УДК 004.056.53 DOI: 10.26102/2310-6018/2020.29.2.040

# Модель комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения

**О.И. Бокова[1], Д.А. Жайворонок[2], С.В. Канавин[3], Н.С. Хохлов[4]**
*[1]ООО «Каскад», Москва, Российская Федерация,*
*[2]ФГБОУВО Российский государственный университет правосудия, Воронеж, Российская Федерация,*
*[3,4]Воронежский институт МВД России, Воронеж, Российская Федерация*

***Резюме:*** В настоящее время сети связи специального назначения получили большое распространение в органах государственной власти, органах, осуществляющих функции обороны страны, безопасности государства и обеспечения правопорядка. 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 предложена модель формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Приведено описание подобных комплексов, рассмотрены ситуации и основания для их применения. Обращается внимание на выявление общих технологических особенностей формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Для формирования требований к комплексам средств противодействия угрозам информационной безопасности в сетях связи специального назначения составлена база правил, на основании которых будут выбираться определенные средства противодействия. Авторами проведено моделирование функционирования комплекса средств противодействия с применением аппарата лингвистических переменных и нечетких экспертных систем. На основе полученных результатов могут быть предложены требования к созданию комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения. Математический аппарат, использованный в данной статье, основан на применении лингвистических переменных и нечетких экспертных систем, может в полной мере характеризовать зависимость эффективности средств противодействия от совокупности реализуемых мер защиты.

***Ключевые слова:*** противодействие угрозам информационной безопасности, сети связи специального назначения, комплексный подход, нечеткие экспертные системы, управление информационной безопасностью.

***Для цитирования:*** 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.* 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

# Model of complex flows address threats to information security in communication networks special purpose

**O.I. Bokova[1], D.A. Zhayvoronok[2], S.V. Kanavin[3], N.S. Khokhlov[4]**
*[1]OOO «Cascade», Moscow, Russian Federation,*
*[2]FGBOUVO Russian State University of Justice, Voronezh, Russian Federation,*
*[3,4]Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russian Federation*

***Abstract:*** Currently, special-purpose communications networks are widely used in government bodies, bodies that carry out the functions of the country's defense, state security and law enforcement. In connection with the features of the functioning of infocommunication systems and communication networks for special purposes, it must be borne in mind that they are deployed and provide management and interaction within the existing departmental and interdepartmental communication systems. The article proposes a model for the formation of a set of means to counter threats to information security in communication networks for special purposes. A description of such complexes is given, situations and grounds for their application are considered. Attention is drawn to the identification of common technological features of the formation of a set of means to counter threats to information security in communication networks for special purposes. To formulate requirements for complexes of means of counteracting threats to information security in communication networks for special purposes, a rule base has been compiled on the basis of which certain countermeasures will be selected. The authors modeled the functioning of a complex of countermeasures using the apparatus of linguistic variables and fuzzy expert systems. Based on the results obtained, requirements can be proposed for creating a set of means to counter threats to information security in special communication networks. The mathematical apparatus used in this article, based on the use of linguistic variables and fuzzy expert systems, can fully characterize the dependence of the effectiveness of countermeasures on the totality of implemented protective measures.

***Keywords:*** countering threats to information security, special-purpose communications networks, integrated approach, fuzzy expert systems, security management.

***For citation:*** Bokova O.I., Zhayvoronok D.A., Kanavin S.V., Khokhlov N.S. Model of complex flows address threats to information security in communication networks special purpose. *Modeling, optimization and information technology.* 2020;8(2). Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/BokovaSoavtors_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.040 (In Russ).

## 1. Введение

Национальная безопасность Российской Федерации в эпоху всеобщей цифровизации существенным образом зависит от обеспечения информационной безопасности. С ростом технического прогресса эта взаимосвязь будет прослеживаться все сильнее. Обеспечение информационной безопасности от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе осуществления враждебных действий и актов агрессии является одной из важнейших государственных задач. Потребности общества определяют быстрый рост информационного обмена, осуществляемого устно и с помощью систем инфокоммуникаций, при этом постоянно растет не только количество, но и ценность передаваемой информации. Одновременно увеличивается и опасность серьезного ущерба в случае нарушения безопасности информации, что определяет актуальность решения задач противодействия угрозам информационной безопасности. В Доктрине информационной безопасности Российской Федерации отмечено, что мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий должны формироваться на комплексной основе.

В настоящее время сети связи специального назначения (СС СН) 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. Для формирования требований к комплексам средств противодействия угрозам информационной безопасности в сетях связи специального назначения необходимо полагаться на современную нормативную правовую базу: международные стандарты в области информационной безопасности, отраслевые стандарты Российской Федерации (ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов», ГОСТ ИСО/МЭК-Р 15408-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки информационной безопасности информационных технологий»), руководящие документы ФСТЭК России, а также ведомственные нормативные акты.

Развитие сетей связи специального назначения связано с использованием в них ресурсов сетей связи общего пользования, интеграцией различного рода трафика (речь, видео, данные), применением новых сетевых технологий (концепция NGN, пакетные технологии передачи, использование технологий виртуализации, самоорганизации и др.). Вместе с неоспоримыми преимуществами применения этих новых технологий в современных сетях связи специального назначения возникают и новые угрозы информационной безопасности. Наиболее характерным отрицательным фактором выступают повышение уровня подготовки современной организованной преступности, рост профессионализма и дальнейшее совершенствование ее технической оснащенности, базирующиеся на новейших достижениях научно-технического прогресса. Особого внимания заслуживают вопросы противодействия угрозам информационной безопасности в области применения робототехнических комплексов (систем), в том числе беспилотных летательных аппаратов.

Очевидно, что задача противодействия угрозам информационной безопасности в СС СН носит стратегический характер. В этом аспекте можно отметить работы [3–5], в которых рассматриваются вопросы противодействия угрозам информационной безопасности с позиции комплексного подхода. В трудах исследователей, не в полной мере раскрыто существо проблемы, что дало предпосылку для проведения дальнейших исследований.

## 2. Постановка задачи

Комплекс средств противодействия угрозам информационной безопасности в сетях связи специального назначения представляет собой сложную многофункциональную систему безопасности, состоящую из множества необходимых подсистем функционирования, объединенных единой интегрированной мультисервисной транспортной средой. Некоторые подсистемы могут отличаться своей внутренней инфраструктурой, наличием собственных систем управления базами данных, интеллектуальными средствами поддержки и принятия решений. Многие из таких комплексов являются самостоятельными информационными системами, доступ к которым осуществляется посредством удаленного подключения субъектов (пользователей или процессов подсистем обеспечения безопасности) к выделенным им информационным ресурсам.

При создании комплекса средств противодействия угрозам информационной безопасности в СС СН необходимо использовать принцип глубоко эшелонированной обороны от внешних и внутренних угроз. Многоуровневая система защиты с централизованным управлением исключает возможность эффективной реализации атаки при прорыве одного из уровней, в этом случае функцию защиты обеспечат другие. Применение блочной архитектуры дает возможности быстрой модернизации систем при использовании унифицированных стандартных блоков. Комплексный подход к построению системы защиты информации позволяет организовать структурированную

многокомпонентную целостную систему противодействия угрозам информационной безопасности.

В настоящее время классическая модель информационного конфликта претерпевает изменения, связанные с повышением количества уровней противодействия, в соответствии с семиуровневой моделью взаимодействия OSI [2]. Такая модель получила свое название – эталонная модель взаимодействия конфликтующих систем CSI (Conflict System Interconnection Reference Model). Модель делает свой акцент на формализацию информационных конфликтов на каждом уровне модели OSI. С учетом этого особое внимание уделяется вопросам вскрытия, мониторинга СС СН и наблюдения за протоколами управления и взаимодействия таких систем.

Информационное противоборство – это совокупность систематизированных, согласованных мероприятий, направленных на достижение информационного превосходства над противником [6]. Информационное противоборство включает в себя два сценария: информационное противодействие и информационную защиту.

Информационное противодействие осуществляется путем проведения комплекса мероприятий, включающих техническую разведку систем связи и управления, перехват передаваемой по каналам связи оперативной информации, мероприятий по дезинформации, радиоэлектронного подавления и выведения из строя информационно-телекоммуникационных систем противника.

Информационная защита рассматривает вопросы разведки информационно-телекоммуникационных систем противника, проверки полученной информации, защиты от поражения элементов информационных систем. В настоящее время информационная защита и информационное противодействие – процессы, автоматизированные с возможностью применения технологии искусственного интеллекта и не требующие постоянного наблюдения и контроля со стороны человека.

С учетом вышеизложенного вопросы формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения являются актуальными и требуют проведения дальнейших исследований в этой области.

Для раскрытия заявленной темы рассмотрим основные термины с соответствующими определениями, опираясь на положения национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. По природе возникновения угрозы подразделяются на естественные и искусственные. По источнику воздействия их принято делить на внешние и внутренние.

В качестве основных угроз информации, на предотвращение которых направлена защита информации, обычно выделяют следующие:

нарушение конфиденциальности (секретности) – потеря ценности информации при ее раскрытии;

нарушение целостности – потеря ценности информации при ее модификации (изменении) или уничтожении;

нарушение доступности – потеря ценности информации при невозможности ее оперативного использования.

В соответствии с Доктриной информационной безопасности Российской Федерации угроза информационной безопасности Российской Федерации (далее –

информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Угрозы информационной безопасности по способам их возможного негативного воздействия подразделяются на информационные, программные, программно-математические, физические, организационные [7, 17].

Информационные угрозы реализуются в виде:

–нарушения адресности и своевременности информационного обмена, противозаконного сбора и использования информации;

–осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

–манипулирования информацией (дезинформации, сокрытия или искажения информации);

–хищения информационных ресурсов из библиотек, архивов, банков и баз данных;

–нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

–внедрения в аппаратные и программные изделия компонентов, реализующих функции, неописанные в документации на эти изделия;

–разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации.

Физические угрозы реализуются в виде:

–уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

–хищения программных или аппаратных ключей и мер криптографической защиты информации;

–перехвата информации в технических каналах связи инфокоммуникационных систем;

–внедрения электронных устройств перехвата информации в технические средства связи инфокоммуникационных систем, а также в служебные помещения органов государственной власти и других силовых ведомств;

–перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

–воздействия на парольно-ключевые системы защиты систем обработки и передачи информации.

Организационные угрозы реализуются в виде:

–невыполнения требований законодательства в информационной сфере;

–неправомерного ограничения конституционных прав граждан на информационную деятельность и доступ к открытой информации;

–противоправной закупки за рубежом несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникаций и связи.

Обобщенная модель реализации воздействий, на информацию, функционирующую в СС СН, и реакции систем противодействия представлена на Рисунке 1.

В модели выделяются внутренние (предотвращение угроз, исходящих из внутренних источников) и внешние (предотвращение угроз, исходящих извне) мера противодействия. Потенциальные угрозы для СС СН выявляются в процессе создания и исследования модели угроз. В качестве угроз безопасности СС СН рассматриваются

потенциально или реально существующие воздействия, которые могут привести (приводят) к некоторому «ущербу».

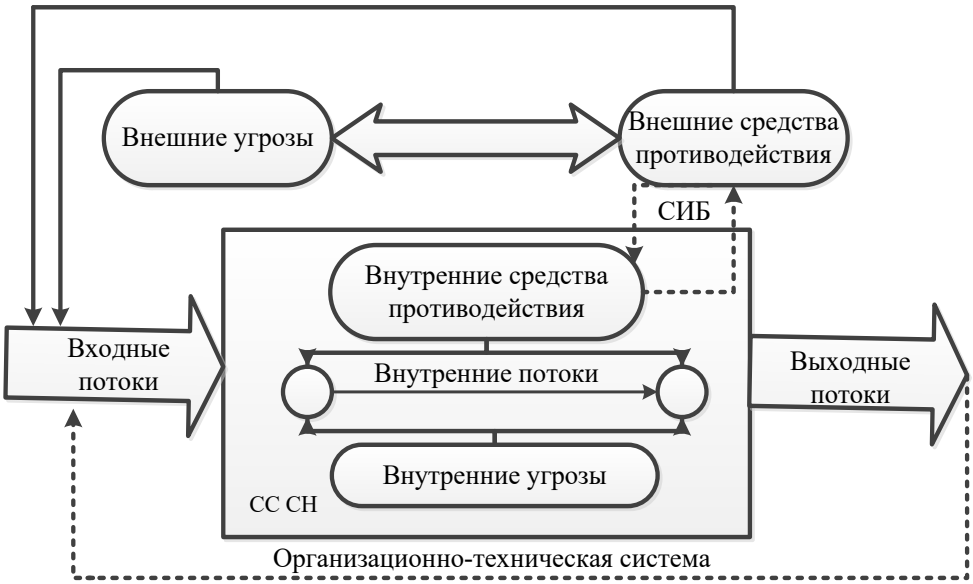


Рисунок 1 – Обобщенная модель реализации воздействий на информацию, функционирующую в СС СН, и реакции систем противодействия
Figure 1 – A generalized model of the implementation of the impacts on the information functioning in the SS SN, and the reaction of counteraction systems

Учитывая комплексность применения технических решений, особую актуальность приобретает задача обеспечения централизованного управления комплексными системами обеспечения информационной безопасности СС СН [11, 13, 18].

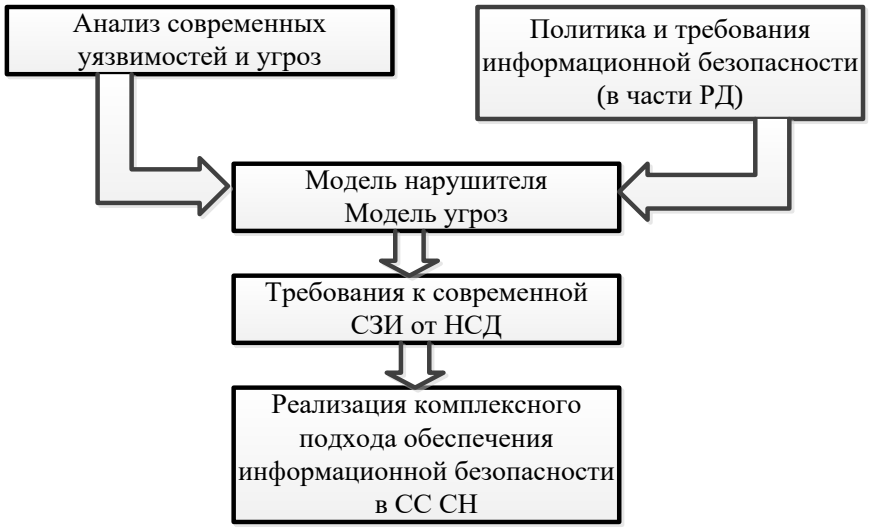


Рисунок 2 – Классический подход к созданию комплексных систем обеспечения информационной безопасности в СС СН
Figure 2 – The classic approach to the creation of integrated information security systems in SS SN

Классический подход к созданию комплексных систем обеспечения информационной безопасности для СС СН заключается в том, что механизмы противодействия, которые используются при построении защищённых СС СН, должны быть взаимоувязаны по месту, времени и характеру действия (Рисунок 2).

За основу в статье берется формализованная модель угроз информационной безопасности с позиции теории множеств, с учетом сложности, неоднозначности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства рассмотренная в работе [14].

Комплексность предполагает также использование в оптимальном сочетании различных методов и средств защиты информации: технических, программных, криптографических, организационных и правовых.

Среди отечественных разработчиков комплексных решений обеспечения информационной безопасности в СС СН можно отметить решения компаний: Код Безопасности − «Secret Net Studio», АО «Концерн «Автоматика» − «Центр мониторинга «СОПКА»», ПАО «Ростелеком» − «Единая платформа сервисов кибербезопасности».

Рассмотренные комплексы имеют модульную структуру и позволяют обеспечить защиту от внешних и внутренних угроз. Кроме этого функционал комплексов включает в себя: централизованное управление защитными механизмами, мониторинг событий безопасности и присвоение им категорий на основе риск-ориентированного подхода.

Интересным решением может являться информационно-аналитическая система - ситуационный центр, реализованная на интеграционной платформе цифрового управления. Опираясь на возможности ситуационного центра в сфере комплексной безопасности можно решать следующие задачи: мониторинг основных показателей и потенциальных объектов, определение интегральных показателей по отдельным подсистемам комплексной безопасности и потенциала угроз в целом, анализ и прогнозирование, планирование, регулирование и контроль мероприятий по противодействию угрозам информационной безопасности.

Применение комплексного подхода позволяет идентифицировать и устранить уязвимости в сетевом периметре, обеспечить круглосуточное реагирование на инциденты безопасности, а также привести процессы защиты информации в соответствие с требованиями регуляторов и законодательства Российской Федерации.

Данные примеры показывают перспективность работ направленных на создание отечественных, инновационных комплексов средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

В рамках работы над задачей противодействия угрозам информационной безопасности в СС СН коллективом авторов разработаны и зарегистрированы программы: ЭВМ «Методы формирования элементов комплекса противодействия разрушению информации в системах связи специального назначения при деструктивных широкополосных воздействиях»; «Программа выбора способов противодействия деструктивным электромагнитным воздействиям на основе нейронных сетей» [10, 15].

## 3. Математическая модель комплекса средств противодействия угрозам информационной безопасности в СС СН, основанная на применении лингвистических переменных и нечетких экспертных систем

Существует большое количество работ посвященных вопросам моделирования вопросов безопасности инфокоммуникационных систем с позиции управления и развития теории информационной безопасности: Буренин А.Н., Легков К.Е. [2, 3]

Макаренко С.И. [4, 5], Хохлов Н.С. [7], Новосельцев В.И., Кочедыков С.С., Орлова Д.Е. [8], Малюк А.А. [9], Новиков Д.А. [12] и др.

В статье рассмотрим построение математической модели комплекса средств противодействия угрозам информационной безопасности в СС СН, построенной с применением лингвистических переменных и нечетких экспертных систем. В качестве основного инструмента при прогнозировании состояния и средств противодействия угрозам информационной безопасности целесообразно использовать нечеткие экспертные системы, поскольку задача прогнозирования состояния системы в условиях информационных поражающих воздействий является сложной (с математической точки зрения) задачей и требует учета всех возможных параметров системы и воздействий [16]. В качестве исходной авторами предложена модель, основанная на концепции комплексной защиты информации [9].

Данная модель позволяет визуализировать эффективность средств противодействия с учетом реализации защиты СС СН. Для моделирования нечеткой экспертной системы уместно использовать пакет Fuzzy Logic Toolboks программы Matlab [13, 19]. Для заполнения базы знаний введем в рассмотрение значения лингвистических переменных:

f1 – предупреждение возникновения условий, способствующих возникновению деструктивных факторов, F1 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f2 – предупреждение непосредственного проявления деструктивных факторов, F2 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f3 – обнаружение проявившихся деструктивных факторов, F3 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f4 – предупреждение воздействия на защищаемую информацию и обнаружение деструктивных факторов, F4 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f5 – обнаружение воздействия деструктивных факторов на защищаемую информацию, F5 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f6 – локализация обнаруженного воздействия деструктивных факторов на защищаемую информацию, F6 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1];

f7 – ликвидация последствий локализированного обнаруженного воздействия деструктивных факторов на информацию, F7 = {НЕ СОБЛЮДАЕТСЯ, СОБЛЮДАЕТСЯ}, [0,1].

На Рисунке 3 приведена структурная схема модели комплекса средств противодействия угрозам информационной безопасности в СС СН, основанная на применении лингвистических переменных и нечетких экспертных систем.

Функции принадлежности термов комплекса средств противодействия изображены на Рисунке 4. OUT – результаты противодействия O = {ЗАЩИТА ОБЕСПЕЧЕНА, ЗАЩИТА НАРУШЕНА, ЗАЩИТА РАЗРУШЕНА}, [0,1].

В модели каждый из исходов является случайным, а все вместе они составляют полную группу событий, не происходящих единовременно. Из теории вероятностей известно, что сумма таких событий равна единице. Благоприятными с точки зрения работы комплекса будут те исходы, при которых сумма их вероятностей будет равна единице «Z1 – Защита обеспечена». В ином случае результатами работы комплекса будут «Z2 – Защита нарушена» или «Z3 – Защита разрушена».

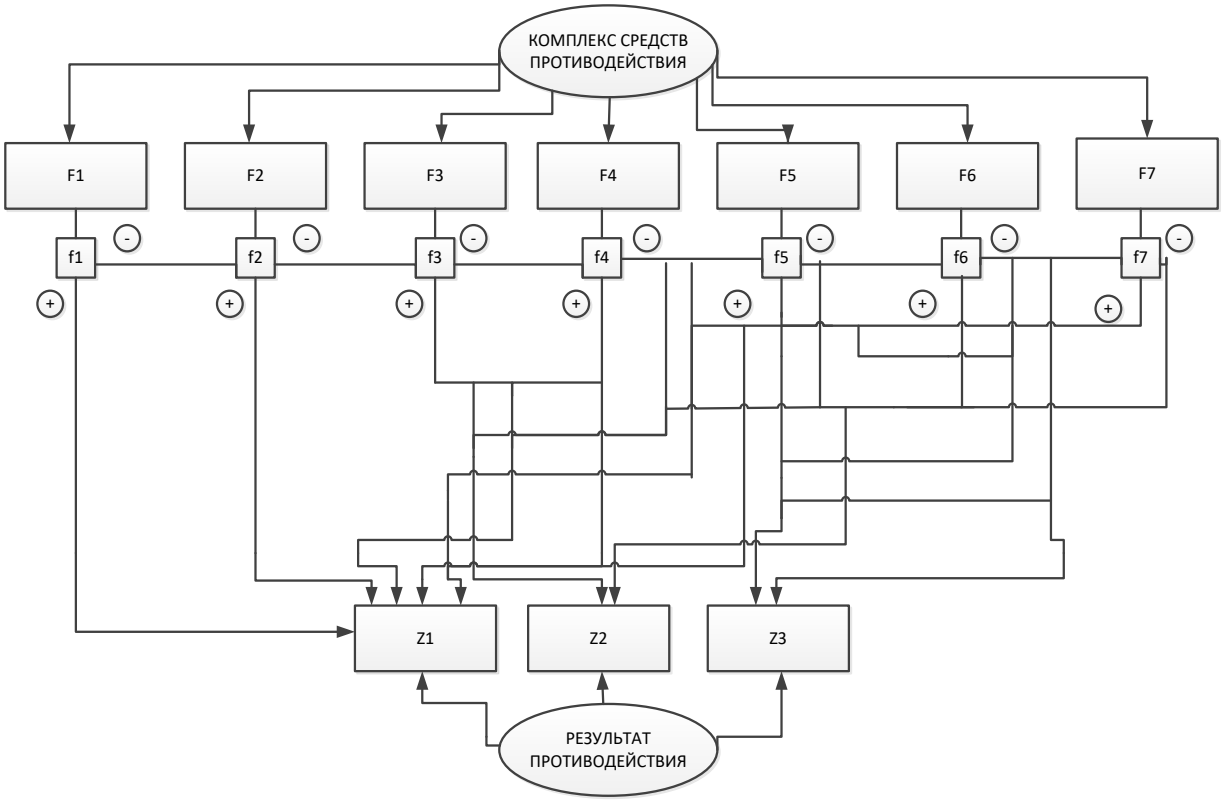


Рисунок 3 – Структурная схема модели комплекса средств противодействия угрозам информационной безопасности в СС СН, основанная на применении лингвистических переменных и нечетких экспертных систем

Figure 3 – The structural diagram of the model of a complex of means of countering threats to information security in the SS SN based on the use of linguistic variables and fuzzy expert systems

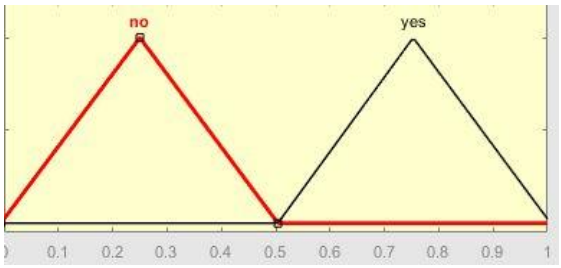


Рисунок 4 – Функции принадлежности термов комплекса средств противодействия

Figure 4 – The membership functions of the terms of the complex of means of counteraction

Следующим шагом является создание базы правил, на основании которых будут выбираться определенные средства противодействия. Пример заполнения базы правил на ряде элементов приведен ниже:

1. If f1 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;
2. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;
3. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = НЕ СОБЛЮДАЕТСЯ & f3 = СОБЛЮДАЕТСЯ & f4 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;

4. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = НЕ СОБЛЮДАЕТСЯ & f3 = НЕ СОБЛЮДАЕТСЯ & f4 = СОБЛЮДАЕТСЯ then Z1 = ЗАЩИТА ОБЕСПЕЧЕНА;

5. If f1 = НЕ СОБЛЮДАЕТСЯ & f2 = НЕ СОБЛЮДАЕТСЯ & f3 = НЕ СОБЛЮДАЕТСЯ & f4 = НЕ СОБЛЮДАЕТСЯ & f5 = СОБЛЮДАЕТСЯ & f6 = НЕ СОБЛЮДАЕТСЯ & f7 = НЕ СОБЛЮДАЕТСЯ then Z3 = ЗАЩИТА РАЗРУШЕНА.

Рисунок 5 иллюстрирует пример реализации правила 1, если первое правило соблюдается, то система делает вывод о том, что безопасность обеспечена. На Рисунке 6 приведена функциональная схема модели системы.

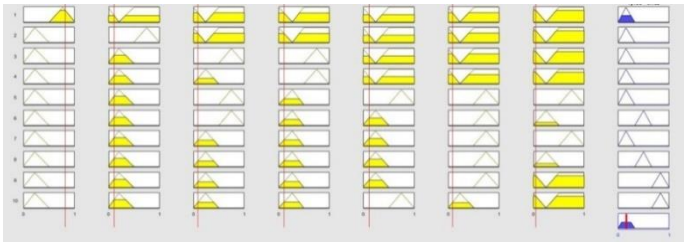

Рисунок 5 – Пример правила 1, если первое правило соблюдается, то система делает вывод о том, что безопасность обеспечена
Figure 5 – Example rule 1, if the first rule is respected, then the system concludes that security is ensured

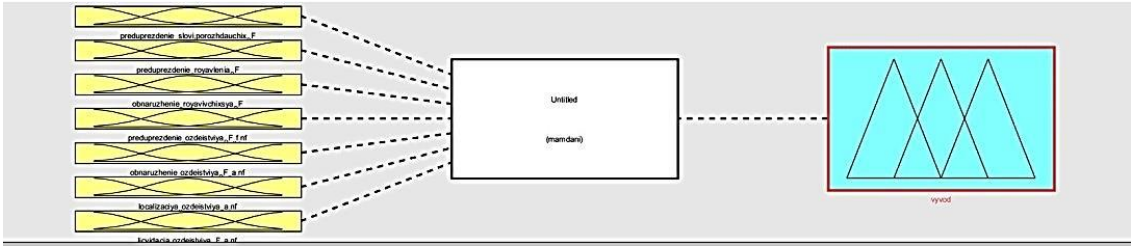


Рисунок 6 – Функциональная схема модели системы
Figure 6 – Functional diagram of the system model

На Рисунке 7 приведена нечеткая зависимость входных переменных от выходных. На данном Рисунке представлена зависимость f4 и f2 от выходных переменных.

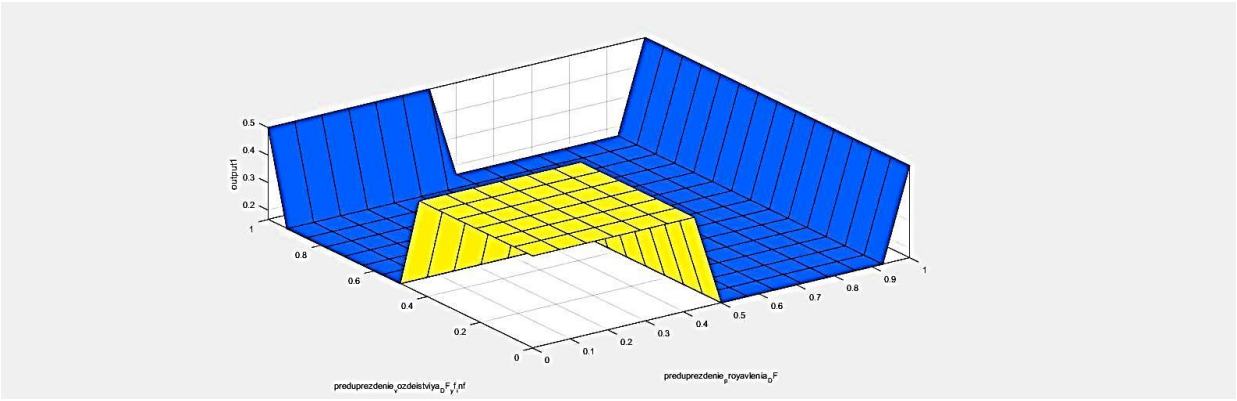


Рисунок 7 – Зависимости средств противодействия от входных переменных
Figure 7 – Dependencies of countermeasures on input variables

При равенстве f4 и f2 = 0,4 (не соблюдается) из графика видно, что безопасность является нарушенной, а при значении f4 и f2 больше 0,5 выходное значение будет близко к 0, следовательно, в данном случае можно сделать вывод, что безопасность обеспечивается.

Опираясь на полученные результаты математического моделирования комплекса средств противодействия угрозам информационной безопасности в СС СН с применением лингвистических переменных и нечетких экспертных систем, можно разработать требования к формированию комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения.

## 4. Заключение

В статье предложена модель формирования комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения, осуществлено исследование общих технологических особенностей формирования комплекса средств противодействия угрозам информационной безопасности в СС СН. Авторами проведено моделирование функционирования комплекса средств противодействия на основе аппарата лингвистических переменных и нечетких экспертных систем. На основе полученных результатов могут быть предложены требования к формированию комплекса средств противодействия угрозам информационной безопасности в СС СН. Математический аппарат, использованный в данной статье, основанный на применении лингвистических переменных и нечетких экспертных систем, может в полной мере характеризовать зависимость эффективности средств противодействия от совокупности реализуемых средств защиты. В рамках комплексного подхода возможно построение такого рода систем с применением элементов искусственного интеллекта, что будет рассмотрено авторским коллективом в дальнейших исследованиях.

## 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=0.05115289769807973 6#08312366978414549 (дата обращения: 03.06.2020).
2. Буренин А.Н., Легков К. Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей. *Наукоемкие технологии в космических исследованиях земли*. 2015;7(3):46-61.
3. Легков К.Е., Буренин А.Н. Модели процессов организации обработки оперативной информации современными вычислительными комплексами в условиях противодействий. *Вопросы оборонной техники.* 2018;3:87-95.
4. Макаренко С.И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления. *Системы управления, связи и безопасности*. 2015;3:122-185.
5. Макаренко С. И. Описательная модель сети связи специального назначения. *Системы управления, связи и безопасности.* 2017;2:113-164.
6. Боговик А. В., Игнатов В.В. Эффективность военной связи и методы ее оценки. Санкт-Петербург: ВАС. 2006:183.
7. Хохлов Н.С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел в условиях

противодействия угрозам информационной безопасности: монография. Воронеж : Воронежский институт МВД России. 2005:181.
8. Новосельцев В.И., Кочедыков С.С., Орлова Д.Е. Тензорный анализ Крона и его приложения: монография. Воронеж: Научная книга. 2017:260.
9. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры : курс лекций. М.: Горячая линия – Телеком. 2019:314.
10. Канавин С.В. Гилев И.В., Попов А.В. Методы формирования элементов комплекса противодействия разрушению информации в системах связи специального назначения при деструктивных широкополосных воздействиях. *Федеральная служба по интеллектуальной собственности*: Свидетельство № 2020611635; зарегистрировано в Реестре программ для ЭВМ от 05 февраля 2020 г.
11. Хохлов Н.С., Канавин С.В., Гилев И.В. Использование многосекторной антенной системы MIMO как элемента комплекса средств противодействия деструктивным электромагнитным воздействиям. *Вестник Воронежского института МВД России.* 2019;4:126-136.
12. Новиков Д.А. Теория управления организационными системами. – 2-е изд. М.: Физмалит. 2007:584.
13. Гилев И.В Модель противодействия разрушению информации при деструктивных электромагнитных воздействиях в системах радиосвязи специального назначения на основе нечетких экспертных систем. *Вестник Воронежского института МВД России.* 2020;1:158-168.
14. Хохлов Н.С., Дунин В.С. Модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город». *Вестник Воронежского института МВД России*. 2011;1:74-79.
15. Хохлов Н.С., Канавин С.В., Гилев И.В., Попов А.В. Программа выбора способов противодействия деструктивным электромагнитным воздействиям на основе нейронных сетей. *Федеральная служба по интеллектуальной собственности:* Свидетельство № 2020615923; зарегистрировано в Реестре программ для ЭВМ от 12 мая 2020 г.
16. Бокова О.И., Бондарь К.М., Дунин В.С., Канавин С.В., Скрипко П.Б. Моделирование процессов вторичных геодинамических факторов в целях обеспечения правоохранительного сегмента АПК «Безопасный город». *Моделирование, оптимизация и информационные технологии.* 2018;4(23). Доступно по: https://moit.vivt.ru/wp-content/uploads/2018/10/BokovaSoavtori_4_18_1.pdf. DOI: 10.26102 /2310-6018/2018.23.4.038 (Дата обращения: 02.06.2020).
17. Хохлов Н.С., Канавин С. В., Серпилин А.С. Требования к информационной безопасности систем радиомониторинга, сбора и обработки информации органов внутренних дел. *Научно-технический портал МВД России*. М.: ФКУ НПО СТИС МВД России. 2019;1:14-22.
18. Kanavin S., Gilev I. Modeling the Destructive Effect of Interference on Mobile Networks, Using the 3G Standard as an Example, Using a Noise Generator // Bulletin of the Lipetsk State Technical University. 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA). Lipetsk. 2019;407-410. DOI: 10.1109/SUMMA48161.2019.8947533.
19. Горемыкина Г.И., Мастяева И.Н., Герасимова Е.К. Моделирование системы оценки эффективности управления качеством на основе Fuzzy-технологии в среде Matlab. *Фундаментальные исследования*. 2013;6(8):1434-1439.

## REFERENCES


1. About the connection: fed. Law dated 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 (accessed 03.06.2020).
2. Burenin AN, Legkov K. E. Security issues of infocommunication systems and networks for special purposes: the main threats, methods and means of ensuring integrated network security. *H&ES Research*. 2015;7(3):46-61.
3. Legkov K.E., Burenin A.N. Models of processes for organizing the processing of operational information by modern computing systems in the context of counteractions. *Questions of defense technology*. 2018;3:87-95.
4. Makarenko S.I. A dynamic model of a communication system under the conditions of a multilevel informational conflict of observation and suppression. *Management, communication and security systems.* 2015;3:122-185.
5. Makarenko S. I. Descriptive Model of a Special Purpose Communication Network. *Management, communication and security systems.* 2017;2:113-164.
6. Bogovik A. V., Ignatov V.V. The effectiveness of military communications and methods for its evaluation. St. Petersburg: VAS. 2006: 183.
7. Khokhlov N.S. Modeling and optimization of counteraction to information destruction in control and communication systems of internal affairs agencies in the context of countering information security threats: a monograph. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2005:181.
8. Novoseltsev V.I., Kochedykov S.S., Orlova D.E. Crohn's tensor analysis and its applications: monograph. Voronezh: Scientific book. 2017:260.
9. Malyuk A.A. The basics of security policy for critical systems of information infrastructure: a course of lectures. M .: Hot line - Telecom. 2019:314.
10. Kanavin S.V. Gilev I.V., Popov A.V. Methods for the formation of elements of a complex to combat information destruction in special-purpose communication systems under destructive broadband influences. *Federal Service for Intellectual Property:* Certificate No. 2020611635; registered in the Register of computer programs of February 05, 2020
11. Khokhlov N.S., Kanavin S.V., Gilev I.V. The use of a multi-sector MIMO antenna system as an element of a set of means of counteracting destructive electromagnetic influences. *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia.* 2019;4:126-136.
12. Novikov D.A. Theory of management of organizational systems. - 2nd ed. M.: Fismalit. 2007:584.
13. Gilev I.V. A model for counteracting the destruction of information under destructive electromagnetic influences in special-purpose radio communication systems based on fuzzy expert systems. *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia.* 2020;1:158-168.
14. Khokhlov N.S., Dunin V.S. A model of information security threats of the Safe City integrated automated intellectual system. *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia.* 2011;1:74-79.
15. Khokhlov N.S., Kanavin S.V., Gilev I.V., Popov A.V. The program of choosing methods of counteracting destructive electromagnetic influences based on neural networks. *Federal Service for Intellectual Property:* Certificate No. 2020615923; registered in the Computer Software Registry of May 12,2020
16. Bokova O.I., Bondar K.M., Dunin V.S., Kanavin S.V., Skripko P.B. Modeling processes of the secondary geodynamic factors for ensuring the law-enforcement segment of the hardware and software complex «Safe city». *Modeling, optimization and information*

*technology*. 2018; 4 (23). Available at: https://moit.vivt.ru/wp-content/uploads/2018/10/BokovaSoavtori_4_18_1.pdf. DOI: 10.26102 /2310-6018/2018.23.4.038 (accessed: 02.06.2020).
17. Khokhlov N.S., Kanavin S.V., Serpilin A.S. Requirements for the information security of radio monitoring systems, collection and processing of information of internal affairs bodies. *Scientific and technical portal of the Ministry of Internal Affairs of Russia.* M .: FKU NPO STIS Ministry of Internal Affairs of Russia. 2019;1:14-22.
18. Kanavin S., Gilev I. Modeling the Destructive Effect of Interference on Mobile Networks, Using the 3G Standard as an Example, Using a Noise Generator // Bulletin of the Lipetsk State Technical University. 1st International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA) – Lipetsk. 2019;407-410. DOI: 10.1109 / SUMMA48161.2019.8947533.
19. Goremykina G.I., Mastyaeva I.N., Gerasimova E.K. Modeling a system for evaluating the effectiveness of quality management based on Fuzzy technology in the Matlab environment. *Fundamental research*. 2013;6(8):1434-1439.

## 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.

**Жайворонок Денис Александрович,** кандидат технических наук, доцент, декан факультета, Центральный филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования "Российский государственный университет правосудия", Воронеж, Российская Федерация.
*e-mail: d.zh007@bk.ru*

**Denis A. Zhayvoronok,** Candidate of Technical Sciences, Associate Professor, Dean of the Faculty, Central Branch of the Federal State Budgetary Educational Institution of Higher Professional Education "Russian State University of Justice", Voronezh, 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.