УДК 004.056.53 DOI: 10.26102/2310-6018/2020.31.4.037

Оценка возможного ущерба и времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности сети связи специального назначения

О.И. Бокова[1], С.В. Канавин[2], Н.С. Хохлов[3]
[1]ООО «Каскад», Москва, Российская Федерация,
[2,3]Воронежский институт МВД России, Воронеж, Российская Федерация

Резюме: В целях определения оптимального алгоритма и методики оценки ущерба в случае реализации угроз информационной безопасности в сетях связи специального назначения рассмотрены и проанализированы существующие подходы к решению данной задачи. Качество распознавания угроз адаптивной системой распознавания можно оценить в виде предотвращенного ущерба при реализации конфликтного воздействия на систему связи. Для этого целесообразно использовать типовую модель реализации угроз конфликтного воздействия на сеть связи, основанную на четырехэтапной стратегии конфликтного взаимодействия. С помощью выражения полученного в работе можно оценить качество распознавания угроз адаптивной системой распознавания в виде предотвращенного ущерба при реализации конфликтного воздействия на сеть связи. Проведена оценка времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности сети связи специального назначения в условиях реализации централизованного и децентрализованного управления. Полученное семейство зависимостей, для конкретных сетей и заданных технических средств, позволяет оценить временные параметры предложенных адаптивных алгоритмов маршрутизации, либо по заданным требованиям к оперативности управления сформировать требования к производительности технических средств системы управления. Из приведенных зависимостей следует, что для рассмотренных вычислительных процедур алгоритмов маршрутизации децентрализованный способ управления для большинства типов структур предпочтительнее по критерию время реакции независимо от производительности технических средств. Однако существуют такие структурные характеристики сетей, для которых преимущество того или другого алгоритма маршрутизации зависит от соотношения производительности технических средств системы управления.

Ключевые слова: противодействие угрозам информационной безопасности, сети связи специального назначения, комплексный подход, угрозы безопасности информации, оценка ущерба.

Для цитирования: Бокова О.И., Канавин С.В., Хохлов Н.С. Оценка возможного ущерба и времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности сети связи специального назначения. *Моделирование, оптимизация и информационные технологии.* 2020;8(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=887 DOI: 10.26102/2310-6018/2020.31.4.037.

Assessment of possible damage and reaction time of a complex of countermeasures to the implementation of information security threats special purpose communication networks

O.I. Bokova[1], S.V. Kanavin[2], N.S. Khokhlov[3]
[1]OOO «Cascade», Moscow, Russian Federation,
[2,3]Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russian Federation

Abstract: In order to determine the optimal algorithm and methods for assessing damage in the event of the implementation of information security threats in special-purpose communication networks, the existing approaches to solving this problem are considered and analyzed. The quality of threat recognition by the adaptive recognition system can be assessed in the form of prevented damage during the implementation of a conflict impact on the communication system. For this, it is advisable to use a standard model for the implementation of threats of conflict impact on the communication network, based on a four-stage strategy of conflict interaction. Using the expression obtained in the work, it is possible to assess the quality of threat recognition by the adaptive recognition system in the form of prevented damage during the implementation of the conflict impact on the communication network. An assessment of the reaction time of a complex of countermeasures to the implementation of threats to information security of a special-purpose communication network in the context of the implementation of centralized and decentralized control has been carried out. The resulting family of dependencies, for specific networks and given technical means, makes it possible to estimate the time parameters of the proposed adaptive routing algorithms, or, according to the specified requirements for control efficiency, form requirements for the performance of technical means of the control system. From the given dependencies it follows that for the considered computational procedures of routing algorithms, the decentralized control method for most types of structures is preferable according to the criterion response time, regardless of the performance of technical means. However, there are such structural characteristics of networks for which the advantage of one or another routing algorithm depends on the ratio of the performance of the technical means of the control system.

Keywords: countering information security threats, special purpose communication networks, an integrated approach, information security threats, damage assessment.

For citation: Bokova O.I., Kanavin S.V., Khokhlov N.S. Assessment of possible damage and reaction time of a complex of countermeasures to the implementation of information security threats special purpose communication networks. *Modeling, optimization and information technology.* 2020;8(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=887 DOI: 10.26102/2310-6018/2020.31.4.037 (In Russ).

Введение

В настоящее время активно обсуждается необходимость придания системам защиты информации качеств, присущих биосистемам, таких как возможность развития и адаптивность при внешних воздействиях. Становится актуальной проблема эволюционного развития систем информационной безопасности, в том числе в условиях конфликтных воздействий различного типа. Функциональная схема комплекса информационного обеспечения, для оценки ущерба наносимого компьютерными атаками, представлена, например, в работе [1]. Авторами Язовым Ю.К., Григорьевой Т.В., Нестеровским И.П. в статьях [2, 3] рассматривается один из вопросов развития методологии количественной оценки эффективности защиты информации – построение шкал комплексной оценки рисков нарушений безопасности информации на основе парадигмы предельного ущерба, приведены особенности финансового, морального, социального и экологического ущерба. В работе [4] рассмотрены модели угроз безопасности информационных систем и способы их реализации. Приведена методология и методический аппарат оценки ущерба от воздействия угроз информационной безопасности. По виду нарушения безопасности информации можно выделить следующие виды ущерба на типовых объектах информатизации: ущерб от нарушения конфиденциальности информации; ущерб от нарушения целостности информации; ущерб от нарушения доступности информации.

Каждый из видов ущерба является итоговым результатом оценки угроз и рисков информационной безопасности в информационно-технических системах. Результаты анализа и содержания подходов к оценке ущерба используемых на практике методик OCTAVE, ISRAM, Risk Watch и других, представлены в Таблице 1.

Таблица 1 – Результаты анализа методик по содержанию подходов к оценке ущерба
Table 1 – Results of the analysis of methods for the content of approaches to damage assessment

Наименование методики	Содержание подхода к оценке ущерба
OCTAVE	Величина потенциального ущерба является итоговой оценкой рисков ИБ. Вычисляется на основе экспертной оценки ценности активов и вероятности реализации угроз ИБ информационно-технических систем.
ISRAM	Величина потенциального ущерба используется для получения итоговой оценки рисков ИБ, определяется экспертным путём на основе табличных значений.
Risk Watch	Размер потенциального ущерба определяется как ожидаемые среднегодовые потери и является итоговой оценкой рисков ИБ. Вычисляется на основе экспертной оценки ценности активов и вероятности реализации угроз ИБ информационно-технических систем.
Методика оценки рисков ИБ Банка России	Потенциальный ущерб определяется экспертным путём на основе вербальной шкалы, шкала имеет четыре градации.

Как правило, оценка потенциального ущерба проводится экспертным путем, согласно заранее определенным критериям, или рассчитывается как возможные среднегодовые потери за год. Далее в работе рассмотрено определение оптимального алгоритма и методики оценки ущерба в случае реализации угроз информационной безопасности (ИБ) применительно к сетям связи специального назначения (СССН) которые на сегодня разработаны не в полной мере.

Оценка возможного ущерба от конфликтного воздействия на сеть связи специального назначения

Под понятием адаптивности или адаптации можно понимать способность системы защиты информации приспосабливаться к изменяющимся внешним и внутренним условиям, возникающим при функционировании информационно-технической системы в условиях противодействия. В статье под конфликтным воздействием будем понимать реализацию угроз информационной безопасности на инфраструктуру сети связи специального назначения.

В соответствии со статьей Федерального закона № 126 «О связи» дается следующее определение сетей связи специального назначения. Сети связи специального назначения предназначены для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка. Реализация оценки возможного ущерба от конфликтного воздействия на сеть связи специального назначения открывает новые возможности в области создания адаптивных систем распознавания ущерба.

Качество распознавания угроз адаптивной системой распознавания можно оценить в виде предотвращенного ущерба при реализации конфликтного воздействия на СССН. Для этого целесообразно использовать типовую модель реализации угроз конфликтного воздействия на СССН [4, 7], основанную на четырехэтапной стратегии конфликтного взаимодействия.

Общий ущерб, который может быть нанесен СССН в случае неправильного распознавания угроз конфликтного воздействия и, как следствие, не предотвращения их, выражается суммой ущербов в каждом элементе:

$$C_{СССН}^{ущерб}(t)=\sum_{k=1}^{l}C_k^{ущерб}(t). \quad (1)$$

Ущерб, который может быть нанесен k - ому элементу СССН в случае неправильного распознавания угроз конфликтного воздействия и, как следствие, не предотвращения его, выражается суммой ущербов на каждом из этапов стратегии конфликтного взаимодействия:

$$C_k^{ущерб}(t)=C_k^{дост}(t)+C_k^{м.\,защ}(t)+C_k^{проц}(t)+C_k^{манип}(t), \quad (2)$$

где $C_k^{дост}(t)$ – ущерб от реализации угроз конфликтного воздействия на этапе исследования механизма доступа к k - му элементу СССН в момент времени t;

$C_k^{м.\,защ}(t)$ – ущерб от реализации угроз конфликтного воздействия на этапе исследования механизмов защиты информации в k - ом элементе СССН в момент времени t;

$C_k^{проц}(t)$ – ущерб от реализации угроз конфликтного воздействия на этапе исследования информационных процессов в k - ом элементе СССН в момент времени t;

$C_k^{манип}(t)$ – ущерб от реализации угроз конфликтного воздействия на этапе несанкционированного манипулирования информацией в k - ом элементе СССН в момент времени t.

На каждом из этапов реализации стратегии конфликтного взаимодействия ущерб от реализации угроз конфликтного воздействия равен сумме ущербов по каждой угрозе:

$$C_k^{дост}(t)=\sum_{i=1}^{n}C_{ik}^{дост}(t), \quad (3)$$

$$C_k^{м.\,защ}(t)=\sum_{i=1}^{n}C_{ik}^{м.\,защ}(t), \quad (4)$$

$$C_k^{проц}(t)=\sum_{i=1}^{n}C_{ik}^{проц}(t), \quad (5)$$

$$C_k^{манип}(t)=\sum_{i=1}^{n}C_{ik}^{манип}(t). \quad (6)$$

Далее, составляющие выражений (3) – (6), ввиду их подобия, будем рассматривать на примере определения ущерба от реализации угроз конфликтного воздействия на этапе исследования механизма доступа. Тогда, ущерб по i – ой угрозе может быть выражен в виде:

$$C_{ik}^{дост}(t)=C_{ik}^{инф\,дост}(t)\cdot\mu_{ik}(t)\cdot P_{ik}^{незащ}, \quad (7)$$

где $C_{ik}^{инф\,дост}(t)$ – информационная ценность k -го элемента СССН по i - ой угрозе в момент времени t на этапе исследования механизма доступа;

$\mu_{ik}(t)$ – показатель эффективности реализации i - ой угрозы в k - ом элементе СССН в момент времени t;

$P_{ik}^{незащ}$ – вероятность незащищенности от i - ой угрозы k - ого элемента СССН.

Вероятность незащищенности от i - ой угрозы k - ого элемента СССН можно записать как:

$$P_{ik}^{незащ}=1-P_{ik}^{защ}. \quad (8)$$

Вероятность защищенности от i-ой угрозы k-ого элемента СССН определяется выражением:

$$P_{ik}^{защ} = P_{ik}^{пред} \cdot P_{ik}^{обн} \cdot P_{ik}^{расп} \cdot P_{ik}^{нейтр}, \quad (9)$$

где $P_{ik}^{пред} = \max_i P_{ijk}^{пред}$ – вероятность предотвращения i- ой угрозы конфликтного воздействия в k- ом элементе СССН;

$P_{ijk}^{пред}$ – вероятность предотвращения i- ой угрозы конфликтного воздействия j-ым средством в k- ом элементе СССН;

$P_{ik}^{обн} = \max_i P_{ijk}^{обн}$ – вероятность обнаружения i- ой угрозы конфликтного воздействия в k- ом элементе СУС;

$P_{ijk}^{обн}$ – вероятность обнаружения i-ой угрозы конфликтного воздействия j- ым средством в k- ом элементе СССН;

$P_{ik}^{расп} = \max_i P_{ijk}^{расп}$ – вероятность распознавания i- ой угрозы конфликтного воздействия в k- ом элементе СССН;

$P_{ijk}^{расп}$ – вероятность распознавания i-ой угрозы конфликтного воздействия j-ым средством в k- ом элементе СССН;

$P_{ik}^{нейтр} = \max_i P_{ijk}^{нейтр}$ – вероятность нейтрализации i- ой угрозы конфликтного воздействия в k- ом элементе СССН;

$P_{ijk}^{нейтр}$ – вероятность нейтрализации i- ой угрозы конфликтного воздействия j-ым средством в k- ом элементе СССН.

После подстановки выражений (2) - (9) в (1) получаем:

$$\begin{aligned} C_{СССН}^{ущерб}(t) = \sum_{k=1}^{l}\Bigg(\sum_{i=1}^{n} C_{ik}^{инф\,дост}(t)\cdot \mu_{ik}(t)\cdot\Big(1-\max_i\Big(P_{ijk}^{пред}\cdot P_{ijk}^{обн}\cdot P_{ijk}^{расп}\cdot P_{ijk}^{нейтр}\Big)\Big)+ \\ + \sum_{i=1}^{n} C_{ik}^{инф\,м.\,защ}(t)\cdot \mu_{ik}(t)\cdot\Big(1-\max_i\Big(P_{ijk}^{пред}\cdot P_{ijk}^{обн}\cdot P_{ijk}^{расп}\cdot P_{ijk}^{нейтр}\Big)\Big)+ \\ + \sum_{i=1}^{n} C_{ik}^{инф\,проц}(t)\cdot \mu_{ik}(t)\cdot\Big(1-\max_i\Big(P_{ijk}^{пред}\cdot P_{ijk}^{обн}\cdot P_{ijk}^{расп}\cdot P_{ijk}^{нейтр}\Big)\Big)+ \\ + \sum_{i=1}^{n} C_{ik}^{инф\,манип}(t)\cdot \mu_{ik}(t)\cdot\Big(1-\max_i\Big(P_{ijk}^{пред}\cdot P_{ijk}^{обн}\cdot P_{ijk}^{расп}\cdot P_{ijk}^{нейтр}\Big)\Big)\Bigg). \end{aligned} \quad (10)$$

На каждом из этапов реализации стратегии конфликтного взаимодействия ущерб от реализации угроз конфликтного воздействия равен сумме ущербов по каждой угрозе. На примере определения ущерба от реализации угроз конфликтного воздействия на этапе исследования механизма доступа. Таким образом, с помощью выражения (10) можно оценить качество распознавания угроз адаптивной системой распознавания в виде предотвращенного ущерба при реализации конфликтного воздействия на СССН.

Оценка времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности сети связи специального назначения

С учетом того, что СССН предназначены для нужд обороны страны, безопасности государства и обеспечения правопорядка одним из важных характеристик таких сетей является возможность оперативного доведения информации. Поэтому помимо возможности реализации оценки возможного ущерба адаптивная система защиты информации должна быть дополнена возможностью оценки времени реакции комплекса средств противодействия. Для этого оценим время реакции T_p для различных способов формирования плана распределения информации сети связи в предположении, что время задержки управляющей информации в узле коммутации пренебрежимо мало и каналы служебной связи однотипны.

При централизованном способе управления, изменение информации о состоянии элементов сети приводит к необходимости перерасчета маршрутных матриц всех узлов коммутации в одном из центров управления сетью и передачи информации управления в узле коммутации. С учетом показателя T_p время реакции при централизованном способе управления на основе матричного метода определения кратчайших путей удовлетворяет такому условию:

$$T_{рц} \le t\left[7N_1 + 2(N+M) + (N_1 - M)(5N-3)\right] + 4t\left\{N^2 + 2M\left[3S_m(N-1) + 5N + 1\right]\right\} + \\ + (NS_m + 1)\left[1 + ent(\log_2 N)\right]/C \qquad (11)$$

где $N_1=N(N-1)/2$; N – количество узлов; M – количество ветвей связи; C – скорость передачи управляющей информации, бит/с; t – время выполнения средней арифметической операции вычислительными средствами центра управления сетью, $t=1/\gamma$, с.

Приведенная оценка $T_{рц}$ является оценкой сверху. При необходимости учета времени выполнения каждой операции можно воспользоваться результатами [8], в этом случае численные значения коэффициентов в выражении (11) могут измениться, но порядок трудоемкости вычислений остается прежним.

Первое и второе слагаемые в (11) определяют время принятия решений по маршрутизации $T_{марш}$, а последнее - время передачи информации управления $T_{пер}$. Эта оценка инвариантна к способу коммутации.

Особенность децентрализованного способа управления на основе метода рельефа заключается в том, что информация о состоянии узла коммутации и направлений связи по сети не передается, а на ее основе формируется информация управления в виде минимальных векторов, которая рассылается смежным узлам коммутации. Время реакции при таком способе управления удовлетворяет такому условию:

$$T_{рд} \le Nt\left[2(S_m - 1) + L + 1\right] + 2t\left[r(S_m + 2)(5N-1) + S_m(3N-2) + N\right] + \\ + 2r\left\{N\left[1 + ent(\log_2 r)\right] + \left[1 + ent(\log_2 N)\right]\right\}/C \qquad (12)$$

где L – число подверженных конфликтному воздействию (перегруженных) направлений связи. Первые слагаемые в (12) определяют время выполнения вычислительных операций, связанных с формированием нового минимального вектора, последнее – время передачи управляющей информации.

Выражение (12) получено в предположении, что обмен информацией инициируется одним из узлов коммутации при отказе (восстановлении) или перегрузке инцидентных ему направлений связи. Если время задержки информации управления в узле коммутации соизмеримо со временем передачи, то эта задержка должна быть учтена в выражениях (11) и (12), причем в (12) с сомножителем *2г.* При неоднородных каналах в выражениях должна быть использована минимальная из скоростей С. Рассмотрим

зависимости T_m, $T_{рд}$ от структурных характеристик сети при использовании современных вычислительных средств (у = 10^5 -е- 10^6 операций/с) и изменении С от 2,4 до 24 кбит/с. Для этого определяются структурные характеристики трех типов сетей:

– полносвязная – $M = N\{N-1\}/2$, $S_m = N-1$, $г = 1$;

– кольцевая – $M = N$, $S_m = 2$, $г = ent\ \{N/2\}$;

– однородная – $degi = S$ для N, $2<S<N-1$.

Известно, что не всякая комбинация N и S имеет отображение в однородный граф. Однако при $N=j\{S-1\}$, $j = 2, 3,...$, однородный граф реализуется и диаметр его определяется аналитически:

$$r = \begin{cases} \dfrac{N}{2(S-1)} + 1 & при \quad j\ четном, \\ \dfrac{1}{2}\left(\dfrac{N}{S-1} + 1\right) & при \quad j\ нечетном \end{cases} \tag{13}$$

На Рисунке 1. приведены зависимости $T_{рц}$ от производительности технических средств системы управления. Анализ подобных зависимостей $T_{рц}$ и $T_{рд}$ показал, что существуют два характерных участка при изменении С: участок, на котором $T_р$ определяется, в основном, временем передачи управляющей информации и изменение С существенно сказывается на изменении $T_{рц}$ и $T_{рд}$, и почти горизонтальный участок, на котором эти величины определяются временем принятия решений [8]. На основе полученных данных можно сделать вывод, что наиболее рациональной скоростью передачи управляющей информации при таких значениях $у$ является диапазон 4,8-14,4 кбит/с.

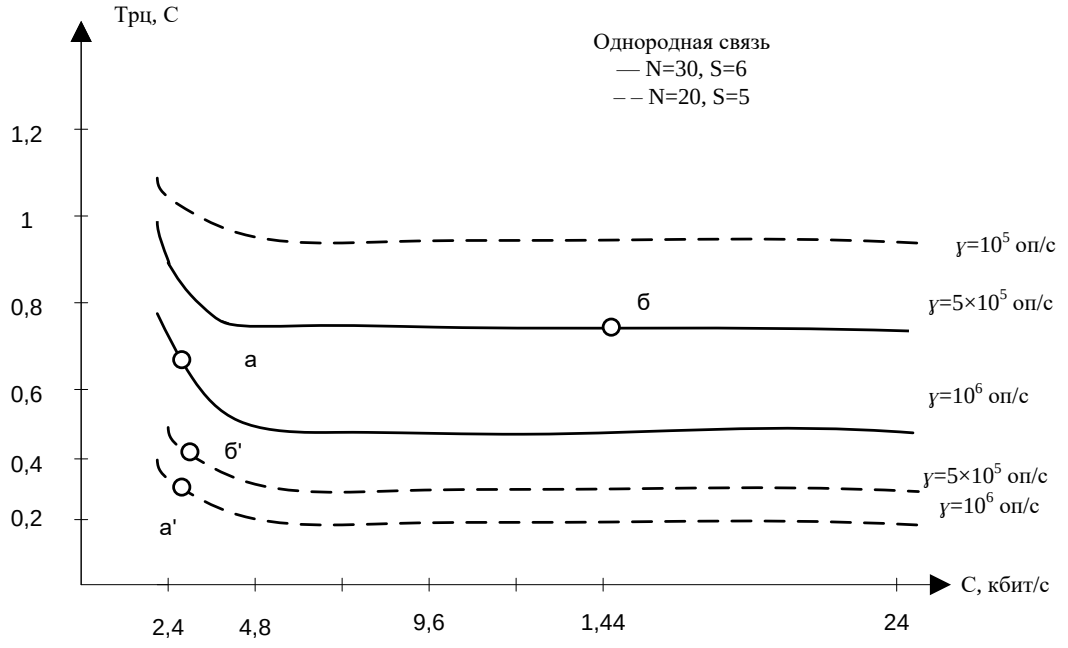

Рисунок 1 – Зависимости величины времени реакции $T_{рц}$ при централизованном способе управления в сети с различными структурными характеристиками и производительностью технических средств от скорости передачи управляющей информации С, кбит/с

Figure 1 – Dependences of the TRC response time for a centralized control method in a network with different structural characteristics and performance of technical means on the transmission rate of control information C, kbit / s

Семейство зависимостей, построенных для конкретных сетей и заданных технических средств, позволяет оценить временные параметры предложенных адаптивных алгоритмов маршрутизации, либо по заданным требованиям к оперативности управления сформировать требования к производительности технических средств системы управления. Кроме того, поскольку одно и то же время реакции может быть получено путем различных комбинаций технических средств (например, точки а, б, и а', б' Рисунок 1), появляется возможность выбора предпочтительного варианта системы управления с учетом стоимости технических средств.

Введем величину 0 = у/С - количество арифметических операций, выполняемых вычислительными средствами центра управления сетью за время передачи одного бита информации. На Рисунке 2 приведены зависимости отношения $T_{рц}/T_{рд}$ от 0 при различных N и *S*. Значения lg $(T_{рц}/T_{рд})>0$ определяют область преимущественного использования децентрализованного способа управления, а $g\{T_m/T_{pd})< 0$ – централизованного способа.

Из приведенных на Рисунке 2 зависимостей следует, что для рассмотренных вычислительных процедур алгоритмов маршрутизации децентрализованный способ управления для большинства типов структур предпочтительнее по критерию T_p независимо от производительности технических средств.

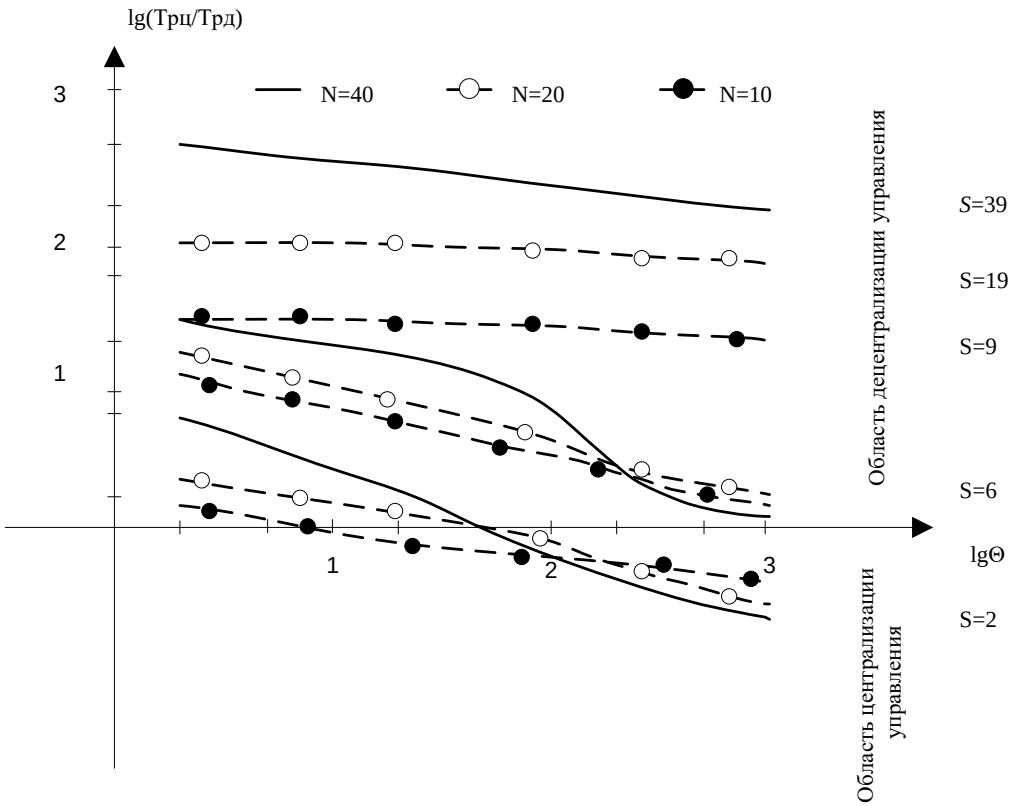

Рисунок 2 – Зависимости отношения времени реакции $T_{рц}/T_{рд}$ при централизованном и децентрализованном способах управления в сети с различными структурными характеристиками и производительностью технических средств от количества арифметических операций 0, выполняемых за время передачи одного бита информации

Figure 2 – Dependences of the ratio of the response time Trc / Trd for centralized and decentralized control methods in a network with different structural characteristics and performance of technical means on the number of arithmetic operations 0 performed during the transmission of one bit of information

Однако существуют такие структурные характеристики сетей 2<*S*<5 (Рисунках 2, 3), для которых преимущество того или другого алгоритма маршрутизации зависит от соотношения производительности технических средств системы управления.

На Рисунке 3. показана зависимость значения 0*, при котором $T_{рц} = T_{рд}$, от структурных параметров сети. Очевидно, что значение 0* при *S = 2* является оценкой снизу, т.е. для других значений *S* предпочтительность централизованного управления (если она существует) проявляется при большем значении у/С.

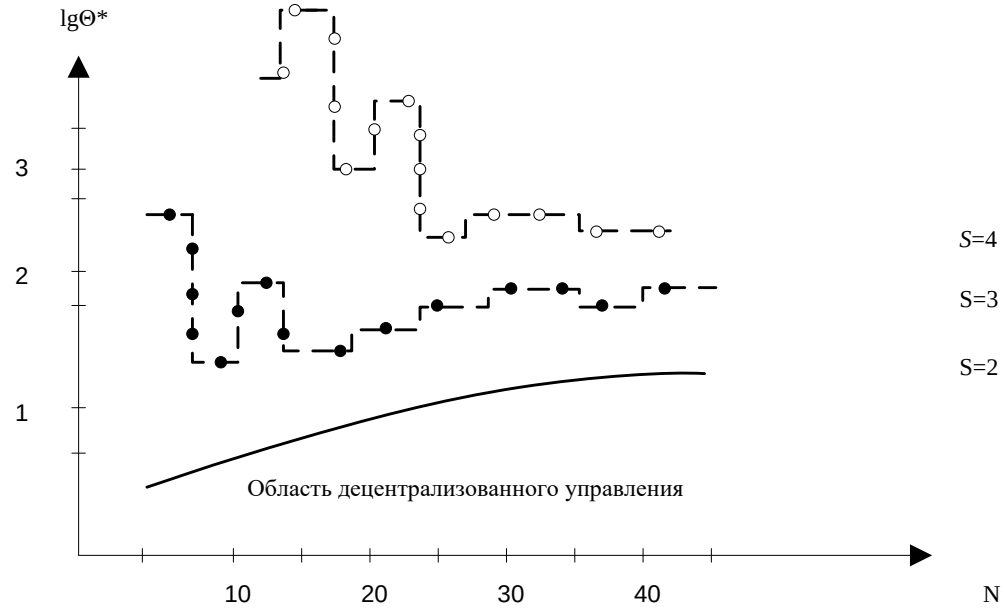

Рисунок 3 – Зависимости величины 0, характеризуемой равенством $T_{рц} = T_{рд}$, от структурных параметров сети S и *N*

Figure 3 – Dependence of the value 0, characterized by the equality $T_{rc} = T_{rd}$, on the structural parameters of the network S and N

При степени вершины *S>2* зависимость уже не является монотонной, изменение 0* происходит скачкообразно. Уменьшение значения 0* происходит при изменении (увеличении) *г* в соответствии с (3) при заданном *S.* Затем при возрастании *N* и том же *г* значение 0* увеличивается, так как объем информации управления при централизованном способе растет быстрее.

Заключение

Предложенный в настоящей статье подход к оценке возможного ущерба и времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности в сети связи специального назначения может быть использован при совершенствовании адаптивных систем защиты информации [8, 9]. В целях определения оптимального алгоритма и методики оценки ущерба в случае реализации угроз информационной безопасности в сетях связи специального назначения рассмотрены и проанализированы существующие подходы к решению данной задачи. Качество распознавания угроз адаптивной системой распознавания можно оценить в виде предотвращенного ущерба при реализации конфликтного воздействия на систему связи. Для этого целесообразно использовать типовую модель реализации угроз конфликтного воздействия на сеть связи, основанную на четырехэтапной стратегии конфликтного

взаимодействия. С помощью выражения полученного в работе можно оценить качество распознавания угроз адаптивной системой распознавания в виде предотвращенного ущерба при реализации конфликтного воздействия на сеть связи. Проведена оценка времени реакции комплекса средств противодействия на реализацию угроз информационной безопасности сети связи специального назначения в условиях реализации централизованного и децентрализованного управления. Полученное семейство зависимостей, для конкретных сетей и заданных технических средств, позволяет оценить временные параметры предложенных адаптивных алгоритмов маршрутизации, либо по заданным требованиям к оперативности управления сформировать требования к производительности технических средств системы управления [10, 11]. Из приведенных зависимостей следует, что для рассмотренных вычислительных процедур алгоритмов маршрутизации децентрализованный способ управления для большинства типов структур предпочтительнее по критерию время реакции независимо от производительности технических средств. Однако существуют такие структурные характеристики сетей, для которых преимущество того или другого алгоритма маршрутизации зависит от соотношения производительности технических средств системы управления.

ЛИТЕРАТУРА

1. Гречишников Е.В., Добрышин М.М., Гуцын Р.В. Комплекс информационного обеспечения оценки защищенности узлов связи от разнородных компьютерных атак. *I-methods*. 2019;11(4):4-9.
2. Нестеровский И.П., Язов Ю.К. Возможный подход к оценке ущерба от реализации угроз безопасности информации, обрабатываемой в государственных информационных системах. *Вопросы кибербезопасности*. 2015;2(10):20-25.
3. Язов Ю.К., Григорьева Т.В. Парадигма предельного ущерба и ее использование при оценке рисков нарушений безопасности информации в компьютерной системе. *Известия ЮФУ. Технические науки.* 2008;8(85):81-87.
4. Bokova O.I., Kanavin S.V., Meshcheryakov V.A., Khokhlov N.S. Information security system model in the automated system developed in the simulation software environment CPN TOOLS. *Journal of Physics: Conference Series. Applied Mathematics, Computational Science and Mechanics: Current Problems.* 2020:012021. DOI: 10.1088/1742-6596/1479/1/012021.
5. Khokhlov N., Kanavin S., Rybokitov A. Modeling information security infringements in mobile self-organizing network of communication using fuzzy logic and theory of graphs. Proceedings – 2019 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency, SUMMA 2019. 2019:60-63. DOI: 10.1109/SUMMA48161.2019.8947572.
6. Хохлов Н.С., Канавин С.В., Гилев И.В. Методика построения нейронной сети, решающей задачи выбора способов противодействия деструктивным электромагнитным воздействиям в сетях связи специального назначения. *Вестник Воронежского института МВД России*. 2020;2:164-174.
7. Хохлов Н.С., Канавин С.В., Гилев И.В. Типовые модели деструктивных широкополосных и сверхширокополосных сигналов, воздействующих на системы связи специального назначения. *Вестник Воронежского института МВД России.* 2019;1:91-101.
8. Хохлов Н.С., Панычев С.Н., Канавин С.В., Самоцвет Н.А., Гилев И.В. Методика количественной оценки влияния радиопомех и сигнала радиоэлектронных средств на

показатели радиоэлектронной защиты. Вестник поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. 2019;1(41):22-30. DOI:10.25686/2306-2819.2019.1.22.

9. Бокова О.И., Жайворонок Д.А., Канавин С.В., Хохлов Н.С. Модель комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. *Моделирование, оптимизация и информационные технологии.* 2020;2(29):41-42. Доступно по https://moit.vivt.ru/wp-content/uploads/2020/05/BokovaSoavtors_2_20_1.pdf. DOI: 10.26102/2310-6018/2020.29.2. 040 (дата обращения 23.12.2020).
10. Гилев И.В., Канавин С.В., Попов А.В., Хохлов Н.С. Способ противодействия деструктивным электромагнитным воздействиям, основанный на дополнительной модуляции с применением вейвлет-преобразования в сетях связи специального назначения. *Моделирование, оптимизация и информационные технологии.* 2020;2(29):12-13. Доступно по https://moit.vivt.ru/wp-content/uploads/2020/05/GilevSoavtors_2_20_1.pdf. DOI: 10.26102/2310-6018/2020.29. 2.039 (дата обращения 23.12.2020).
11. Хохлов Н.С., Канавин С.В., Гилев И.В. Экспериментальное исследование по воспроизведению деструктивных электромагнитных воздействий, приводящих к разрушению и модификации информации в системах связи специального назначения Вестник Воронежского института МВД России. 2020;4:25-38.

REFERENCES

1. Grechishnikov E.V., Dobryshin M.M., Gutsyn R.V. Complex of information support for assessing the security of communication nodes from heterogeneous computer attacks. *I-methods*. 2019;11(4):4-9. (In Russ)
2. Nesterovskiy I.P., Yazov Yu.K. Possible approach to assessing damage from the implementation of threats to the security of information processed in state information systems. *Voprosy kiberbezopasnosti*. 2015;2(10):20-25. (In Russ)
3. Yazov Yu.K., Grigorieva T.V. The marginal damage paradigm and its use in assessing the risks of information security breaches in a computer system. *Izvestiya YUFU. Technical science*. 2008;8(85):81-87. (In Russ)
4. Bokova O.I., Kanavin S.V., Meshcheryakov V.A., Khokhlov N.S. Information security system model in the automated system developed in the simulation software environment CPN TOOLS. *Journal of Physics: Conference Series. Applied Mathematics, Computational Science and Mechanics: Current Problems.* 2020: 012021. DOI:10.1088/1742-6596/ 1479/1/012021.
5. Khokhlov N., Kanavin S., Rybokitov A. Modeling information security infringements in mobile self organizing network of communication using fuzzy logic and theory of graphs. *Proceedings – 2019 1st International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency, SUMMA*. 2019.2019: 60-63. DOI: 10.1109/ SUMMA48161.2019.8947572.
6. Khokhlov N.S., Kanavin S.V., Gilev I.V. A technique for constructing a neural network that solves the problem of choosing ways to counteract destructive electromagnetic influences in special-purpose communication networks. *Vestnik Voronezhskogo instituta MVD Rossii*. 2020;2:164-174. (In Russ)

7. Khokhlov N.S., Kanavin S.V., Gilev I.V. Typical models of destructive broadband and ultra-wideband signals affecting special-purpose communication systems. Vestnik Voronezhskogo instituta MVD Rossii. 2019;1:91-101. (In Russ)
8. Khokhlov N.S., Panychev S.N., Kanavin S.V., Samotsvet N.A., Gilev I.V. Methodology for quantitative assessment of the influence of radio interference and the signal of radio electronic equipment on the indicators of electronic protection. Vestnik povolzhskogo gosudarstvennogo tekhnologicheskogo universiteta. Seriya: Radiotekhnicheskiye i infokommunikatsionnyye sistemy. 2019;1(41):22-30. DOI:10.25686/2306-2819.2019.1.22. (In Russ)
9. Bokova O.I., Zhaivoronok D.A., Kanavin S.V., Khokhlov N.S. Model of a complex of means to counter information security threats in special-purpose communication networks. *Modeling, optimization and information technology*. 2020;2(29):41-42. Available at https://moit.vivt.ru/wp-content/uploads/2020/05/BokovaSoavtors_2_20_1.pdf. DOI: 10.26102/2310-6018/2020.29.2.040 (accessed 23.12.2020).
10. Gilev I.V., Kanavin S.V., Popov A.V., Khokhlov N.S. A method of counteracting destructive electromagnetic influences based on additional modulation using wavelet transform in special-purpose communication networks. Modeling, optimization and information technology. 2020;2(29):12-13. Available at https://moit.vivt.ru/wp-content/uploads/2020/05/GilevSoavtors_2_20_1.pdf. DOI:10.26102/2310-6018/ 2020.29.2.039 (accessed 23.12.2020).
11. Khokhlov N.S., Kanavin S.V., Gilev I.V. An experimental study on the reproduction of destructive electromagnetic influences leading to the destruction and modification of information in special-purpose communication systems *Vestnik Voronezhskogo instituta MVD Rossii*. 2020;4:25-38. (In Russ).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Бокова Оксана Игоревна, доктор технических наук, профессор, научно-технический консультант, ООО «Каскад», Москва, Российская Федерациия.
e-mail: o.i.bokova@gmail.com

Oksana I. Bokova, Doctor of Technical Sciences, Professor, Scientific and Technical Consultant, OOO «Cascade», Moscow, Russian Federation.

Канавин Сергей Владимирович, кандидат технических наук, доцент кафедры инфокоммуникационных систем и технологий, Воронежский институт МВД России, Воронеж, Российская Федерация.
e-mail: sergejj-kanavin@rambler.ru

Sergey V. Kanavin, Candidate of Technical Sciences, Associate Professor of the Department of Infocommunication Systems and Technologies, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russian Federation.

Хохлов Николай Степанович, доктор технических наук, профессор, профессор кафедры инфокоммуникационных систем и технологий, Воронежский институт МВД России, Воронеж, Российская Федерация.
e-mail: nikolayhohlov@rambler.ru

Nikolay S. Khokhlov, Doctor of Technical Sciences, Professor, Professor of the Department of Information and Communication Systems and Technologies, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russian Federation.