех	$\overline{t}_{\text{рпмх}}$	12 минут
24	Функция распределения времени $t_{\text{рпмх}}$	$M(t)$	normal (5,20)
25	Запуск передатчика радиопомех	$\overline{t}_{\text{перрпмх}}$	3 минуты
26	Функция распределения времени $t_{\text{перрпмх}}$	$N(t)$	normal (2,5)
27	Вероятность подавления несущей частоты	$P_{\text{нес}}$	normal (0.4,0.99)

Вычисление математического ожидания и дисперсии позволяет приближенно определить функцию распределения времени реализации цикла управления как неполную гамма-функцию [11].

Тогда эквивалентные Q-функции реализации атаки будут иметь вид:

$$\begin{cases} Q_{\text{ус\_серия}}(s) = \dfrac{\dfrac{b}{b+s}\dfrac{c}{c+s}\dfrac{d}{d+s}P_{\text{М0}}}{1-\dfrac{c}{c+s}(1-P_{\text{М0}})}; \\ \text{где } Q_{\text{ус\_серия}}(0)=1;\ P_{ам}=1;\ P_{\text{М}}=1 \\ Q_{\text{ус\_ответ}}(s) = \dfrac{\dfrac{b}{b+s}\dfrac{c}{c+s}\dfrac{d}{d+s}P_{\text{М}}}{1-\dfrac{c}{c+s}\dfrac{d}{d+s}(1-P_{\text{М}})}; \\ \text{где } Q_{\text{ус\_ответ}}(0)=1;\ P_{ам}=1;\ P_{\text{М0}}=1 \\ Q_{\text{ус}}(s) = Q_{\text{ус\_серия}}(s) * Q_{\text{ус\_ответ}}(s);\ \text{где } Q_{\text{ус}}(0)=1 \\ Q_{\text{запрос}}(s) = \dfrac{\dfrac{b}{b+s}\dfrac{g}{g+s}P_{\text{цикл}}}{1-\dfrac{g}{g+s}(1-P_{\text{цикл}})};\ \text{где } Q_{\text{запрос}}(0)=1 \\ Q_{\text{рэл}}(s) = \dfrac{\dfrac{h}{h+s}\dfrac{j}{j+s}\dfrac{k}{k+s}\dfrac{l}{l+s}\dfrac{m}{m+s}\dfrac{n}{n+s}P_{\text{обн}}P_{\text{нес}}}{1-\dfrac{j}{j+s}\dfrac{k}{k+s}\dfrac{l}{l+s}(1-P_{\text{обн}})-\dfrac{m}{m+s}\dfrac{n}{n+s}(1-P_{\text{нес}})+} \\ \dfrac{}{+\dfrac{j}{j+s}\dfrac{k}{k+s}\dfrac{l}{l+s}\dfrac{m}{m+s}\dfrac{n}{n+s}(1-P_{\text{обн}})(1-P_{\text{нес}})};\ \text{где } Q_{\text{рэл}}(0)=1 \end{cases}$$

В силу достаточной сложности объекта исследования был использован аппарат имитационного моделирования, позволяющий предусмотреть наличие уязвимостей исследуемой сети, а также рассмотреть различные характеристики объектов реализации атаки, что является преимуществом по сравнению с аналитическими моделями, используемыми в [7]. Для создания модели использовалась среда имитационного моделирования AnyLogic [10].

Для представленного на рис. 1 алгоритма разработана модель действия нарушителя (рис. 3) в ходе выполнения всех операций для совершения несанкционированного доступа к информации.

Исходные данные, представленные в таблице, получены с помощью метода экспертной оценки специалистов, осуществляющих деятельность в области информационной безопасности.

В случае неуспешной реализации атаки злоумышленник предпринимает повторную попытку совершения несанкционированного доступа, причем число таких попыток (n) зависит от возможности злоумышленника оставаться необнаруженным в ходе реализации атаки, а также его оснащенности и подготовленности. С учетом этого получена вероятность успешного выполнения атаки «Отказ в обслуживании» для 1000 попыток реализации. При этом в случае неуспешной реализации одного из этапов атаки, злоумышленник выполняет повторную попытку в соответствии с заданным числом попыток реализации (n).

Результаты моделирования

Результаты моделирования представлены на рисунках 4–7, анализ которых позволил сделать следующие выводы:

– среднее время реализации «атаки на маршрутизатор» с вероятностью ее успешной реализации не менее 0,8 составляет 7 минут, при этом достаточно осуществить 3 попытки реализации;

– реализация «радиоэлектронной атаки» с вероятностью не менее 0,8 составит 57 минут, при этом также достаточно осуществить 3 попытки.

Полученные результаты показали, что в условиях информационного воздействия степень опасности атаки

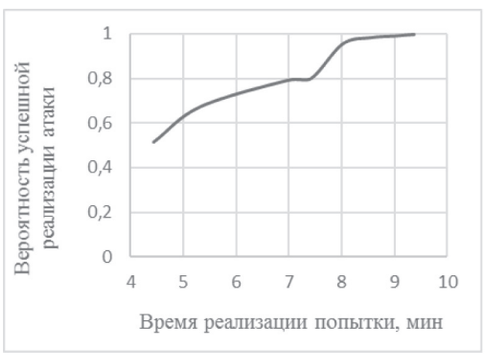

Рис. 4. Вероятностно-временные характеристики процесса реализации атаки на маршрутизатор

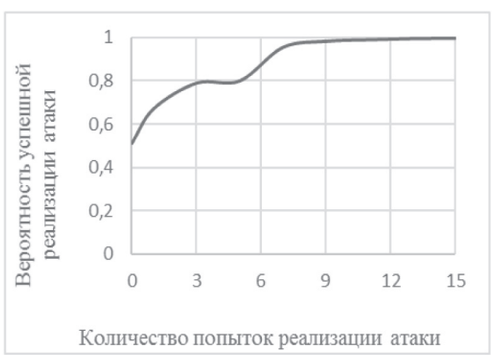

Рис. 5. Зависимость вероятности успешной реализации атаки на маршрутизатор от количества попыток реализации

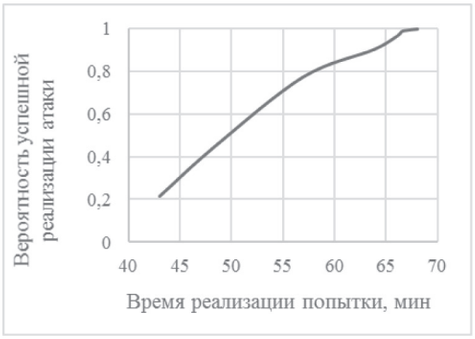

Рис. 6. Вероятностно-временные характеристики реализации радиоэлектронной атаки

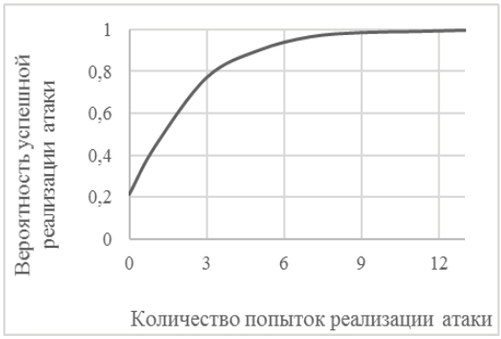

Рис. 7. Зависимость вероятности успешной реализации радиоэлектронной атаки от количества попыток реализации

предопределяется исходным уровнем защиты радиосети. На основе анализа рассмотренных атак, их принципов действия и структуры получены вероятностно-временные характеристики реализации информационного воздействия, позволяющие провести сравнение с нормативными требуемыми значениями, определяемыми исходным уровнем защиты передачи информации, что позволяет осуществить выбор комплекса средств защиты и провести повторное моделирование с учетом полученных значений.

Заключение

Разработанная модель позволяет оценивать вероятностно-временные характеристики при различных значениях исходных параметров реализации этапов атаки, а также с учетом влияния различных факторов обеспечения безопасности передачи информации в условиях функционирования пакетной радиосети.

Анализ результатов моделирования информационных воздействий позволит выдвинуть предложения по формированию программного модуля сканирования и обработки атак в сетевом трафике.

Применение имитационного моделирования в качестве основного метода исследования позволит совершенствовать алгоритм реализации атаки без кардинального изменения аппарата модели при выявлении новых уязвимостей сетей связи. На основе изученной методики возможна разработка аналогичных моделей реализации множества сетевых атак для расширения диапазона проводимого исследования.

Литература

1. Присяжнюк, С. П. Модель управления когнитивной декаметровой радиосетью / С.П. Присяжнюк, А.С. Присяжнюк // Информация и Космос. – 2018. –№ 4. – С. 44–48.

2. Дискретно-событийная модель функционирования пакетной радиосети КВ-диапазона общего пользования / С.П. Присяжнюк [и др.] // Информация и Космос. – 2019. – № 2. – С. 41–48.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). – ФСТЭК России, 2008.

4. Канаев, А. К. Формирование процесса управления безопасностью организации, реализующей технологический процесс / А.К. Канаев, Е.В. Опарин // Сборник трудов 73-й Всероссийской научно-технической конференции, посвященная Дню радио, 2018 – С. 302–303.

5. ГОСТ Р 56205–2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. – Введ. 01–01–2016. – Москва: Стандартинформ, 2014. – 77 с.

6. Канаев, А. К. Модели функционирования транспортной сети связи специального назначения, учитывающие высокую динамику изменения состояний сети вследствие внешнего воздействия / А.К. Канаев, Д.В. Марченко, Д.В. Субботин // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. Т. 4. / под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб.: СПбГУТ, 2018.– С. 304–308.

7. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М.А. Коцыняк [и др.] – СПб.: ЛО ЦНИИС, 2014. – 126 с.

8. Ануфренко, А. В. Модель воздействия злоумышленника на фрагмент транспортной сети связи на основе технологии Carrier Ethernet / А.В. Ануфренко, А.К. Канаев, Э.В. Логин // Труды учебных заведений связи. – 2018. – Т. 4, № 3. – С. 17–25.

9. Куприянов, А. И. Радиоэлектронные системы в информационном конфликте / А.И. Куприянов, А.В. Сахаров. – 2-е изд. – М.: Вузовская книга, 2015. – 528 с.

10. Боев, В. Д. Компьютерное моделирование: Пособие для курсового и дипломного проектирования / В.Д. Боев, Д.И. Кирик, Р.П. Сыпченко. – СПб.: ВАС, 2011. – 348 с.

11. Pritsker, A. A. B. GERT: Graphical evaluation and review technique / A.A.B. Pritsker // Memorandum RM-4973-NASA: April 1966. – 138 p.