Модель узла компьютерной сети как объекта компьютерной разведки учитывающая динамику использования арендуемых информационных потоков

М.М. Добрышин, П.В. Закалкин, С.И. Жук

Академия ФСО России, город Орел

Аннотация: Представлена модель потоковой и сетевой компьютерных разведок, позволяющая оценить способность злоумышленника идентифицировать искомый узел компьютерной сети. На основании аппроксимации результатов имитационного моделирования получена зависимость вероятности идентификации узла от ряда параметров узла связи, фрагмента единой сети электросвязи и параметров средств ведения компьютерной разведки.
Ключевые слова: потоковая и сетевая компьютерные модели, имитационная модель, узел компьютерной сети.

Перевод практически всех сфер деятельности в информационное пространство позволил на базе арендуемых у провайдеров транспортных сетей связи развертывать и использовать различные частные компьютерные сети. Существующие законы рынка требуют перемещения части персонала предприятия как внутри страны, так и за ее пределами, что требует и динамического изменения сетей связи. Данные публикуемые организациями в сфере информационной безопасности показывают, что одними из основных угроз информационной безопасности являются различные виды компьютерных разведок (далее КР). Средства защиты информационной безопасности, установленные на средствах связи абонентов, находящихся вне контролируемой зоны (мобильные узлы компьютерной сети (далее МУзКС) менее эффективны, чем аналогичные средства стационарных узлов [1,2]. Проводя компьютерные атаки на МУзКС, злоумышленник способен получать искомую информацию при меньших затратах.

Анализируя тактику действий злоумышленников, можно сделать вывод о том, что проведению компьютерных атак предшествует проведение разведки направленной на идентификацию атакуемого узла компьютерной сети, определению его основных характеристик и выявлению уязвимостей

[2-4, 9]. Исходя из данной стратегии, злоумышленник должен на основании множества информационных потоков найти искомый, далее определить электронный адрес, после чего осуществить сканирование сетевого оборудования данного узла, с целью определения параметров атакуемого узла [1, 5, 10].

В связи с этим определение способности злоумышленника эффективно провести КР позволяет определить степень защищенности узла связи и определить требуемую стратегию защиты.

Для решения данной задачи разработана модель, позволяющая определить вероятность идентификации узла связи средствами потоковой и сетевой КР имеющихся у злоумышленника.

Сущность моделирования заключается в передачи информации между узлами компьютерной сети, с учетом переключения информационных потоков между несколькими арендуемыми информационными потоками; имитации переключения между информационными потоками и наблюдении демаскирующих признаков средствами потоковой КР с целью идентификации информационного потока; имитации сканирования сетевого оборудования и выявлении заданных уязвимостей средствами сетевой КР.

Постановка задачи на исследование. Целью моделирования является получение зависимости вероятности идентификации (вскрытия) МУзКС средствами потоковой и сетевой КР от количества информационных потокам, по которым передается информация, длительности использования каждого из каналов связи, времени выявления демаскирующих признаков, а также времени сканирования сетевого оборудования узла связи.

Выходным результатом являются зависимость вероятности идентификации МУзКС ($P_{\text{идент}}(t_{\text{ф}}) = f(R_{\text{есэ}}; t_{\text{ф}i}; R_{\text{ПиС КР}})$ от параметров сегмента RuNet ($R_{\text{есэ}}$), времени использования $i-$го канала связи ($t_{\text{ф}i}$), а также характеристик средств потоковой и сетевой КР ($R_{\text{ПиС КР}}$).

Основными исходными данными модели являются: время функционирования МУзКС ($t_{ф}$); время использования $i-$го канала связи ($t_{ф\,i}$) МУзКС ($t_{ф}$); количество независимых каналов связи в сегменте RuNet ($N_{кан}$); количество используемых независимых каналов связи в сегменте RuNet ($N^{*}_{кан}$); количество средств потоковой КР используемых злоумышленником; среднее время анализа информационного потока средствами потоковой КР $i-$го канала связи ($t_{ПКР\,i}$); объем информации передаваемый по $i-$го канала связи (V_i) за время наблюдения злоумышленником $i-$го канала связи; быстродействие средств потоковой КР ($b_j^{пкр}$); количество параметров анализируемых средством сетевой КР ($N_{Уз}$); быстродействие средств сетевой КР ($b_j^{скр}$).

Основными допущениями считается, что в районе функционирования защищаемого узла функционируют сторонние узлы; ресурс сил и средств потоковой КР конечен и требует конечного времени; злоумышленнику не известен электронный адрес атакуемого узла. К основным ограничениям относится время идентификации узла компьютерной сети другими видами разведки многим больше чем аналогичное время средствами сетевой и потоковой КР. Сущность разработанной модели заключается в поэтапной имитации поиска, наблюдения и идентификации узла компьютерной сети средствами потоковой и сетевой КР [5].

Первый этап моделирования (рис. 1) заключается в имитации отправки узлом компьютерной сети (блок 1.1) пакетов по одному из каналов связи. Одновременно осуществляется имитация ведения потоковой КР (отправка пакетов по одному из каналов связи) (блок 1.2). Время имитации отправки узлом пакетов и имитации работы потоковой КР задается. Переключение между каналами связи осуществляют коммутаторы (блоки 2.1, 2.2) на основании случайного выбора с равномерным распределением.

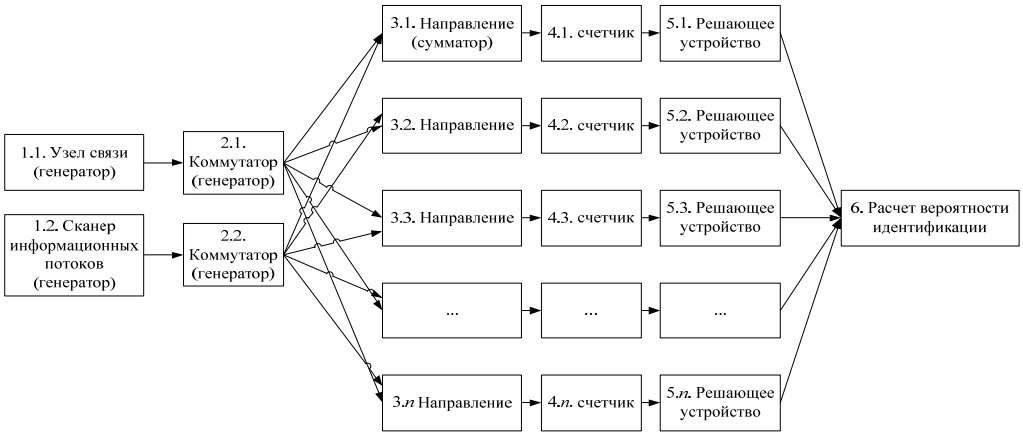

Рис. 1. Схема имитационной модели узла компьютерной сети как объекта потоковой КР

В блоках 3.1-3.*n* при одновременном поступлении пакетов от узла компьютерной сети и средства потоковой КР на выходе формируется логическая «1», если на один из входов не поступает сообщение, то присваивается логический «0». На рис. 2 показано визуальное представление имитируемого процесса. Исходные данные $t_{\text{ф}\,i} = 10$ (тактов), $t_{\text{пкр}\,i} = 5$.

В блоках 4.1-4.*n* подсчитываются поступившие «1», если на вход поступил логический «0», то счетчик обнуляется.

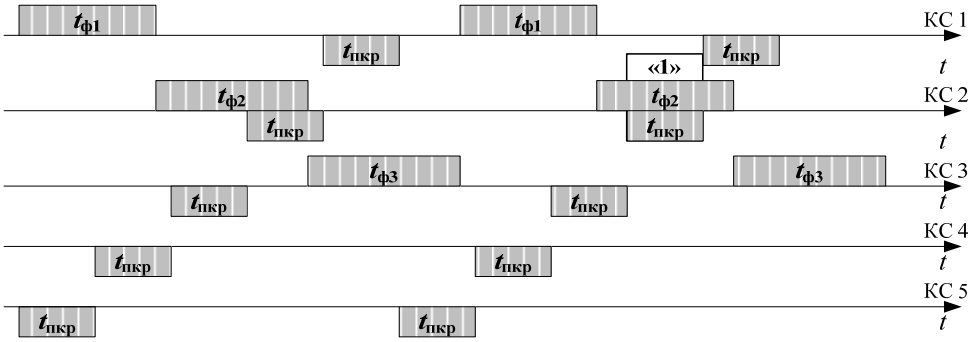

Рис. 2. Визуальное представление имитации процесса идентификации информационного потока защищаемого узла средствами потоковой КР

В блоках 5.1-5.n осуществляется принятие решения об идентификации информационного потока защищаемого узла. Если количество логических

единиц соответствует заданному значению, то считается, что информационный поток идентифицирован. На рис. 3 показаны вероятности идентификации узла средствами потоковой разведки от времени функционирования, при использовании одного информационного потока и различном времени использования данного узла.

В блоке 6 рассчитывается вероятность идентификации информационного потока защищаемого узла.

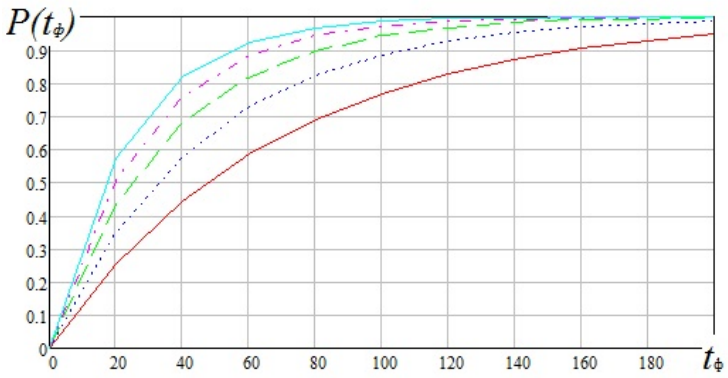

Рис. 3. Зависимость вероятности идентификации МУС средствами потоковой и сетевой КР при различных длительностях использования канала связи

Далее осуществляется имитация процессов сканирования сетевого оборудования и определяется вероятность выявления уязвимости узла в течение заданного времени. На рис. 4 показана зависимость вероятности идентификации МУС средствами потоковой и сетевой КР при переключении информационных потоков между пятью каналами связи.

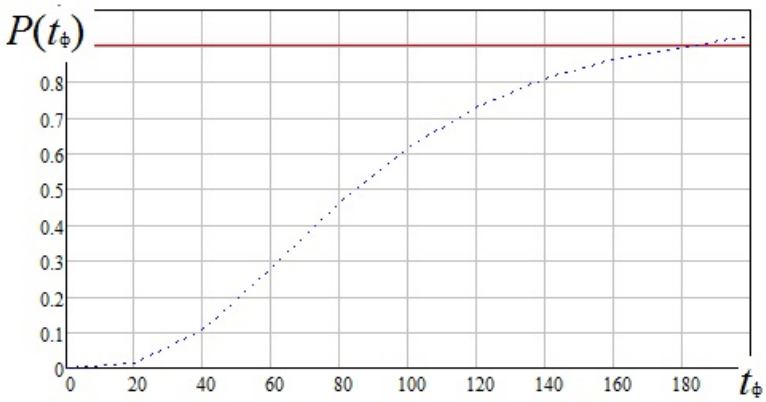

Рис. 4. Зависимость вероятности идентификации МУС средствами потоковой и сетевой КР при переключении информационных потоков между несколькими каналами связи

Из анализа полученных результатов (рис. 3, 4), очевидно, что использование нескольких каналов связи существенно увеличивает время идентификации защищаемого узла.

Аппроксимация результатов имитационного моделирования, выявлена зависимость вероятности идентификации ($P_{\text{идент}\,i}(t_{\text{ф}})$) МУС средствами потоковой и сетевой КР от параметров указанных в цели разработки модели:

$$P_{\text{идент}\,i}(t_{\text{ф}}) = 1 - e^{-\frac{K_1 \cdot K_2 \cdot t_{\text{ф}\,i}}{\overline{T}_{\text{идент}}}}, \quad (1)$$

$$K_1 = \frac{N_i^* \cdot N_{\text{пкр}}}{N_{\text{кан}}}, \quad (2)$$

$$K_2 = \frac{t_{\text{ф}}^2 - (t_{\text{ф}} - t_{\text{ф}\,i})(t_{\text{ф}} - t_{\text{идент}})}{t_{\text{ф}}^2}, \quad (3)$$

$$\overline{T}_{\text{идент}} = \frac{V_{ИП}}{B_{\text{пкр}\,j}} + \frac{N_{\text{парам}}}{B_{\text{скр}\,j}} + t_{\text{идент}}, \quad (4)$$

$$P_{\text{идент}} = \prod_i^g P_{\text{идент}\,i}. \quad (5)$$

Полученная аналитическая модель оформлена в виде программы для ЭВМ зарегистрированной в Роспатенте [6]. Внешний вид программы представлен на рис. 5.

Научная новизна разработанной модели заключается в учете динамики переключения информационных потоков между несколькими каналами связи, а также ряд параметров средств сетевой и потоковой КР. Разработанная модель предназначена для научно-исследовательских организаций с целью обоснования и разработки руководящих документов, регламентирующих порядок планирования, развертывания и функционирования МУС

интегрированных с ЕСЭ РФ в условиях ведения злоумышленником потоковой и сетевой КР.

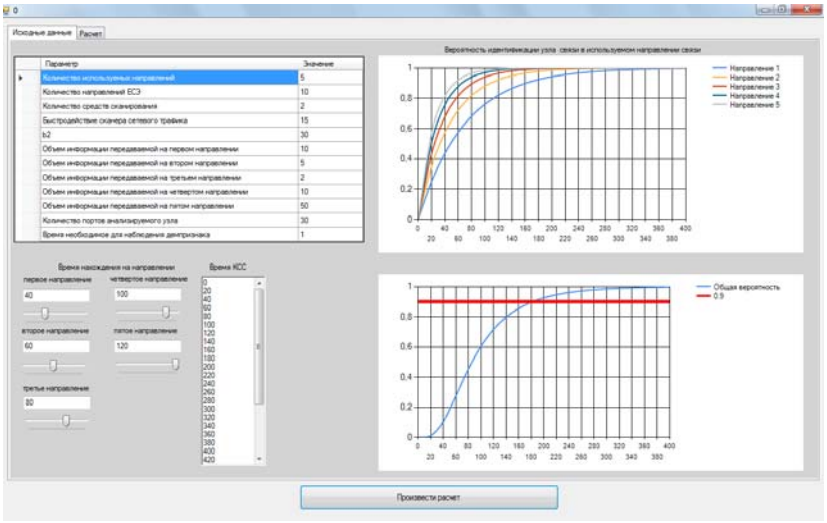

Рис. 5. Внешний вид программы для ЭВМ по расчету вероятности идентификации мобильных узлов связи средствами потоковой и сетевой КР

Оценка результатов разработанной модели и аналогов показывают выигрыш в 12-15 % достоверности результатов оценки способности злоумышленника идентифицировать узел связи.

Литература

1. Макаренко С. И. Системы управления, связи и безопасности. 2016. № 3. С. 292-376.

2. Кибербезопасность 2018-2019, Positive technologies 2018. 14 с.

3. Актуальные киберугрозы. II квартал 2018 года, Positive technologies, 2018. 23 с.

4. Хазов Владимир. Этапы проведения кибератак. URL: vasexperts.ru/blog/etapy-provedeniya-kiberatak.

5. Добрышин М.М., Реформат А.Н., Закалкин П.В. Комплексный алгоритм мониторинга защищенности узлов VPN от компьютерной разведки и DDoS-атак / Научный журнал : Электросвязь № 7 – 2018. С. 44-50.

6. Добрышин М.М., Закалкин П.В., Жук С.И. и др. Программа расчета способности сетевой и потоковой компьютерных разведок идентифицировать узел связи учитывающая динамику использования арендуемых информационных потоков. Свидетельство о государственной регистрации программы для ЭВМ № 2019615627 06.05.2019 г. Бюл. № 5.

7. Маро Е.А. Алгебраический анализ стойкости криптографических систем защиты информации // Инженерный вестник Дона, 2013, №4 URL: ivdon.ru/ru/magazine/archive/n4y2013/1996/.

8. Панкратов С.А. Использование графической информации для защиты программного и информационного обеспечения // Инженерный вестник Дона, 2012, №2 URL: ivdon.ru/ru/magazine/archive/n2y2012/792/.

9. Roigas H., Jakschis R., Lindstrom L., Minárik T. 9th International Conference on Cyber Conflict: Defending the Core – 2017. pp. 7-23, 43-59.

10. Minarik T., Jakschis R., Lindstrom L.10 th InternatIonal ConferenCe on Cyber ConflICtCyCon X: MaXIMISInG effeCtS – 2018. pp. 321-344, 409-425.

References

1. Makarenko S. I. Sistemy upravleniya, svyazi i bezopasnosti. 2016. № 3. pp. 292-376.

2. Kiberbezopasnost' [Cybersecurity] 2018-2019, Positive technologies 2018. 14 p.

3. Aktual'nye kiberugrozy [Current cyberthreats]. II kvartal 2018 goda. Positive technologies, 2018. 23 p.

4. Khazov Vladimir. Etapy provedeniya kiberatak [Stages of carrying out cyber attacks]. URL://vasexperts.ru/blog/etapy-provedeniya-kiberatak.

5. Dobryshin M.M., Reformat A.N., Zakalkin P.V. Nauchnyy zhurnal : Elektrosvyaz' № 7,2018. pp. 44-50.

6. Dobryshin M.M., Zakalkin P.V., Zhuk S.I. i dr. Programma rascheta sposobnosti setevoy i potokovoy komp'yuternykh razvedok identifitsirovat' uzel svyazi uchityvayushchaya dinamiku ispol'zovaniya arenduemykh informatsionnykh potokov kiberatak [The program of calculation of ability of network and stream computer investigations to identify hub site considering dynamics of use of the rented information flows]. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2019615627 06.05.2019 g. Byul. № 5.

7. Maro E.A. Inženernyj vestnik Dona (Rus), 2013, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2013/1996.

8. Pankratov S.A. Inženernyj vestnik Dona (Rus)), 2012, № 2. URL: ivdon.ru/ru/magazine/archive/n2y2012/792.

9. Roigas H., Jakschis R., Lindstrom L., Minárik T. 9th International Conference on Cyber Conflict: Defending the Core, 2017. pp. 7-23, 43-59.

10. Minarik T., Jakschis R., Lindstrom L. 10 th InternatIonal ConferenCe on Cyber ConflICtCyCon X: MaXIMISInG effeCtS, 2018. pp. 321-344, 409-425.