УДК 004.056.53 DOI: 10.26102/2310-6018/2021.34.3.020

К вопросу выбора стратегии защиты системы связи специального назначения при угрозах информационной безопасности

С.В. Канавин

Воронежский институт МВД России, Воронеж, Российская Федерация

Резюме. Вызовы современных угроз информационной безопасности, оказывающих дестабилизирующее воздействие на системы связи специального назначения (СССН), требуют ответной реакции. При этом противодействие в СССН рассматривается как сложный, многоуровневый иерархический процесс, а информационный конфликт – как способ взаимодействия компонентов системы, результат которого заранее предопределить крайне сложно. В связи с этим возможны реализации различных стратегий защиты информационных систем, исходя из возможных вариантов действий. При анализе информационного конфликта в СССН рассмотрены модели конфликтов на основе теории управления, теории игр, вероятностно-временного подхода. На основе принципа прямого моделирования процесса конфликта предложена модель конфликтного взаимодействия «СССН – нарушитель». Предлагаемая модель конфликта «СССН – нарушитель» на понятийном уровне структурно представлена в виде системы с двумя контурами управления, имеющими общий объект воздействия – СССН и прямо противоположные цели функционирования, а динамика их взаимодействия представлена в виде схемы «воздействие – ответная реакция» с возможностью принятия решения на применение мер противодействия конфликтному воздействию как после факта воздействия, так и после установления факта активного сканирования уязвимостей. Стратегия противодействия в данном случае предполагает использование имеющегося ресурса по определенному алгоритму для ответной реакции системы на воздействие. Показано, что выбор стратегии противодействия, как и само конфликтное взаимодействие, зависит от условий функционирования и параметров СССН. В результате моделирования выявлено, что конфликтное взаимодействие на всем отрезке времени носит циклический характер, т. е. происходит преобладание конфликтного воздействия либо стратегии противодействия конфликтному воздействию на каждом шаге конфликтного взаимодействия сторон.

Ключевые слова: стратегии защиты, угрозы информационной безопасности, система связи специального назначения, информационный конфликт, конфликтное взаимодействие, управление системой защиты информации.

Для цитирования: Канавин С.В. К вопросу выбора стратегии защиты системы связи специального назначения при угрозах информационной безопасности. *Моделирование, оптимизация и информационные технологии.* 2021;9(3). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1033 DOI: 10.26102/2310-6018/2021.34.3.020

To the question of choosing a defense strategy communication systems for special purposes in case of information security threats

S.V. Kanavin

Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russian Federation

Abstract: The challenges of modern information security threats that have a destabilizing effect on special purpose communication systems (SSSN) require a response. At the same time, counteraction in

the SSSN is considered as a complex, multilevel hierarchical process, and the information conflict is considered as a way of interaction between the components of the system, the result of which is not predetermined in advance. As a result, it is possible to implement various strategies for protecting information systems based on possible options for action. When analyzing the information conflict in the SSSN, the models of conflicts based on control theory, game theory, and the probabilistic-temporal approach are considered. On the basis of the principle of direct modeling of the conflict process, a model of conflict interaction "CCCH-intruder" is proposed. The proposed model of the conflict "CCCH-intruder" at the conceptual level is structurally presented in the form of a system with two control loops, having a common object of influence CCCH and directly opposite goals of functioning, and the dynamics of their interaction is presented in the form of a scheme "impact-response" with the possibility of making a decision on the application of measures to counter conflict impact both after the fact of impact, and after establishing the fact of active scanning of vulnerabilities. The counteraction strategy in this case involves the use of the available resource, according to a certain algorithm, for the response of the system to the impact. It is shown that the choice of the countermeasures strategy, as well as the conflict interaction itself, depends on the operating conditions and parameters of the SCCH. As a result of modeling, it was shown that the conflict interaction over the entire time interval is cyclical, i.e. there is a predominance of the conflict impact or the strategy of counteraction to the conflict impact, at each step of the conflicting interaction of the parties.

Keywords: protection strategies, threats to information security, communication system of special purpose, information conflict, conflict interaction, management of the information security system.

For citation: Kanavin S.V. On the issue of choosing a strategy for protecting a special-purpose communication system in case of information security threats. *Modeling, Optimization and Information Technology*. 2021;9(3). Available from: https://moitvivt.ru/ru/journal/pdf?id=1033 DOI: 10.26102/2310-6018/2021.34.3.020 (In Russ).

Введение

В настоящее время сети и системы связи специального назначения получили большое распространение в органах государственной власти, органах, осуществляющих функции обороны страны, безопасности государства и обеспечения правопорядка [1]. В связи с особенностями функционирования инфокоммуникационных систем и сетей связи специального назначения необходимо учитывать, что они развернуты и обеспечивают управление и взаимодействие в рамках существующих ведомственных и межведомственных систем связи. В статье под системой связи специального назначения (ССCН) понимают специализированную защищенную инфокоммуникационную систему.

Стратегия применения средств противодействия угрозам информационной безопасности ССCН определяет структуру, приоритеты, методы принятия решений при организации и обеспечении соответствующего вида деятельности, направлена на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов. Обзор стратегий обеспечения информационной безопасности в информационных системах представляет собой систематизацию процесса выбора инструментов защиты информации на основе целесообразности и имеющихся возможностей [2]. Классификация стратегий защиты информации в компьютерных системах может основываться на наличии отличительных признаков, таких как: организация защиты информации; направленность действий; адаптивность; превентивность; активность [3]. В настоящее время для поддержания защищенности информационной системы могут применяться следующие подходы: на основе прогнозирования состояний информационной безопасности [4], теоретико-игрового подхода [5] и других. Проводятся научные исследования по применению

множества стратегий в масштабе объекта защиты информации с возможностью их оптимизации [6].

Выработка стратегии защиты информации может быть представлена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами. Состав и структура средств защиты информации в СССН существенно зависят от выбранной стратегии защиты. Классификация возможных стратегий защиты приведена на Рисунке 1.

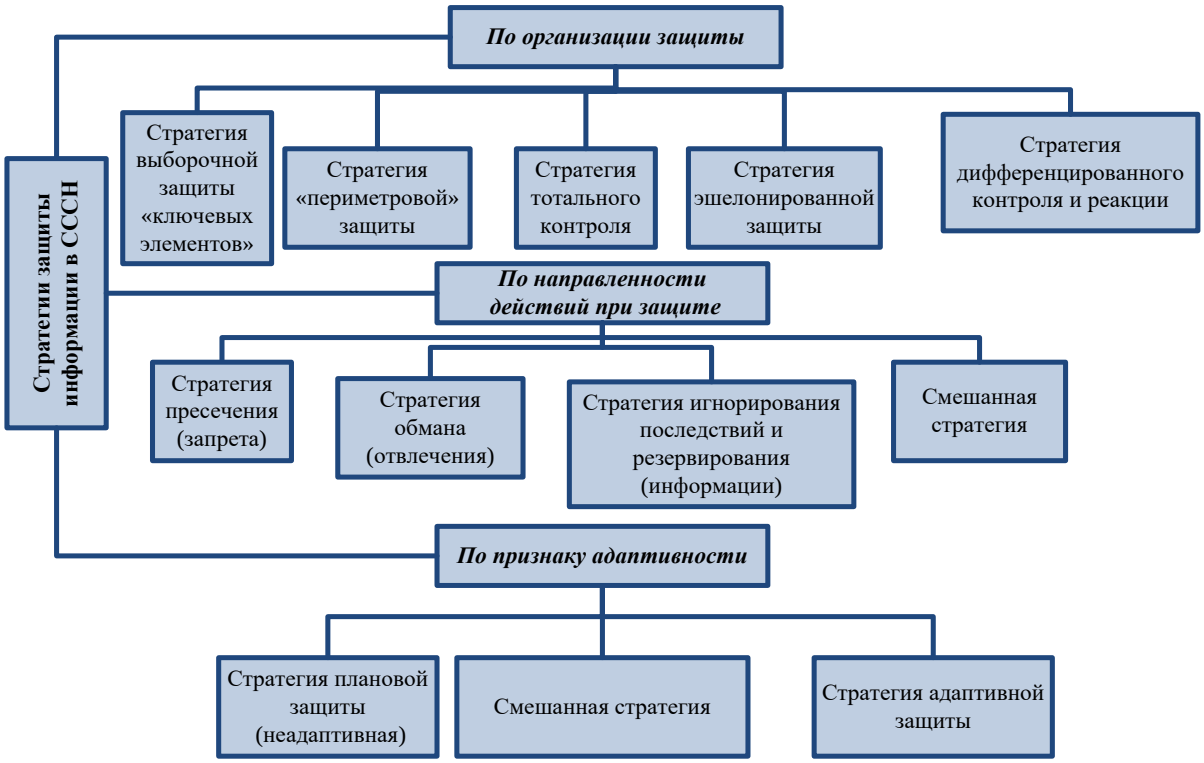

Рисунок 1 – Классификация стратегий защиты в СССН
Figure 1 – Classification of protection strategies in the SSSN

В аспекте функционирования средств защиты информации в СССН можно выделить три предельные стратегии, которые представлены в Таблице 1.

Таблица 1 – Стратегии защиты СССН
Table 1 – Strategies for protecting the SSSN

Учитываемые угрозы	Влияние на СССН		
	Отсутствует	Частичное	Полное
Наиболее опасные	Оборонительная стратегия		
Все идентифицированные угрозы		Наступательная стратегия	
Все потенциально возможные угрозы			Упреждающая стратегия

В настоящее время выбор стратегии защиты не выделяется в отдельную процедуру. Это связано с непроработанностью общей методологии защиты с использованием разных стратегий.

В зависимости от типа воздействия необходимо подобрать стратегию защиты. Стратегия защиты есть реакция системы на конфликтное воздействие с последующим принятием оптимального адекватного решения, принадлежащего множеству допустимых решений

$$R=\{r_i\},\ i=1,2,\ldots I.$$

Причем время реакции системы $\tau_{рс}$ не должно превышать время воздействия $\tau_{вз}$:

$$\tau_{рс} \leq \tau_{вз}.$$

Для организации контроля и управления схемой выявления и противодействия конфликтному воздействию на СССН следует создать систему управления (СУ). СУ может состоять из программно-аппаратного комплекса, содержащего базы данных о наиболее распространенных видах конфликтных воздействий, методиках их выявления, множестве стратегий противодействия и способах их применения с возможностью подключения к реально функционирующей СССН.

СССН, являясь основой информационного обмена оперативной информацией, наиболее подвержена влиянию со стороны криминальных образований, иностранных технических разведок и отдельных нарушителей. Данное влияние в совокупности образует конфликтное взаимодействие.

Описание информационного конфликта в СССН

Система связи специального назначения может включать в себя информационные системы, объединенные в единую структуру системы связи специального назначения (СССН), что увеличивает возможность нанесения преднамеренных воздействий со стороны преступных сообществ и отдельных злоумышленников.

Рассмотрим ряд определений понятия конфликт.

Конфликт – специфический процесс взаимодействия двух или большего количества компонентов системы (или систем в целом), преследующих разные интересы. Если интересы противодействующих систем (сторон) противоположны, то говорят об антагонистическом конфликте, а само взаимодействие сторон трансформируется в столкновение интересов [7].

Конфликт, согласно [8], рассматривается как способ взаимодействия компонентов системы, результат которого заранее не предопределен. От выбора стратегий взаимодействующих систем зависят пути развития конфликта.

В динамике конфликта различают четыре основных стадии:

– *возникновение конфликтной ситуации*, где формируются противоречия между системами в информационном пространстве;

– *латентная*, а именно ожидание активного противоборства с конкурирующей стороны;

– *активная* – непосредственно само конфликтное взаимодействие;

– *завершающая* – разрешение конфликта.

Основой исследования конфликта являются схемы и механизмы взаимодействия, взаимоуправления или манипулирования. Ключевым моментом при анализе конфликта является выбранные оппонентами стили управления.

В [9] приведена следующая классификация:

– *адаптивное управление* – опирается на существование адекватной математической модели процесса взаимодействия, оценивающей неизвестные параметры системы и определяющей закон противодействия;

– *рефлексивное управление* – подразумевает воздействие на выбор стратегии поведения. Различают *простое* и *сложное* рефлексивное управление. *Простое рефлексивное управление* – воздействие на процесс отображения оперативно-тактической обстановки. *Сложное рефлексивное управление* – воздействие на процесс принятия решений системой;

– *ситуационное управление* – анализ входных воздействий из конечного, определенного набора и принятие управляющих решений на основе заранее отработанных сценариев поведений системы.

Таким образом, применение теории управления является одним из вариантов описания конфликтного взаимодействия СССН и нарушителя. Теоретические аспекты управления динамических систем приведены в [8]. Особенностью данного подхода является рассмотрение не одной системы как объекта управления, а взаимодействия противодействующих между собой компонентов систем («СССН – нарушитель»), каждая из которых осуществляет манипулирование компонентами противостоящей стороны.

С точки зрения теории игр при рассмотрении процесса взаимодействия СССН динамика конфликта описывается графом переходов между состояниями во времени [10]. Особенность представления графа заключается в прогнозировании ответной реакции противоборствующей стороны на дестабилизирующие воздействия. Анализ конфликта заключается в решении или определении оптимальной стратегии воздействия. Для этого вводится матрица потерь, которая характеризует выигрыш или проигрыш каждой из стратегий сторон. Для трудно формализуемых систем, меняющих стили принятия решений на основе анализа предыдущих состояний и предсказания динамики конфликта, а СССН представляет собой именно такой класс, построение таких матриц себя не оправдывает.

Другим методом описания динамики конфликта является вероятностно-временной подход [11], математический аппарат которого основывается на теории марковских и полумарковских процессов. При этом модель динамики конфликта строится исходя из доминирующей стратегии воздействия. Первоначально задают граф основных и вспомогательных состояний. Вводится среднее количество переходов в состояние и вероятность пребывания. Данные характеристики определяются на основе статистических характеристик переходов, известных для каждой из противодействующих сторон в отдельности. Для этого вводится операция конфликтного взаимодействия, в соответствии с которой определяются плотности вероятности «упреждения» – достижения цели компонентами одной из сторон раньше, чем другая осуществит свое противодействие, и наоборот. В данном случае конфликт рассматривается как последовательность элементарных воздействий каждой из сторон, причем каждое из состояний предыдущего этапа является начальным условием для следующего. Если необходимо учесть последствия переходов и ухода от воздействия, вводятся нестационарные во времени статистические характеристики. Этот подход позволяет не только получать адекватную модель конфликтного функционирования систем [7], но и синтезировать различные их классы [10]. Учет случайного характера самих воздействий и момента их начала имеет главенствующее значение для уравнений статистик (апостериорных вероятностей) переходов между состояниями [7]. Такой метод описания информационного взаимодействия СССН позволяет, с одной стороны, рассматривать взаимодействие как детерминированное перемещение в пространстве состояний динамических систем, как в адаптивных системах управления, а с другой как нелинейное стохастическое взаимодействие [10]. Недостатком описания взаимодействия СССН является то, что в этом случае она рассматривается как система параметрического

распознавания (в широком смысле), а в большинстве практических случаев из-за недостатка априорных сведений о дестабилизирующих факторах и противоборствующей стороне речь идет о непараметрическом распознавании.

Построение модели конфликта «СССН – нарушитель»

Возможности СССН по реализации различных мер противодействия конфликтному воздействию (ПКВ) применительно к складывающейся обстановке требуют не только наличия способов парирования этих мер. Главным условием при обосновании требований к характеристикам СССН и ее подсистем должно стать рассмотрение изменяющихся во времени ситуаций принятия мер ПКВ и способов их преодоления с учетом того, что противоборствующая сторона не является пассивной средой, а оптимизирует свои действия в интересах решения возложенных на нее задач.

В этом случае корректное обоснование требований к подсистеме контроля (ПК) СССН возможно путем оценки ее влияния на процесс развития и конечные результаты конфликта «СССН – нарушитель», причем конфликта динамического (развивающегося во времени), характеризуемого применением со стороны СССН широкого набора мер повышения ПКВ, а со стороны злоумышленника – достаточного набора парирования этих мер. Из этого положения будем исходить при разработке модели конфликта «СССН – нарушитель». Основные требования к данной модели будут состоять в следующем [13].

1. Основу построения модели должен составлять принцип прямого моделирования процесса конфликта «СССН – нарушитель» с детализацией его состояний до уровня, позволяющего исследовать информационные возможности сторон по оценке текущих состояний объекта управления. При этом функционирование СССН должно воспроизводиться в той мере, как это необходимо для обоснования требований к подсистеме контроля.

2. При разработке модели, прежде всего, должен учитываться тот факт, что противоборствующая сторона не является «пассивной» средой, а осуществляет целенаправленную оптимизацию алгоритма своих действий, выбирая те или иные меры повышения воздействий в соответствии с поставленными задачами и складывающимися условиями обстановки.

3. Рассчитываемый с использованием модели показатель эффективности должен определять конечную целевую направленность функционирования сторон в ходе конфликта, а именно: доведение требуемых (управляющих) сообщений до получателя в заданные сроки (со стороны СССН) и срыв своевременного доведения этих сообщений (со стороны нарушителя).

При разработке понятийной модели конфликта «СССН – нарушитель» будем исходить из следующего. Воздействие на СССН сопровождается ответной реакцией в виде принятия мер ПКВ. В свою очередь применение этих мер вызывает необходимость реализации злоумышленником ответных действий, направленных на повышение эффективности воздействий. Такой процесс повторяется до тех пор, пока одна из сторон не выполнит поставленную перед ней задачу: либо СССН обеспечит доведение до получателя требуемых сообщений к заданному сроку, либо злоумышленник сорвет доведение до получателя требуемых сообщений к заданному сроку. Следовательно, на понятийном уровне рассматриваемый процесс конфликта может быть представлен в виде совокупности действий противоборствующих сторон, протекающих по схеме «воздействие – ответная реакция», в зависимости от достигнутых состояний процесса конфликта.

В теории конфликта подобные ситуации описываются с использованием понятия контура управления, под которым понимается совокупность объекта воздействия

(управления), источника воздействия, управляющего элемента, а также датчика информации, связанных отношениями воздействия, передачи распорядительной, осведомительной и первичной информации соответственно, реализующих управление по принципу обратной связи по состоянию объекта воздействия [12].

Особенностью рассматриваемого процесса является наличие двух контуров управления (контура СССН и контура нарушителя), имеющих общий объект воздействия СССН и прямо противоположные цели функционирования. Причем ПК в этом процессе выступает в роли датчика информации состояния конфликта в контуре СССН. С учетом сказанного модель конфликта «СССН – нарушитель» может быть представлена в виде взаимосвязанных контуров управления с замкнутыми обратными связями по состоянию процесса воздействия, как это показано на Рисунке 2, где:

$V_п$ – воздействия на СССН со стороны нарушителя;

$V_у$ – управляющие воздействия со стороны СССН;

$K_п$ – команды управления средствами воздействия, поступающие от подсистемы выбора воздействия;

$K_у$ – команды управления, поступающие от подсистемы принятия решений;

$I_п$ – первичная информация о состоянии процесса воздействия, добываемая подсистемой сканирования уязвимостей;

$I_у$ – первичная информация о состоянии СССН, добываемая подсистемой контроля;

$I'_п$ – осведомительная информация о состоянии конфликтного процесса, получаемая от ПСУ подсистемой выбора воздействия;

$I'_у$ – осведомительная информация о состоянии СССН, поступающая от подсистемы контроля в подсистему принятия решений;

$I_{пкв}$ – информация о противодействии конфликтному воздействию.

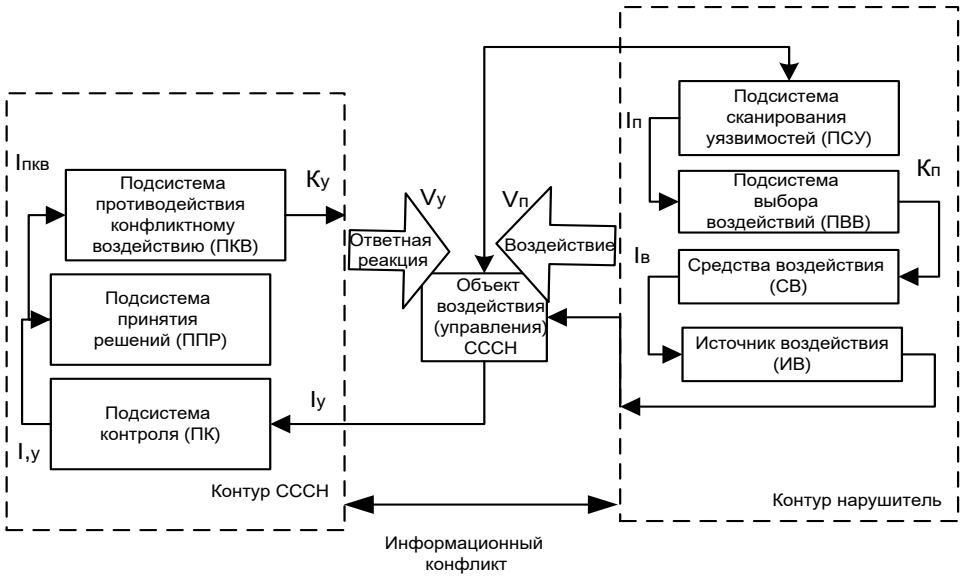

Рисунок 2 – Модель конфликта «СССН – нарушитель»
Figure 2 – Model of the conflict «SSSN – intruder»

Указанная схема отражает статическую структуру конфликта «СССН – нарушитель», а для оценки эффективности необходимо развертывание этого процесса во времени, т.е. воспроизведение его динамической структуры. Будем исходить из соблюдения принятых в теории управления условий «управляемости», «наблюдаемости» и «идентифицируемости», выполнение которых гарантирует

получение нетривиальных (неочевидных) результатов оценки эффективности. Применительно к рассматриваемому случаю указанные условия интерпретируются следующим образом.

С учетом отмеченных условий динамическая схема конфликта «СССН – нарушитель» в детерминированном виде (т.е. без учета случайного характера протекающих процессов) состоит в следующем.

Пусть в некоторый момент времени Т по СССН начинается передача сообщения. Подсистема сканирования уязвимостей (ПСУ) через время $t_{псу}$ на основе обработки первичной информации ($I_п$) выдает в подсистему выбора воздействия (ПВВ) осведомительную информацию ($I'_п$) о состоянии СССН и принятых мерах ПВВ. На ПВВ в течение времени $t_{пр}$ на основе этой информации принимается решение о выборе способа воздействия и вырабатывается команда целеуказания на средства воздействия. С получением команды средства воздействия осуществляют через интервал времени $t_{исп}$ воздействия на СССН с заданными параметрами. Работа СССН нарушается. ПК СССН через время $t_{пк}$ обнаруживают факт воздействия ($I_у$) и доводят до подсистемы принятия решений (ППР) осведомительную информацию ($I'_у$) о состоянии СССН. ППР на основе этой информации через время $t_{ппр}$ принимает решение о выборе меры ПКВ и вырабатывает команды целеуказания на средства противодействия, при этом через интервал времени $t_в$ реализуется выбранная мера ПКВ. Функционирование СССН восстанавливается, и цикл конфликтного взаимодействия повторяется.

В том случае, если подсистема контроля СССН имеет возможность обнаруживать факт ведения активного сканирования уязвимостей, развитие конфликтного процесса меняется. Подсистема контроля (ПК) на основе первичной информации ($I_у$) обнаруживает факт активного сканирования уязвимостей и передает осведомительную информацию ($I'_у$) в подсистему принятия решений (ППР), где, не дожидаясь появления воздействий в СССН, заблаговременно принимается решение о выборе меры ПКВ за время $t_{ппр}$, и СССН ожидает начала факта воздействий нарушителем. После обнаружения ПК факта воздействий система управления СССН через время $t_{пк}$ сразу же реализует меру ПКВ за время $t_в$, исключая время на принятие решения о выборе меры противодействия, что приводит к сокращению реального времени реакции $t_р = t'_р - t_{ппр}$ и обеспечивает упреждение действий нарушителя.

Такие циклы конфликтного взаимодействия будут продолжаться до тех пор, пока удачной будет передача сообщения, либо будут прекращены попытки передачи. В первом случае нарушитель не выполнит, а во втором случае – выполнит свою задачу.

Теоретически возможен случай принятия мер ПКВ сразу же после обнаружения факта ведения нарушителем активного сканирования уязвимостей. Однако в дальнейшем такой порядок работы не рассматривается, поскольку при существующих временных затратах на реализацию мер ПКВ в практике эксплуатации СССН не применяется.

Таким образом, предлагается модель конфликта «СССН – нарушитель» на понятийном уровне структурно представить в виде системы с двумя контурами управления, имеющими общий объект воздействия (СССН) и прямо противоположные цели функционирования, а динамику их взаимодействия представить в виде схемы «воздействие – ответная реакция» с возможностью принятия решения на применение мер ПКВ как после факта воздействия, так и после установления факта активного сканирования уязвимостей.

Моделирование стратегии противодействия в условиях конфликтного взаимодействия

Все процессы, взаимодействующие когда-либо, протекали всегда в условиях конфликта. Конфликтность в настоящее время проявляется на более высоком уровне.

С увеличением темпов роста технического прогресса информация приобрела более значимый характер, что привело к пониманию конфликтного взаимодействия с этой точки зрения как к явлению, наиболее негативному для информационного ресурса.

Пусть общее количество (качество) переданной информации в единицу времени будет равно $I_п(t)$, количество (качество) принятой информации – $I_{пр}(t)$, а количество негативного воздействия – $I_{вз}(t)$. Тогда количество информационного ущерба в единицу времени составит

$$I_{ущ}(t)= I_{вз}(t) / I_п(t).$$

Отсюда, если значение информационного ущерба $I_{ущ}(t)$ превышает значение принятой информации $I_{пр}(t)$,

$$I_{ущ}(t) > I_{пр}(t),$$

можно сделать вывод, что нанесен существенный вред информационному ресурсу.

Как отмечалось ранее, конфликтное взаимодействие предполагает воздействие одной из сторон на другую с целью повлиять на информационный ресурс, циркулирующий в СССН. Воздействие может быть внешнее и внутреннее.

Информация с момента ее образования может начать подвергаться негативному влиянию. И в процессе ее прохождения в системе управления (СУ) СССН, затем к участникам информационного обмена и в последнюю очередь к исполнителям в любой момент, как в период передачи, так и непосредственно на местах, может претерпевать воздействие со стороны криминальных элементов.

Исходя из вышесказанного, одной из главных задач СУ СССН можно считать своевременное выявление и предупреждение конфликтного воздействия.

Процесс взаимодействия конфликтного воздействия с СССН можно представить, как показано на Рисунке 3.

Состояние системы и циркулирующей в ней информации в любой момент времени можно охарактеризовать определенными параметрами и значениями. В результате конфликтного воздействия они могут изменяться, что показывает наличие конфликтного взаимодействия с СССН.

СУ СССН, отслеживая состояние системы, может при обнаружении конфликтного взаимодействия принять решение на выбор и применение стратегии противодействия и тем самым снизить уровень потерь информационного ресурса СССН.

Стратегия противодействия предполагает использование имеющегося ресурса, по определенному алгоритму для ответной реакции системы на воздействие. При этом время на принятие решения противодействия СУ не должно превышать время криминального воздействия. Иначе стратегия противодействия будет бессмысленной, так как уровень конфликта будет значительно ее превышать.

Своевременное выявление конфликтного взаимодействия, позволяет предупредить потери информации в СССН и обеспечить ее эффективную работу.

СССН предназначены для выполнения операций обработки, хранения, передачи информации, а также управления информационным ресурсом. Эффективность функционирования ведомственных инфокоммуникационных систем зависит от оперативности и качества использования информации.

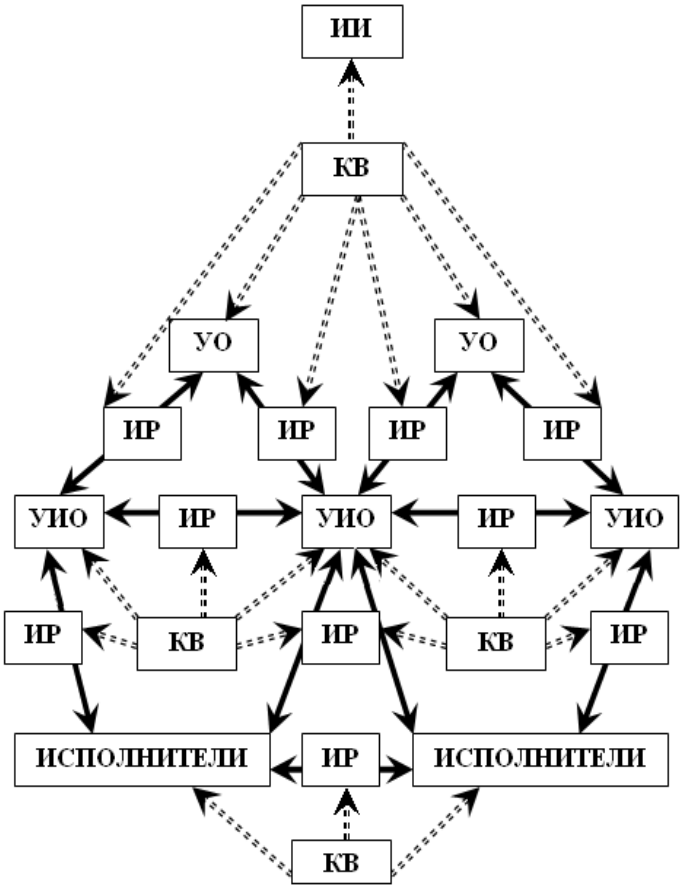

Рисунок 3 – Модель конфликтного взаимодействия
Элементы схемы: ИИ – источник информации; КВ – конфликтное воздействие;
УО – управляющий объект; ИР – информационный ресурс;
УИО – участники информационного обмена.
Figure 3 – Model of conflict interaction
Elements of the scheme: ИИ – a source of information; КВ – conflict impact;
УО – control object; ИР – information resource;
УИО – participants in information exchange

Циркулирующая в СССН информация органов внутренних дел (ОВД) представляет значительный интерес для криминальных группировок, иностранных технических разведок и отдельных нарушителей, что обуславливает конфликтное взаимодействие сторон.

В результате такого взаимодействия участники конфликта воздействуют на информацию, циркулирующую в СССН.

Каждому конфликтному взаимодействию соответствует определенный уровень, зависящих от времени параметров воздействия $\mathbf{G_{вз}(t)}$:

$$\mathbf{G_{вз}(t)=\{ G_{вз1}, G_{вз2}, \ldots, G_{взi}\}.} \quad (1)$$

Конфликтное взаимодействие предполагает выбор и принятие решения противодействия конфликтному воздействию. Реакция системы при этом будет выражаться в множестве стратегий противодействия $\mathbf{G_{пр}(t)}$ конфликтному воздействию на каждом шаге конфликтного взаимодействия:

$$\mathbf{G_{пр}(t)=\{ G_{пр1}, G_{пр2}, \ldots, G_{прi}\}.} \quad (2)$$

Сам процесс функционирования СССН в условия конфликтного взаимодействия сторон будет выглядеть следующим образом.

Здесь элемент Таблицы 2 $\mathbf{G_{пр}/G_{вз}}$ представляет собой отношение значений параметров и условий противодействия к конфликтному воздействию.

Таблица 2 – Процесс функционирования СССН в условия конфликтного взаимодействия
Table 2 – The process of functioning of the SSSN in conditions of conflict interaction

$G_{пр}$ / $G_{вз}$	$G_{пр1}$	$G_{пр2}$	. . .	$G_{прi}$
$G_{вз1}$	$\frac{G_{пр1}}{G_{вз1}}$	$\frac{G_{пр2}}{G_{вз1}}$	. . .	$\frac{G_{прi}}{G_{вз1}}$
$G_{вз2}$	$\frac{G_{пр1}}{G_{вз2}}$	$\frac{G_{пр2}}{G_{вз2}}$	. . .	$\frac{G_{прi}}{G_{вз2}}$
. . .	. . .	. . .	. . .	. . .
$G_{взi}$	$\frac{G_{пр1}}{G_{взi}}$	$\frac{G_{пр2}}{G_{взi}}$	. . .	$\frac{G_{прi}}{G_{взi}}$

Процесс функционирования СССН можно описать на основе генетических алгоритмов, так как это сокращает время принятия системой управления адекватного решения по противодействию на конфликтное воздействие.

Генетические алгоритмы помогают выбрать из множества стратегий противодействия минимизирующие информационный ущерб информационному ресурсу СССН.

Информационный ущерб $\mathbf{V_{ущ}}$ может быть представлен как разность между количеством переданной $\mathbf{V_0}$ и принятой информации $\mathbf{V_п}$:

$$\mathbf{V_{ущ}=V_0 - V_п}. \quad (3)$$

При конфликтном взаимодействии могут быть реализованы следующие условия:

1. Стратегия противодействия конфликтному воздействию должна быть больше или равна конфликтному воздействию: $\mathbf{G_{пр}(t) \geq G_{вз}(t)}$. Данное условие определяет динамику конфликтного взаимодействия;
2. Если стратегия противодействия меньше конфликтного воздействия $\mathbf{G_{пр}(t) < G_{вз}(t)}$, то эксплуатация СССН в условиях конфликтного взаимодействия становится нецелесообразной.

Динамика развития конфликтного взаимодействия зависит от начальных условий функционирования $\mathbf{u_0}$ и параметров СССН $\mathbf{n_0}$, позволяющих отследить состояние системы в любой момент времени конфликтного взаимодействия и выбрать оптимальную стратегию противодействия.

Условия функционирования СССН определяются множеством всех возможных элементов участвующих в процессе функционирования системы:

$$\mathbf{U_j}=\sum_{i=1}^{j} u_i. \quad (4)$$

Параметры СССН описываются совокупностью значений состояния системы:

$$\mathbf{N_j}=\sum_{i=1}^{j} n_i. \quad (5)$$

j – количество параметров и условий участвующих в работе системы.

Погрешности в измерениях параметров и начальных условиях могут привести к «катастрофе», т.е. может быть выбрано неверное решение и принята неадекватная стратегия противодействия, таким образом, что динамика конфликта будет развиваться в пользу криминального воздействия. Это приведет к существенному росту информационного ущерба.

Функция конфликтного воздействия $\mathbf{G_{вз}(t)}$, так же как и функция стратегии противодействия конфликтному воздействию $\mathbf{G_{пр}(t)}$, будет все время существования конфликтного взаимодействия стремиться к максимуму, т.е.

$$\mathbf{F(G_{пр})=max\ G_{пр}(t);}$$
$$\infty$$
$$\mathbf{F(G_{вз})=max\ G_{вз}(t).}$$
$$\infty$$

Тогда конфликтное взаимодействие будет носить циклический характер и выглядеть следующим образом Рисунок 4.

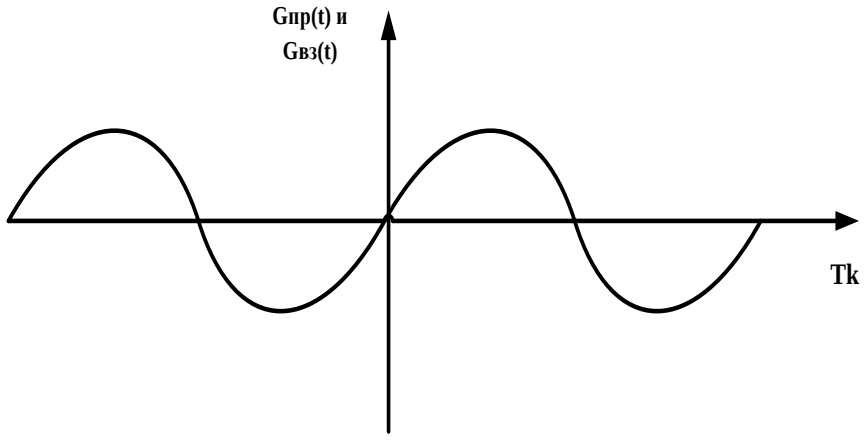

Рисунок 4 – График минимаксного состояния зависимости от количественных показателей Gпр(t) и Gвз(t) на каждом шаге конфликтного взаимодействия
Figure 4 – Graph of the minimax state of dependence on quantitative indicators Gпр (t) and Gвз (t) at each step of the conflict interaction

Функции максимума конфликтного воздействия и стратегия противодействия могут во время протекания конфликта $\mathbf{T_к}$ меняться местами в зависимости от количественных показателей $\mathbf{G_{пр}(t)}$ и $\mathbf{G_{вз}(t)}$ на каждом шаге конфликтного взаимодействия.

Для выбора стратегии противодействия необходимо использовать алгоритм конфликтного взаимодействия, представленный на Рисунке 5.

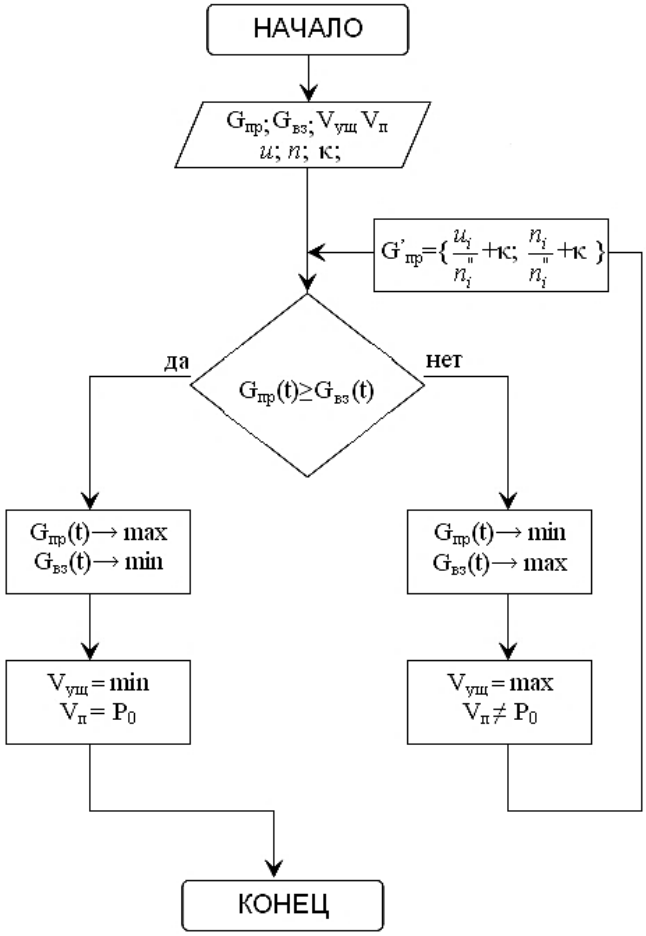

Рисунок 5 – Алгоритм конфликтного взаимодействия
Figure 5 – Algorithm of conflict interaction

Для этого необходимо в заданный момент времени сравнить значения конфликтного воздействия и стратегии противодействия. Если значение стратегии противодействия превышает уровень значения криминального воздействия, то это означает, что стратегия противодействия выбрана правильно и стремится к максимуму, а конфликтное воздействие уменьшается. При этом количество принятой информации соответствует уровню $\mathbf{P_0}$, необходимому для нормального функционирования системы связи специального назначения.

Если же значение конфликтного воздействия превышает значение стратегии противодействия, то стратегия противодействия выбрана неправильно и ее значение уменьшается, а конфликтное воздействие стремится к максимуму. Соответственно, количество принятой информации не соответствует требуемому уровню, что приводит к нарушению функционирования СССН. Поэтому после изменения условий и параметров функционирования информационно-телекоммуникационной системы $\mathbf{G'_{пр}}$ процесс сравнения повторяется до тех пор, пока не будет достигнут положительный результат.

Изменение условий и параметров функционирования СССН предполагает, что условия и параметры системы, в которых стало возможно преобладание конфликтного воздействия над стратегией противодействия, будут записаны во внутреннюю память системы и учтутся в дальнейшем как критические состояния.

Так как $\mathbf{G_{вз}}$ и $\mathbf{G_{пр}}$ зависят от условий функционирования и параметров СССН, то выразим $\mathbf{G_{вз}}$ и $\mathbf{G_{пр}}$ через них, и получим:

$$G_{\text{пр}j}=\{(u_1, n_1), (u_2, n_2), \ldots, (u_i, n_i)\};$$
$$G_{\text{вз}j}=\{(u''_1, n''_1), (u''_2, n''_2), \ldots, (u''_i, n''_i)\}.$$

Сумма этих значений равна:

$$G_{\text{пр}j}=\sum_{i=1}^{j}(u_i, n_i); \quad G_{\text{вз}j}=\sum_{i=1}^{j}(u''_i, n''_i). \tag{6}$$

Отсюда общее состояние конфликтного взаимодействия на каждом шаге будет определяться следующим образом:

$$K_j=\sum_{i=1}^{j}\left(\frac{u_i}{u''_i}, \frac{n_i}{n''_i}\right). \tag{7}$$

Для обеспечения функционирования СССН в условиях конфликта сторон можно ввести дополнительный параметр **к**:

$$G'_{\text{пр}}=\left(\frac{u_i}{u''_i}+\kappa, \frac{n_i}{n''_i}+\kappa\right). \tag{8}$$

Увеличение стратегии противодействия на **к** обеспечит выполнение необходимого условия противодействия конфликтному воздействию $G_{\text{пр}}(t) \geq G_{\text{вз}}(t)$.

Таким образом, выбор стратегии противодействия, как и само конфликтное взаимодействие, зависит от условий функционирования и параметров СССН. Конфликтное взаимодействие на всем отрезке времени носит циклический характер, т.е. происходит преобладание конфликтного воздействия либо стратегии противодействия конфликтному воздействию на каждом шаге конфликтного взаимодействия сторон.

Заключение

Выработка стратегии защиты информации может быть представлена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами. Состав и структура средств защиты информации в СССН существенно зависят от выбранной стратегии защиты. В работе предложена классификация возможных стратегий защиты в СССН. На основе принципа прямого моделирования процесса конфликта предложена модель конфликтного взаимодействия «СССН – нарушитель». Модель конфликта «СССН – нарушитель» на понятийном уровне структурно представлена в виде системы с двумя контурами управления, имеющими общий объект воздействия СССН и прямо противоположные цели функционирования, а динамика их взаимодействия представлена в виде схемы «воздействие – ответная реакция» с возможностью принятия решения на применение мер противодействия конфликтному воздействию как после факта воздействия, так и после установления факта активного сканирования уязвимостей. Стратегия противодействия в данном случае предполагает использование имеющегося ресурса, по определенному алгоритму для ответной реакции системы на воздействие. Показано, что выбор стратегии противодействия, как и само конфликтное взаимодействие, зависит от условий функционирования и параметров СССН. В результате моделирования показано, что конфликтное взаимодействие на всем отрезке времени носит циклический характер, т.е. происходит преобладание конфликтного воздействия либо стратегии противодействия конфликтному воздействию на каждом шаге конфликтного

взаимодействия сторон. Частные вопросы решения данной проблематики решены в работах автора [14 – 16]. В последующих публикациях будут описаны методы, модели и результаты решения поставленной задачи.

ЛИТЕРАТУРА

1. О связи : федер. закон от 07.07.2003 № 126-ФЗ Доступно по: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284635&fld=134&dst=1000000001,0&rnd=0.051152897698079736#08312366978414549 (дата обращения: 10.08.2021).
2. Язов Ю. К., Бурушкин А. А., Иванов С. М. Основные стратегии защиты информации в компьютерных системах. *Информация и безопасность*. 2008;1:118-121.
3. Северин Д. В. Пахоменкова Д. В., Дроздов Д. В. Обзор стратегий обеспечения информационной безопасности в информационных системах. *Наука и бизнес : пути развития*. 2019;10(100):137-140.
4. Мальцев Г. Н., Лесняк Д. А. Применение стратегий поддержания защищенности в информационных системах. *Информационно-управляющие системы*. 2017;3(88):67-74.
5. Вахний Т. В., Гуц А. К. Теоретико-игровой подход к выбору оптимальных стратегий защиты информационных ресурсов. *Математические структуры и моделирование*. 2009;19:104-107.
6. Atif A., Sean B., Sangseo P. Information Security Strategies: Towards an Organizational Multi-Strategy Perspective. *Journal of Intelligent Manufacturing*. 2014;2(25) DOI:10.1007/s10845-012-0683-0. Доступно по: http://dx.doi.org/10.1007/s_10845-012-0683-0 (дата обращения 10.08.2021).
7. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления. *Системы управления, связи и безопасности*. 2015;3:122-183.
8. Хохлов Н. С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел в условиях противодействия угрозам информационной безопасности. Воронеж. 2005.
9. Новиков Д. А. Иерархические модели военных действий. *Управление большими системами*. 2012;37:25–62.
10. Макаренко С. И. Модель динамического многостороннего информационного конфликта с различными стратегиями участников. *Радиопромышленность*. 2021;2(31):35-48.
11. Козирацкий Ю. Л. Методический подход к построению вероятностных моделей конфликта группировок на основе полумарковских процессов. *Вестник Воронежского института МВД России*. 2017;4:135-143.
12. Шакирова А. Е. Имитационные модели в контуре управления организационными конфликтами. *Инженерный вестник Дона*. 2020;8:268-279.
13. Хохлов Н. С., Наумец А. В. Состав и структура системы управления сетями связи в условиях конфликтного взаимодействия сторон. *Вестник Воронежского института МВД России*. 2007;4:132-136.
14. 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: 10.08.2021).

15. 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: 10.08.2021).
16. 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. DOI: 10.26102/2310-6018/2020.31.4.037 (дата обращения: 10.08.2021).

REFERENCES

1. About communication: Feder. Law of 07.07.2003 No. 126-FZ Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284635&fld=134&dst=1000000001,0&rnd=0.051152897698079736#08312366978414549. (date of access : 08/10/2021).
2. Yazov Yu. K., Burushkin A. A., Ivanov S. M. Basic information security strategies in computer systems. *Information and security*. 2008;1:118-121.
3. Severin D. V., Pakhomenkova D. V., Drozdov D. V. Review of strategies for ensuring information security in information systems. *Science and Business: Ways of Development*. 2019;10(100):137-140.
4. Maltsev G. N., Lesnyak D. A. Application of strategies for maintaining security in information systems. *Information and Control Systems*. 2017;3(88):67-74.
5. Vakhniy T. V., Guts A. K. Game-theoretic approach to the choice of optimal strategies for protecting information resources. *Mathematical Structures and Modeling*. 2009;19:104-107.
6. Atif A., Sean B., Sangseo P. Information Security Strategies: Towards an Organizational Multi-Strategy Perspective. *Journal of Intelligent Manufacturing*. 2014;2(25). DOI: 10.1007 / s10845-012-0683-0. Available at: http://dx.doi.org/10.1007/s 10845-012-0683-0 (date accessed 10.08.2021).
7. Makarenko S. I. A dynamic model of a communication system in the context of a functional multilevel information conflict of observation and suppression. *Systems of Control, Communication and Security*. 2015;3:122-183.
8. Khokhlov N. S. Modeling and optimization of counteraction to information destruction in control and communication systems of internal affairs bodies in conditions of counteraction to information security threats. Voronezh. 2005.
9. Novikov D. A. Hierarchical models of military operations. *Large-Scale Systems Control*. 2012; 37: 25–62.
10. Makarenko S. I. Model of dynamic multilateral information conflict with different strategies of participants. *Radiopromyslennost*. 2021;2(31):35-48.
11. Koziratskiy Yu. L. Methodical approach to the construction of probabilistic models of the conflict of groups on the basis of semi-Markov processes. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia*. 2017;4:135-143.
12. Shakirova A. E. Simulation models in the contour of managing organizational conflicts. *Engineering journal of Don*. 2020;8:268-279.

13. Khokhlov N. S., Naumets A. V. Composition and structure of the control system of communication networks in conditions of conflict interaction of the parties. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia*. 2007;4:132-136.
14. Bokova O. I., Zhayvoronok D. A., Kanavin S. V., Khokhlov N. S. Model of a complex of means of counteracting threats to information security 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 (date of access: 08/10/2021).
15. Gilev I. V., Kanavin S. V., Popov A. V., Khokhlov N. S. 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 (date of access: 08/10/2021).
16. 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 threats to information security of a special-purpose communication network. *Modeling, optimization and information technology*. 2020; 8 (4). Available at: https://moitvivt.ru/ru/journal/pdf?id=887. DOI: 10.26102 / 2310-6018 / 2020.31.4.037. DOI: 10.26102 / 2310-6018 / 2020.31.4.037 (date accessed: 10.08.2021).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

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
ORCID: 0000-0003-0575-2773

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.

Статья поступила в редакцию 11.08.2021; одобрена после рецензирования 15.09.2021; принята к публикации 17.09.2021.

The article was submitted 11.08.2021; approved after reviewing 158.09.2021; accepted for publication 17.09.2021.