УДК 004.056.53
DOI: 10.26102/2310-6018/2022.36.1.029

Формирование требований к защищенной информационно-телекоммуникационной инфраструктуре сети связи специального назначения

О.И. Бокова[1], С.В. Канавин[2]✉, Н.С. Хохлов[2]

[1]ООО «Каскад», Москва, Российская Федерация,
[2]Воронежский институт Министерства внутренних дел России, Воронеж, Российская Федерация
sergejj-kanavin@rambler.ru✉

Резюме: В современных условиях хорошо отлаженная защищенная информационно-телекоммуникационная инфраструктура как симбиоз средств информатизации, автоматизации, связи и средств защиты информации способна сыграть значительную роль в формировании цифрового общества. Актуальной задачей в сложившейся обстановке является формирование требований к защищенной информационно-телекоммуникационной инфраструктуре сети связи специального назначения. В работе выявлены особенности обеспечения информационной безопасности в контексте управления защищенной информационно-телекоммуникационной инфраструктурой сети связи специального назначения. На основе анализа работ, посвященных данной области научных исследований, предложена архитектура управления информационной безопасностью сети связи специального назначения. Система обеспечения информационной безопасности, защиты и управления является комплексной и реализует централизованное управление средствами защиты информации, мониторинг и анализ возможных угроз информационной безопасности сети связи специального назначения. Предложен алгоритм управления средствами обеспечения безопасности информации защищенной информационно-телекоммуникационной инфраструктуры сети связи специального назначения. На основе функционально ориентированных информационных процессов рассмотрена возможность управления защищенной информационно-телекоммуникационной инфраструктурой сети связи специального назначения. В статье показаны результаты применения основных положений оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов сети связи специального назначения, представленные в виде зависимости эффективности сети связи специального назначения при реализации процесса обнаружения воздействий угроз информационной безопасности. Актуальность исследования обусловлена обеспечением защиты на всех жизненных циклах сети связи специального назначения. Материалы статьи представляют практическую ценность для специалистов в области информационной безопасности сетей связи специального назначения.

Ключевые слова: информационная безопасность; защищенная информационно-телекоммуникационная инфраструктура; управление средствами защиты информации; безопасность сети связи специального назначения, адаптивная подсистема безопасности и защиты информации, противодействие угрозам информационной безопасности.

Для цитирования: Бокова О.И., Канавин С.В., Хохлов Н.С. Формирование требований к защищенной информационно-телекоммуникационной инфраструктуре сети связи специального назначения. *Моделирование, оптимизация и информационные технологии.* 2022;10(1). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1157 DOI: 10.26102/2310-6018/2022.36.1.029

Formation of requirements for protected information and telecommunications infrastructure 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 the Interior of Russia,
Voronezh, Russian Federation
sergejj-kanavin@rambler.ru✉

Abstract: In modern conditions, a well-established secure information and telecommunications infrastructure as a symbiosis of informatization, automation, communications and information security tools can play a significant role in the formation of a digital society. An urgent task in the current situation is the formation of requirements for a secure information and telecommunication infrastructure of a special-purpose communication network. The paper reveals the features of ensuring information security in the context of managing the protected information and telecommunication infrastructure of a special-purpose communication network. Based on the analysis of works devoted to this area of scientific research, an architecture for managing the information security of a special-purpose communication network is proposed. The system for ensuring information security, protection and control is complex and implements centralized management of information security tools, monitoring and analysis of possible threats to information security of a special-purpose communication network. An algorithm for managing information security means of a protected information and telecommunication infrastructure of a special-purpose communication network is proposed. On the basis of functionally oriented information processes, the possibility of managing a secure information and telecommunication infrastructure of a special-purpose communication network is considered. The article obtained the results of applying the main provisions of the optimal control of functionally oriented information processes while ensuring the security of territorial segments of a special-purpose communication network, presented as a dependence of the effectiveness of a special-purpose communication network in the implementation of the process of detecting the impact of information security threats. The relevance of the study is due to the provision of protection at all life cycles of a special-purpose communication network. The materials of the article are of practical value for specialists in the field of information security of special-purpose communication networks.

Keywords: information security; secure information and telecommunications infrastructure; management of information security tools; special purpose communications network security, adaptive subsystem of security and information protection, counteraction to information security threats.

For citation: Bokova O.I., Kanavin S.V., Khokhlov N.S. Formation of requirements for protected information and telecommunications infrastructure special purpose communication networks. *Modeling, Optimization and Information Technology*. 2022;10(1). Available from: https://moitvivt.ru/ru/journal/pdf?id=1157 DOI: 10.26102/2310-6018/2022.36.1.029 (In Russ.).

Введение

В настоящее время современное общество находится на пороге цифровой трансформации, текущим этапом которой является глобальная цифровизация. Интеграция систем управления в сеть Интернет повышает уязвимость сетей связи с точки зрения информационной безопасности. Обнаружение и управление инцидентами безопасности в высоконагруженных системах реализуются с помощью инновационных технологий и инструментариев систем искусственного интеллекта, квантовых вычислений, Big Data, фрактального анализа, сетевых аномалий и др. Виртуализация инфраструктуры, облачные вычисления, программно-конфигурируемые сети и другие направления развития технологий дали толчок к развитию информационной безопасности. Все чаще встречаются в научной литературе термины «киберпространство», «кибербезопасность». В соответствии с современными требованиями должны меняться подходы к управлению информационной безопасностью. Базой для достижения информационного превосходства является

создание современной информационно-телекоммуникационной инфраструктуры. Хорошо отлаженная защищенная информационно-телекоммуникационная инфраструктура как симбиоз средств информатизации, автоматизации, связи и средств защиты информации способна сыграть значительную роль в формировании цифрового общества.

Для защиты информации в защищенной информационно-телекоммуникационной инфраструктуре сети связи специального назначения (СССН) применяется комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. Комплексность предполагает использование в оптимальном сочетании организационных, правовых, технических, программных, криптографических методов и средств защиты информации [1]. В Стратегии национальной безопасности Российской Федерации (указ Президента Российской Федерации от 2 июля 2021 г. № 400) сделан акцент на развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения источников, оперативной ликвидации последствий реализации таких угроз. Вопросам обеспечения информационной безопасности защищенной информационно-телекоммуникационной инфраструктуры посвящены научные работы [2], [3], [4], [5], [6]. А. В. Кузнецов рассматривает в рамках системы управления информационной безопасностью предприятия способ управления событиями [7]. В. И. Мищенко для управления информационной безопасностью в автоматизированных системах использует управление рисками с учетом методической базы стандарта NIST 800-30 [8]. А. Н. Буренин и др. для обеспечения информационной безопасности информационных подсистем рассматривают управление инцидентами [9]. В работах [10, 11] уделено внимание интеллектуальному анализу и визуализации информации при управлении информационной безопасностью. Проведенный анализ работ показывает, что представленные в них способы управления, методики, модели, методы и алгоритмы используются для решения прикладных задач в своих предметных областях. Вопросы обеспечения комплексной безопасности информации отражены поверхностно и требуют более детальной проработки.

В качестве защищенной информационно-телекоммуникационной инфраструктуры рассмотрим СССН, которая предназначена для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка в соответствии с положениями Федерального закона «О связи» от 07.07.2003 № 126. Информационно-телекоммуникационная инфраструктура – это организационно-техническое объединение программных, вычислительных и телекоммуникационных средств и связей между ними. Отказ или выход из строя любого из элементов может оказать воздействие на работоспособность системы в целом [2]. Информационно-телекоммуникационная инфраструктура СССН может включать в себя следующие элементы: единую сквозную транспортную среду для сигналов управления и информационных сигналов на базе стека протоколов TCP/IP, в том числе по потоку E1; IP-каналы связи, построенные на базе Ethernet-сетей с использованием протоколов TCP/IP; каналы мобильного широкополосного радиодоступа на основе технологий Wi-Fi и WiMAX; радиорелейные и спутниковые каналы связи. Информационно-телекоммуникационная инфраструктура СССН на уровне городских и районных центров субъектов Российской Федерации создается для обеспечения технической возможности подключения удаленных абонентов. Транспортная среда реализована на базе протокола TCP/IP с учетом собственной или арендованной инфраструктуры связи.

В таких системах процесс управления представляет собой осуществление информационных воздействий на объекты управления для их целенаправленного поведения. В основе информационно-телекоммуникационной инфраструктуры лежит

информационно-телекоммуникационная система, базирующаяся на информационно-телекоммуникационной сети, защита ресурсов которой должна осуществляться на этапах разработки, производства, эксплуатации и модернизации, а также по всей технологической цепочке ввода, обработки, передачи, хранения и выдачи информации. Такой подход применим к любым элементам и на различных этапах жизненных циклов систем защиты информации. Он позволяет минимизировать ущерб, а вероятность развития негативных сценариев можно свести к величине, очень близкой к нулю.

Требования к системе обеспечения информационной безопасности защищенной информационно-телекоммуникационной инфраструктуры СССН

Требования по защите информации к защищенной информационно-телекоммуникационной инфраструктуре СССН предъявляются в интересах формирования условий, при которых в случае их выполнения достигается определенный уровень защищенности информации, достаточный для недопущения нанесения существенного ущерба государству, обществу или личности.

Система обеспечения информационной безопасности защищенной информационно-телекоммуникационной инфраструктуры СССН может включать в себя централизованно управляемые средства защиты информации. Она функционирует с учетом регистрации событий информационной безопасности, неотложного реагирования на инциденты информационной безопасности и аудита информационной безопасности на всех уровнях защищенной информационно-телекоммуникационной инфраструктуры [2].

При использовании стандартных протоколов передачи данных возникают различные угрозы возникновения нарушений информационной безопасности, ведущие к несанкционированному доступу к данным со стороны злоумышленников. В целях минимизации угроз проникновения в информационные системы вредоносного кода в состав подсистемы обеспечения информационной безопасности может входить технологическая инфраструктура антивирусной защиты.

Формирование требований к информационной безопасности СССН опирается на актуальную нормативно-правовую базу: международные стандарты в области информационной безопасности, отраслевые стандарты в области информационной безопасности (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 [12].

Архитектура управления информационной безопасностью СССН

Система обеспечения информационной безопасности, защиты и управления является комплексной и реализует централизованное управление. На основе принципа системности – одного из концептуальных принципов защиты информации – реализуется мониторинг и анализ возможных угроз информационной безопасности СССН, обеспечивается защита на всех этапах жизненного цикла СССН, во всех звеньях СССН, а также комплексное использование механизмов защиты. С учетом подходов, приведенных в работе [13], общую архитектуру управления информационной безопасностью защищенной информационно-телекоммуникационной инфраструктуры СССН можно представить следующим образом (Рисунок 1).

В этом случае система управления безопасностью защищенной информационно-телекоммуникационной инфраструктуры СССН состоит из трех компонентов: системы мониторинга, системы принятия решений и системы обеспечения информационной безопасности, защиты и управления.

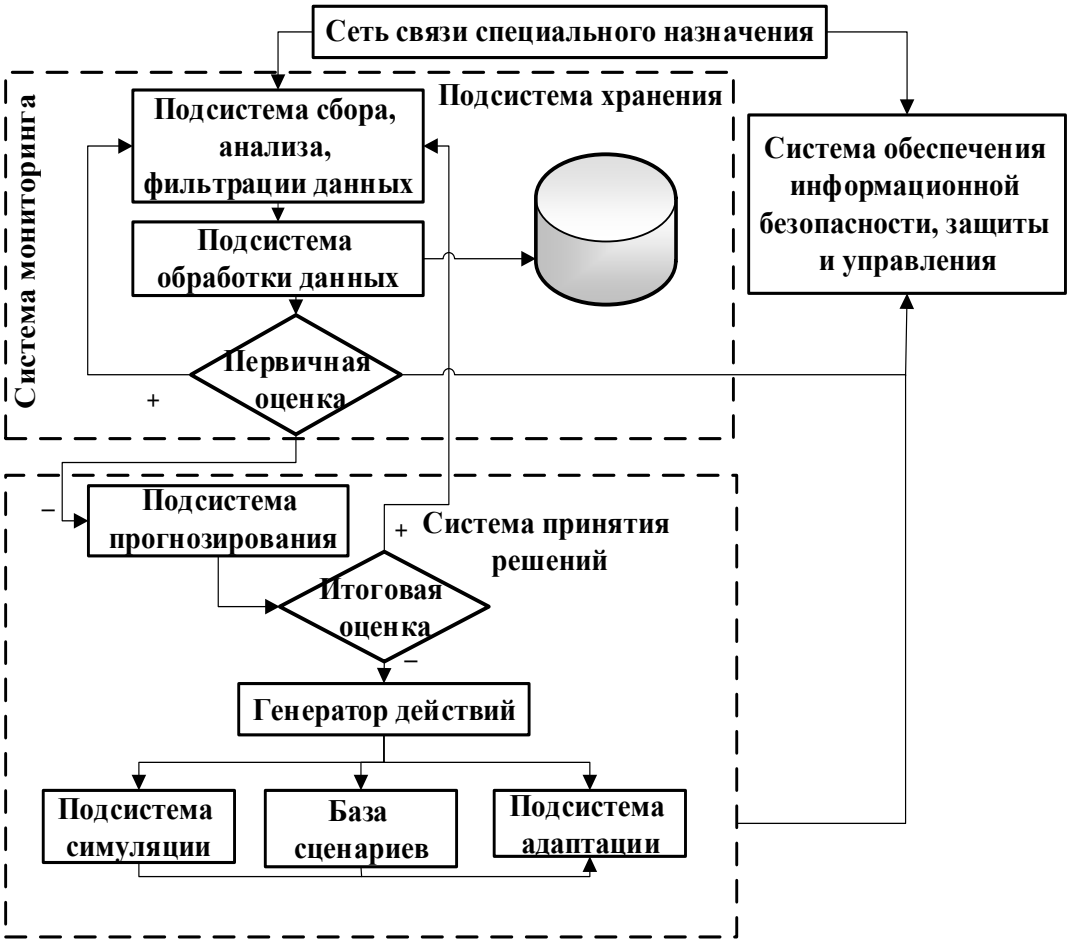

Рисунок 1 – Архитектура управления информационной безопасностью СССН
Figure 1 – SPCN information security management architecture

Система мониторинга осуществляет сбор, обработку, хранение и анализ данных, поступающих от компонентов СССН. В ней реализуются предобработка, нормализация и анализ данных, расчет первичной оценки о состоянии СССН. На основе полученных данных принимается решение о необходимости вмешательства.

Подсистема прогнозирования объединяет систему мониторинга и систему принятия решения. Она определяет тенденции поведения системы принятия решений. По результатам прогнозирования система принятия решений определяет необходимость вмешательства в функционирование СССН.

В условиях получения негативного прогноза запускается подсистема генерации компенсирующего воздействия. Генератор действий включает в себя подсистему симуляции действий, а также базу известных сценариев и подсистему адаптации. База известных сценариев состоит из нейронной сети, включающей в себя базу для обучения, предназначена для выбора мер противодействия и реализована в виде программы. Авторами получены свидетельства о государственной регистрации программы для ЭВМ (Программа выбора способов противодействия деструктивным электромагнитным

воздействиям на основе нейронных сетей. / Гилев И. В., Канавин С. В., Попов А. В., Хохлов Н. С. Свидетельство о регистрации программы для ЭВМ 2020615923, 04.06.2020. Заявка № 2020614645 от 12.05.202) и регистрации изобретения (Система выбора и реализации способов противодействия деструктивному электромагнитному воздействию, оказываемому нарушителем. / Гилев И. В., Канавин С. В., Хохлов Н. С. Свид. на изобретение № 2755743 РФ, С1 12/10, Н 04 W, № 2755743; Заявл. 18.12.2020; Опубл. 21.09.2021. – Бюл. № 27). Адаптационное взаимодействие системы принятия решений с системой защиты и управления обусловливает ее адаптивность – приспособление системы к внешнему воздействию путем синтеза управляющего вмешательства. Ключевую роль для этих процессов играет отрицательная обратная связь, обеспечивающая возвращение к равновесию в ответ на возмущающие воздействия.

Технологии, применяемые в системе обеспечения информационной безопасности, могут меняться, развиваться, адаптироваться под новые условия функционирования и переходить на более высокий уровень состояний развития. Набор технологий, способных обеспечить информационную безопасность СССН, может включать в себя следующие технологии:

− технологии Big Data, Deep Lerning и искусственного интеллекта (ИИ) позволяют эффективно обрабатывать неструктурированные данные сверхвысокого объема;

− технология блокчейна обеспечивает децентрализацию, отказоустойчивость и модульность СССН, а технология программно-конфигурируемых сетей – динамическое управление сервисами безопасности;

− технология адаптации поддерживает устойчивое функционирование инфраструктуры СССН в условиях активного воздействия угроз информационной безопасности;

− технология поведенческого анализа (UBA) отвечает за мониторинг и анализ поведения, детектирование поведенческих отклонений и расстановку для них приоритетов, которая, в свою очередь, должна обеспечивать оперативное реагирование на наиболее серьезные инциденты информационной безопасности.

Современная защищенная информационно-телекоммуникационная инфраструктура сети связи специального назначения представляет собой совокупность информационных и телекоммуникационных инфраструктур на территории зоны обслуживания пользователей с учетом ведомственной принадлежности.

Конфиденциальность, целостность, доступность достигаются путем создания в защищенной информационно-телекоммуникационной инфраструктуре СССН интегрированной виртуальной защищенной среды, включающей в себя: средства криптографической защиты каналов связи; средства межсетевого экранирования; средства антивирусной защиты; средства защиты от несанкционированного доступа; программно-аппаратный комплекс аутентификации и хранения ключевой информации; средства предотвращения компьютерных атак; комплекс организационных мер.

Система обеспечения информационной безопасности, защиты и управления СССН (Рисунок 2) реализует механизмы управления элементами средств защиты информации (СЗИ) с учетом совокупности правил, процедур принятия управленческих решений на основе адекватных механизмов управления. Выработка вариантов решения по управлению СЗИ определяет выбор действий, направленных на обеспечение безопасности информации, циркулирующей в защищенной информационно-телекоммуникационной инфраструктуре СССН.

Современные системы обеспечения информационной безопасности, такие как «Secret Net Studio», «Центр мониторинга «СОПКА», «Единая платформа сервисов

кибербезопасности», имеют модульную структуру и позволяют обеспечить защиту от внешних и внутренних угроз [6]. Кроме того, функционал системы обеспечения информационной безопасности включает в себя централизованное управление защитными механизмами, мониторинг событий безопасности и присвоение им категорий на основе риск-ориентированного подхода.

Данные системы могут использоваться в совокупности с информационно-аналитической системой – ситуационным центром. Ситуационный центр реализован на интеграционной платформе цифрового управления. Опираясь на возможности ситуационного центра, в сфере информационной 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. Интеллектуализация ситуационных центров – одно из приоритетных направлений, которое позволит эффективно решать вопросы информационной безопасности.

Рисунок 2 – Система обеспечения информационной безопасности, защиты и управления СССН
Figure 2 – System for ensuring information security, protection and control of SPCN

Необходимо учитывать, что для специалиста по информационной безопасности немаловажным фактором является визуализация сигналов тревоги при обнаружении внешних воздействий на СССН. В этом случае мы можем рассматривать визуальную защиту как один из элементов комплексной информационной защиты [12].

Алгоритм управления средствами защиты информации

Описание процессов управления средствами обеспечения информационной безопасности защищенной информационно-телекоммуникационной инфраструктуры СССН основывается на введении иерархических контуров, охватывающих прямыми и обратными связями как управляющие элементы, так и объекты управления. Алгоритм

управления СЗИ включает в себя последовательность действий, определяющих цикл контроля, и непосредственно цикла управления средствами защиты информации (Рисунок 3).

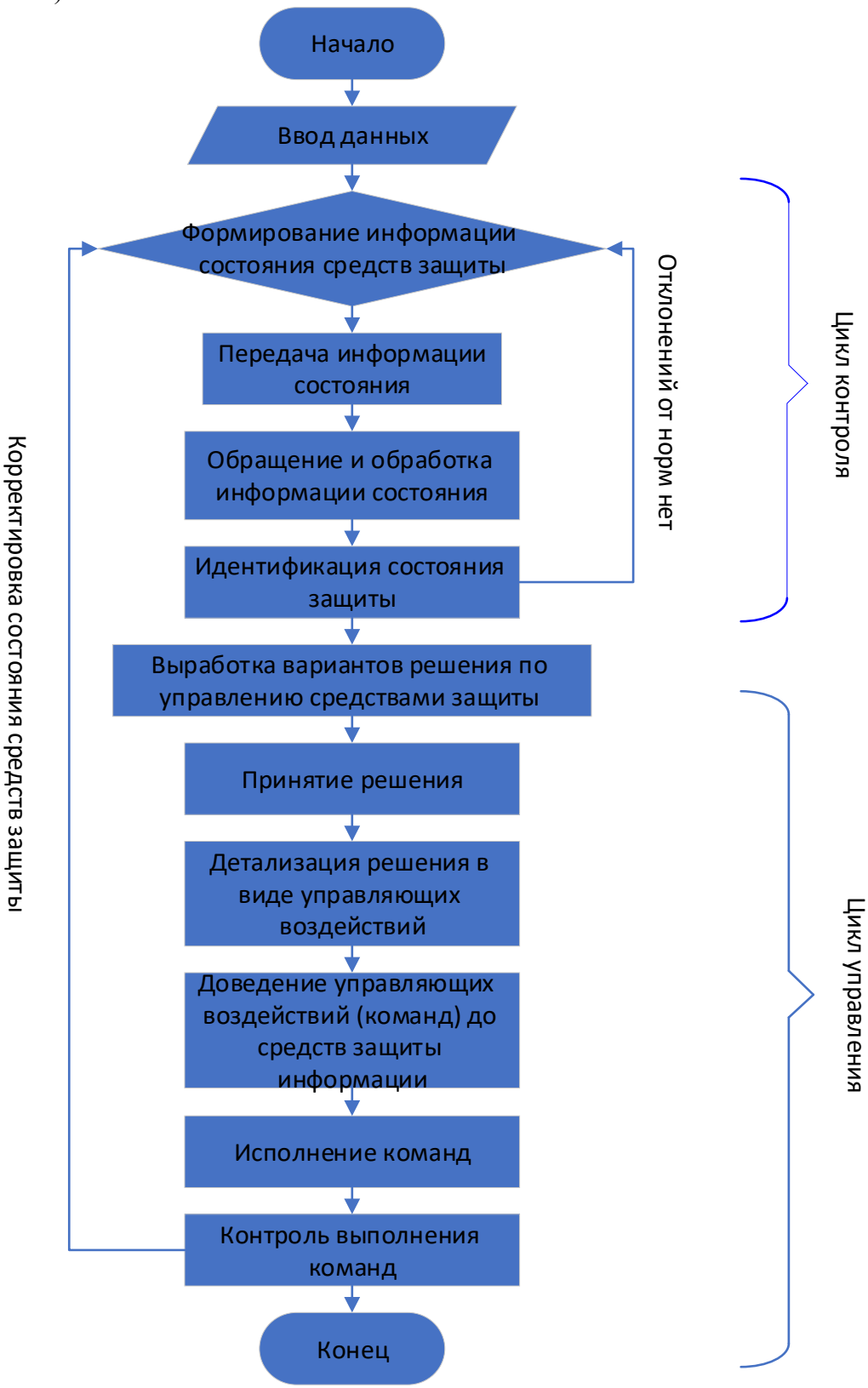

Рисунок 3 – Алгоритм управления средствами защиты информации
Figure 3 – Algorithm for managing information security tools

Процессы управления средствами обеспечения информационной безопасности могут быть представлены в виде алгоритма управления. Формирование множества вариантов решения по управлению СЗИ основывается на использовании формальной модели безопасности. При этом каждый вариант соответствует прогнозу изменения состояния системы защиты в результате выполнения тех или иных действий, направленных на изменение режимов функционирования объектов управления (средств защиты). Решения по управлению должны включать только те операции, которые «нормализуют» состояние системы защиты [14].

Основным моментом в цикле контроля является анализ поведения критерия функционирования системы защиты, называемого далее функцией безопасности информации Θ=F(X). X – вектор показателей защищенности информации в различных элементах СССН [15].

Схема формирования сигналов несоответствия приведена на Рисунке 4. При этом выделяются три зоны состояния объекта защиты: «норма», «критическое» и «тревога». Сигнал μ формируется из двух компонентов, характеризующих попадание значение X_i в требуемый (μ_0) и в допустимый (μ_1) диапазон. Значение сигнала μ формируется следующим образом: $\mu=\mu_0 \wedge \mu_1$, хотя для принятия решений могут использоваться и значения μ_0 и μ_1.

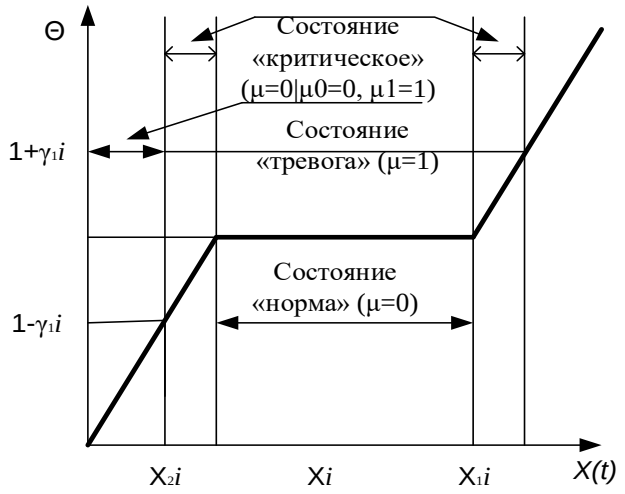

Рисунок 4 – Схема формирования сигнала *F(X)*
Figure 4 – *F(X)* signal conditioning circuit

Векторный показатель безопасности должен быть связан с параметрами состояния средств защиты, используемыми в цикле контроля. Ситуация называется критической, если значения параметров состояния будут изнутри приближаться к границам диапазонов $[(1-\gamma_1^i)X_1^i,\ (1+\gamma_2^i)X_2^i]$. В этом случае γ_1^i и γ_2^i – величины, обратные числу решений, принимаемых в единицу времени. Повышение устойчивости управления СЗИ достигается путем введения значений γ_1^i и γ_2^i отличных от нуля. С помощью величин γ_1^i и γ_2^i, можно регулировать скорость реакции СЗИ в условиях управления информационной безопасностью. Чем достовернее сведения о поведении параметров состояния, тем меньше должны быть значения величин γ_1^i и γ_2^i. Снижение осведомленности о действиях нарушителя и вследствие неопределенности поведения нарушителя, его оснащенности, месте и времени попыток несанкционированного доступа к информации требует увеличения допустимых диапазонов изменения параметров состояния. Если же значение хотя бы одного показателя состояния X_i выйдет

за пределы допустимого диапазона, то такая ситуация называется катастрофической и формируется сигнал «тревога».

Необходимо учитывать, что выход за допустимые пределы одного из показателей X_j не может быть компенсирован даже очень хорошими значениями других показателей X_i, $j \neq i$. Следовательно, необходимо «придерживать» приближение неблагоприятных показателей состояния к граничным значениям, контролируя при этом возможные ухудшения остальных составляющих безопасности X_i.

Поскольку каждый показатель X_i ограничен собственным диапазоном изменения допустимых значений, его можно привести к нормализованному виду, трактуемому как относительные потери безопасности по этому показателю:

$$X_i^t = \frac{2\left|X_i - X_i^m\right|}{(1+\gamma_2)X_2 + (1-\gamma_1)X_1}; \quad (1)$$

$$X_i^t = \frac{(1+\gamma_2)X_2 - (1-\gamma_1)X_1}{2}. \quad (2)$$

Такое представление потерь безопасности позволяет заметить, что $X_i \in [0,1]$. Этот диапазон открыт справа, поскольку X_i никогда не может принять значения $(1+\gamma_2^i)X_2^i$ или $(1-\gamma_1^i)X_1^i$ и, следовательно, невозможна ситуация, когда

$$2\left|X_i - X_i^m\right| (1+\gamma_2)X_2 - (1-\gamma_1)X_1.$$

В этом случае в соответствии с методическими рекомендациями [14] по исследованию поведения сложных систем при многокритериальной оптимизации можно осуществлять выбор одного из вариантов управления средствами защиты информации на основе меры близости относительно потерь к своему предельному значению (единице).

Основные положения оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности защищенной информационно-телекоммуникационной инфраструктурой сети связи специального назначения

В целях обеспечения информационной безопасности защищенной информационно-телекоммуникационной инфраструктуры СССН авторами были рассмотрены вопросы управления информационной безопасностью на примере оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов защищенной-информационно-телекоммуникационной инфраструктурой СССН. Для условий выбранного множества показателей эффективности СССН сформулированы следующие утверждения [16]:

1. Показатель своевременности обработки информации в компьютерной системе будет представлять собой монотонно убывающую в интервале [0, 1] функцию объема информационного пространства, реализующего процессы обработки накопления и выдачи данных.

2. Показатель защищенности СССН будет представлять собой монотонно убывающую в интервале [0, 1] функцию объемов информационного пространства, реализующих процессы обнаружения и парирования воздействий угроз информационной безопасности. Показано, что в условиях синтеза функционально

ориентированных информационных процессов в СССН справедливо следующее утверждение:

3. Существует экстремум эффективности СССН как функции объема информационного пространства, реализующего процесс обнаружения воздействий угроз ее информационной безопасности.

Из этого следует, что экстремум зависимости времени обработки информации в СССН как функции объема информационного пространства, реализующего процесс обнаружения воздействий угроз ее информационной безопасности, существует, т. е.

$$x_{(ext)} = \arg\{\text{extr}[П^{(c)}(V^{(обн)})]\}. \quad (3)$$

Было показано, что на основании монотонности функции будет существовать и экстремум зависимости эффективности СССН как функции объема информационного пространства $V^{(обн)}$, реализующего процесс обнаружения воздействий угроз ее информационной безопасности $П^{(c)}$ [16, 17].

С учетом применения основных положений оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов сети связи специального назначения получены результаты, представленные в виде зависимости эффективности СССН при реализации процесса обнаружения воздействий угроз информационной безопасности.

Заключение

В работе выявлены особенности обеспечения информационной безопасности в контексте управления защищенной информационно-телекоммуникационной инфраструктурой сети связи специального назначения. На основе анализа работ, посвященных данной области научных исследований, предложена архитектура управления информационной безопасностью сети связи специального назначения. Система обеспечения информационной безопасности, защиты и управления является комплексной и реализует централизованное управление средствами защиты информации, мониторинг и анализ возможных угроз информационной безопасности сети связи специального назначения. Предложен алгоритм управления средствами обеспечения безопасности информации защищенной информационно-телекоммуникационной инфраструктуры сети связи специального назначения. На основе функционально ориентированных информационных процессов рассмотрена возможность управления защищенной информационно-телекоммуникационной инфраструктурой сети связи специального назначения. В статье получены результаты применения основных положений оптимального управления функционально ориентированными информационными процессами при обеспечении безопасности территориальных сегментов сети связи специального назначения, представленные в виде зависимости эффективности сети связи специального назначения при реализации процесса обнаружения воздействий угроз информационной безопасности.

СПИСОК ИСТОЧНИКОВ

1. 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):33–34. Доступно по: https://moitvivt.ru/ru/journal/pdf?id=887 (дата обращения: 01.03.2022). DOI: 10.26102/2310-6018/2020.31.4.037.

2. Глухов А.П. Подходы к управлению информационной безопасностью в ОАО «РЖД» и модель ситуационного управления в нечеткой среде. *Естественные и технические науки.* 2015;9(87):127–136.
3. 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.
4. Канавин С.В. К вопросу выбора стратегии защиты системы связи специального назначения при угрозах информационной безопасности. *Моделирование, оптимизация и информационные технологии*. 2021;9;3(34):21–22. Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1033 (дата обращения: 01.03.2022). DOI: 10.26102/2310-6018/2021.34.3.020.
5. Хохлов Н.С., Канавин С.В., Журавлев М.Ю. Моделирование защищенного канала спутниковой связи органов внутренних дел с использованием аппаратуры оптимизации трафика. *Вестник Воронежского института МВД России*. 2021;3:25–35.
6. Хохлов Н.С., Канавин С.В., Гилев И.В. Оценка эффективности применения методов противодействия разрушению и модификации информации в системах связи специального назначения. *Вестник Воронежского института МВД России*. 2021;2:158–168.
7. Кузнецов А.В. Способ организации процесса управления событиями в части их обработки в рамках системы управления информационной безопасностью предприятия. *Вопросы защиты информации*. 2015;2(109):57–62.
8. Мищенко В.И., Шилов А.К. Управление рисками информационной безопасности в автоматизированных системах управления. *Информационные системы и технологии*. 2015;2(88);138–142.
9. Буренин А.Н., Легков К.Е., Оркин В.В. Управление инцидентами при обеспечении безопасности информационных подсистем автоматизированных систем управления сложными организационно-техническими объектами. *Инфокоммуникационные технологии*. 2018;16;1:122–131.
10. Агеев С.А. Методы интеллектуального анализа данных для управления рисками информационной безопасности в защищенных мультисервисных сетях специального назначения. *Автоматизация процессов управления*. 2015;2:42–49.
11. Милославская Н., Толстой А., Бирюков А. Визуализация информации при управлении информационной безопасностью информационной инфраструктуры организации. *Научная визуализация*. 2014;6;2:74–91.
12. 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;8;2(29):41–42. Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/05/BokovaSoavtors_2_20_1.pdf (дата обращения: 01.03.2022). DOI: 10.26102/2310-6018/2020.29.2.040.
13. Зегжда Д.П. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам*. М.: Горячая линия – Телеком; 2020. 560 с.
14. Ухлинов Л.М., Сычев М.П., Скиба В.Ю., Казарин О.В. *Обеспечение безопасности информации в центрах управления полетами космических аппаратов*. М.: Издательство МГТУ им Н.Э. Баумана; 2000. 366 с.
15. Жидко Е.А., Разиньков С.Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта. *Системы*

управления, связи и безопасности. 2018;1:122–135. Доступно по: https://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf (дата обращения: 01.03.2022).
16. Бокова О.И. Принципы оптимального управления безопасностью компьютерных систем региональных органов внутренних дел на основе функционально ориентированных информационных процессов. *Наука – производству*. 2006;3:16–17.
17. Хохлов Н.С., Бокова О.И., Канавин С.В., Гилев И.В. *Модели и методы формирования комплексов противодействия угрозам информационной безопасности в сетях связи специального назначения*. Воронеж: Воронежский институт МВД России;2020.175 с.

REFERENCES

1. Bokova O.I., Kanavin S.V., Hohlov N.S. Assessment of possible damage and response time of a complex of countermeasures to the implementation of threats to information security of a special-purpose communication network. *Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii = Modeling, Optimization and Information Technology*. 2020;8(4):33–34. Available from: https://moitvivt.ru/ru/journal/pdf?id=887. (accessed on: 01.03.2022). DOI: 10.26102/2310-6018/2020.31.4.037. (In Russ.)
2. Gluhov A.P. Approaches to Information security management at russian railways and a model of situational management in a fuzzy environment. *Estestvennye i tehnicheskie nauki = Natural and technical sciences*. 2015;9(87):127–136. (In Russ.)
3. Hohlov 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 effects in special-purpose communication networks. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh institute of the Ministry of interior of Russia.* 2020;2:164–174. (In Russ.)
4. Kanavin S.V. On the issue of choosing a strategy for protecting a special-purpose communication system under threats to information security. *Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii = Modeling, Optimization and Information Technology*. 2021;9;3(34):21–22. Available from: https://moitvivt.ru/ru/journal/pdf?id=1033 (accessed on: 01.03.2022). DOI: 10.26102/2310-6018/2021.34.3.020. (In Russ.)
5. Hohlov N.S., Kanavin S.V., Zhuravlev M.Ju. Modeling a secure satellite communication channel of internal affairs bodies using traffic optimization equipment. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh institute of the Ministry of interior of Russia.* 2021;3:25–35. (In Russ.)
6. Hohlov N.S., Kanavin S.V., Gilev I.V. Evaluation of the effectiveness of applying methods to counteract the destruction and modification of information in special-purpose communication systems. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh institute of the Ministry of interior of Russia.* 2021;2:158–168. (In Russ.)
7. Kuznecov A.V. Method for organizing the event management process in terms of their processing within the enterprise information security management system. *Voprosy zashhity informacii = Information security questions.* 2015;2(109):57–62. (In Russ.)
8. Mishhenko V.I., Shilov A.K. Information security risk management in automated control systems. *Informacionnye sistemy i tehnologii = Information systems and technologies.* 2015;2(88);138–142. (In Russ.)
9. Burenin A.N., Legkov K.E., Orkin V.V. Incident management while ensuring the security of information subsystems of automated control systems for complex organizational and technical objects. *Infokommunikacionnye tehnologii = infocommunication technologies.* 2018;16;1:122–131. (In Russ.)

10. Ageev S.A. Data mining methods for information security risk management in protected special-purpose multiservice networks. *Avtomatizacija processov upravlenija = Automation of control processes.* 2015;2:42–49. (In Russ.)
11. Miloslavskaja N., Tolstoj A., Birjukov A. Visualization of information in the management of information security of the organization's information infrastructure. *Nauchnaja vizualizacija = Scientific visualization.* 2014;6;2:74–91. (In Russ.)
12. Bokova O.I., Zhajvoronok D.A., Kanavin S.V., Hohlov N.S. Model of a complex of means of countering information security threats in special-purpose communication networks. *Modeling, Optimization and Information Technology.* 2020;8;2(29):41–42. Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/BokovaSoavtors_2_20_1.pdf (accessed on: 01.03.2022). DOI: 10.26102/2310-6018/2020.29.2.040. (In Russ.)
13. Zegzhda D.P. *Cybersecurity of the digital industry. Theory and practice of functional resilience to cyberattacks*. M.: Gorjachaja linija – Telekom, 2020. 560 p. (In Russ.)
14. Uhlinov L.M., Sychev M.P., Skiba V.Ju., Kazarin O.V. *Ensuring information security in spacecraft flight control centers.* M.: Izdatel'stvo MGTU im N.Je. Baumana; 2000. 366 p. (In Russ.)
15. Zhidko E.A., Razin'kov S.N. Model of the security and information protection subsystem of the communication and control system of a critically important facility. *Sistemy upravlenija, svjazi i bezopasnosti = Systems of Control, Communication and Security*. 2018;1:122–135. Available from: https://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf (accessed on: 01.03.2022). (In Russ.)
16. Bokova O.I. Principles of optimal security management of computer systems of regional internal affairs bodies based on functionally oriented information processes. *Nauka – proizvodstvu = Science to production*. 2006;3:16–17. (In Russ.)
17. Hohlov N.S., Bokova O.I., Kanavin S.V., Gilev I.V. *Models and methods for the formation of complexes for countering information security threats in special-purpose communication networks.* Voronezh: Voronezh institute of the Ministry of interior of Russia; 2020. 175 p. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Бокова Оксана Игоревна, доктор технических наук, профессор, научно-технический консультант, ООО «Каскад», Москва, Российская Федерация.
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
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.

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.

Статья поступила в редакцию 16.03.2022; одобрена после рецензирования 23.03.2022; принята к публикации 30.03.2022.

The article was submitted 16.03.2022; approved after reviewing 23.03.2022; accepted for publication 30.03.2022.