DOI 10.37882/2223-2966.2025.03.36

ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НАЗЕМНОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СРЕДНЕОРБИТАЛЬНОЙ СИСТЕМЫ СПУТНИКОВОЙ СВЯЗИ «СКИФ»

OPTIMIZATION OF THE MANAGEMENT OF THE INFORMATION SECURITY PROCESS IN THE GROUND-BASED INFORMATION AND TELECOMMUNICATIONS NETWORK OF THE MEDIUM-ORBIT SATELLITE COMMUNICATION SYSTEM «SKIF»

A. Pervushkina
D. Sakharov
A. Begaev
S. Krivtsov

Summary. The article examines the planning and management of the process of ensuring information security in the ground-based information and telecommunications network of the medium-orbit satellite communications system «SKIF».

Keywords: information security process management; satellite communication system; information protection; unauthorized access, Internet.

Первушкина Алиса Артуровна
Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича
a.pervushkina@spean.ru
Сахаров Дмитрий Владимирович
Кандидат технических наук, Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича
sguard7@mail.ru
Бегаев Алексей Николаевич
Генеральный директор АО «ИНСЕК»
a.begaev@inseq.ru
Кривцов Станислав Петрович
Генеральный директор АО «Спин»
s.krivtsov@spean.ru

Аннотация. В статье рассматривается планирование и управление процессом обеспечения информационной безопасности в наземной информационно-телекоммуникационной сети среднеорбитальной системы спутниковой связи «СКИФ».

Ключевые слова: управления процессом информационной безопасностью; система спутниковой связи; защита информации; несанкционированный доступ, интернет.

Значительная часть территории нашей страны расположена в высоких широтах, где плотность населения невелика, а зоны тайги, тундры и вечной мерзлоты мешают прокладке сетей оптоволоконной связи. В таких местах предоставить полный комплекс телекоммуникационных услуг для стационарных и подвижных объектов, обеспечить связанность территорий помогут спутники. Достичь указанных целей планируется путем развертывания группировок со спутниками связи. [1]

Система «Скиф» предназначена для обеспечения широкополосного доступа в Интернет на территории России и сопредельных регионов, что предусмотрено федеральным проектом «Сфера». Федеральный проект «Сфера» включает орбитальные группировки космических аппаратов связи и дистанционного зондирования Земли. Аппараты будут предоставлять широкополосный доступ в Интернет, а также Интернет вещей для 50 миллионов пользователей. Также «Сфера» обеспечит специальную связь — президентскую, правительственную, ведомственную.

Спутники «Скиф» обеспечат доступ в интернет в арктическом регионе. В настоящее время в северных широтах широкополосного интернета либо нет или он работает по сеансам и с большими задержками. Обеспечение интернет-связи посредством спутников «Скиф» позволит улучшить работу не только объектов морского, но и воздушного транспорта, а также научных экспедиций, полярников, работников метеорологических служб и объектов энергетики.

Всего в состав полномасштабной орбитальной группировки «Скиф» должно войти 12 спутников. Они будут работать на средней круговой орбите высотой 8070 км и наклонением 90 градусов к экватору. Для выполнения целевых задач космические аппараты оснастят многолучевой гибкой полезной нагрузкой на основе активной

фазированной антенной решётки. Её применение позволит быстро и гибко формировать зоны обслуживания, а также повысить суммарную пропускную способность системы. [2]

Целью работы является оптимизация рабочего пространства администратора безопасности информации в наземной информационно-телекоммуникационной сети среднеорбитальной системе спутниковой связи «СКИФ», путём применения специального программного обеспечения и специализированных методик поиска и нейтрализации инцидентов информационной безопасности.

Задачей исследования в статье является поиск методов сокращения времени цикла управления процесса поиска и нейтрализации инцидентов информационной безопасности администратором безопасности информации в наземной информационно-телекоммуникационной сети среднеорбитальной системе спутниковой связи «СКИФ».

1. Описание наземной информационно-телекоммуникационной сети среднеорбитальной системы спутниковой связи «СКИФ»

Структурная схема системы управления наземной информационно-телекоммуникационной сети (ИТКС) среднеорбитальной системы спутниковой связи «СКИФ» представлена на рисунке 1.

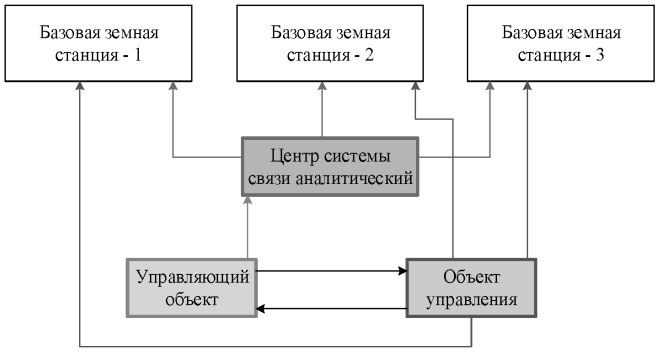


Рис. 1. Структурная схема системы управления наземной ИТКС среднеорбитальной системы спутниковой связи «СКИФ»

Центр системы связи аналитический (ЦССА) помимо своих основных задач управляет ИТКС и потоками информации для взаимодействия с базовыми станциями, которые входят в состав наземного специального комплекса (НСК).

ИТКС НСК состоит из основных частей, таких как:

1. Транспортная сеть НСК — это сеть связи, обеспечивающая взаимодействие между ЦССА и базовыми станциями через сети связи общего пользования, при использовании услуг связи операторов связи, средствами интернет-соединений с использованием крипто-туннелей.

Транспортная сеть НСК включает в себя:

— набор услуг связи от провайдеров сети связи общего пользования, как правило это будут операторы Ростелеком или ТрансТелеКом, а также могут использоваться компании местных операторов для доведения услуг связи не посредственно до района размещения ЦССА и базовых станций;
— отказоустойчивых кластеров межсетевых экранов, работающих по пограничному шлюзовому протоколу BGP v.4, который является сегодня основным протоколом обмена маршрутной информацией между автономными системами Интернета, со стороны пограничного маршрутизатора узла; [5]

В состав отказоустойчивых кластеров межсетевых экранов ЦССА будут входить:

— пограничный маршрутизатор узла;
— автоматизированное рабочее место менеджера конфигураций;
— отказоустойчивый кластер центра управления сетью;
— отказоустойчивый кластер узла безопасности;
— внутренний коммутатор.

В состав отказоустойчивого кластера межсетевого экрана базовых станций будут входить:

— пограничный маршрутизатор узла;
— отказоустойчивый кластер узла безопасности;
— внутренний коммутатор.

Схема взаимодействия отказоустойчивых кластеров межсетевых экранов ЦССА представлена на рисунке 2.

Отказоустойчивых кластеров межсетевых экранов используется для связи сетей ИТКС. При выходе из строя межсетевого экрана связь между сетями будет утеряна. Чтобы этого не произошло, используется резервирование. Вместо одного межсетевого экрана, устанавливается два одинаковых межсетевых экрана. В каждый момент времени активен только один из них. Второй находится в резерве. Один из межсетевых экранов считается основным (master), второй резервным (slave). Когда работает основной межсетевой экран, резервный блокирует все свои интерфейсы, кроме одного служебного.

Резервный межсетевой экран связан с основным специальной выделенной линией связи (dedicated link). Резервный межсетевой экран прослушивает выделенную линию связи и получает от основного межсетевой экрана всю информацию, характеризующую состояние компонента TCP/IP, и специально сформированные «пакеты жизни» (heartbeat или advertizing message), которые

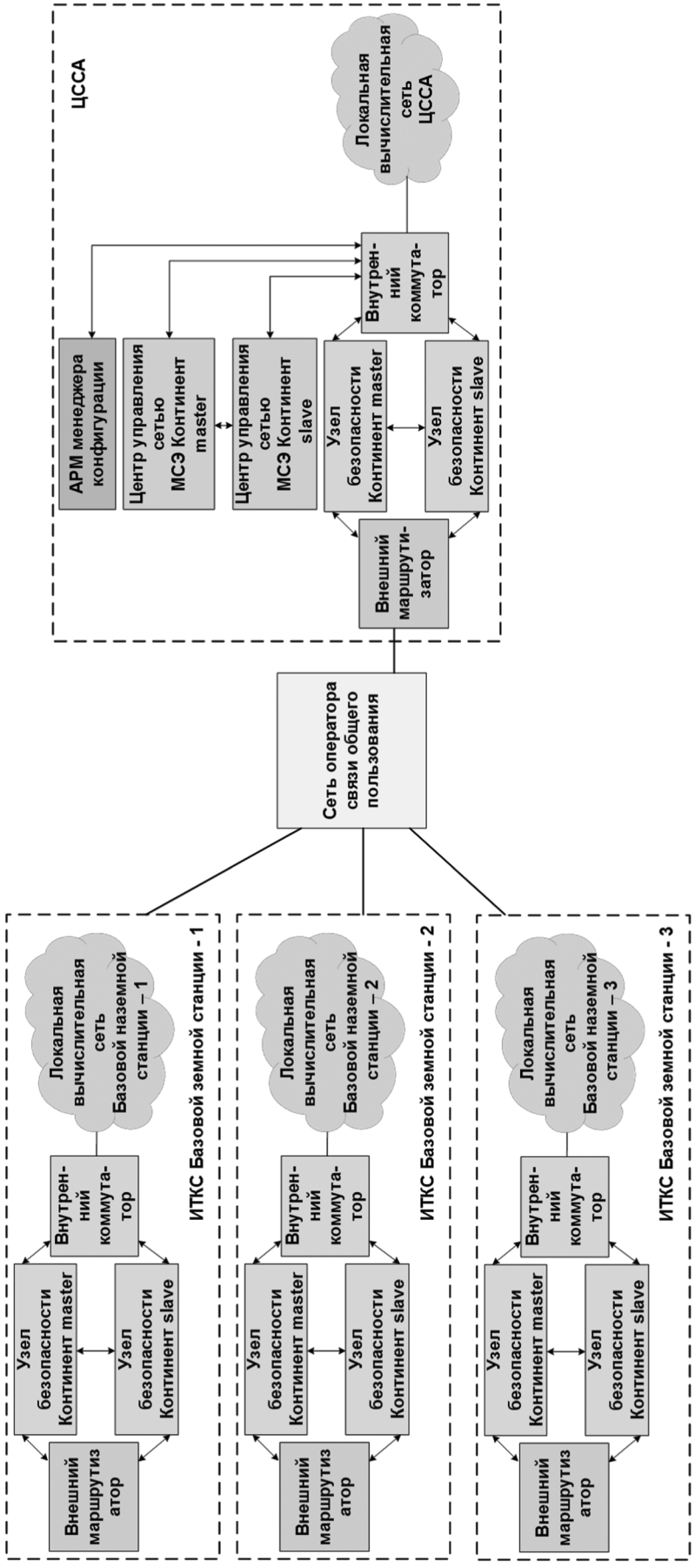


Рис. 2. Схема взаимодействия отказоустойчивых кластеров межсетевых экранов ЦССА

служат признаком того, что основной межсетевой экран работоспособен. Если пакетов нет слишком долго, считается, что основной межсетевой экран вышел из строя. При этом резервный межсетевой экран временно становится основным (temp master), разблокирует свои интерфейсы и берет на себя все функции по обработке трафика.

Если, после проведения ремонта или замены, основной межсетевой экран становится снова доступен и начинает генерировать пакеты жизни, резервный межсетевой экран возвращается в состояние ожидания. Кроме обмена пакетами жизни, выделенная линия связи между основным и резервным межсетевым экраном используется для синхронизации настроек и обмена информацией о текущих соединениях. [3]

— VPN-туннели. В комплексе «Континент» технология VPN позволяет создать защищенные каналы (туннели) между двумя узлами безопасности. За каждым из узлов безопасности, выполняющим функции шлюза, расположена локальная сеть или сегмент сети. При передаче трафика из одной защищаемой сети в другую в узлах безопасности выполняется шифрование данных до того, как они попадут в туннель, и расшифровка этих данных после того, как они туннель покинут;

В комплексе «Континент» L2VPN представляет собой виртуальный коммутатор, объединяющий сетевые интерфейсы узлов безопасности в распределенный сетевой мост. Сетевые интерфейсы узлов безопасности выполняют функции портов коммутации сетевого моста.

При добавлении портов разных узлов безопасности в один виртуальный коммутатор между такими узлами безопасности автоматически создаются VPN-туннели, обеспечивающие безопасную передачу Ethernet-кадров.

Между портами виртуального коммутатора осуществляется прозрачное прохождение служебного трафика по протоколам STP, RSTP, MSTP, MVRP, LACP, LLDP. Предусмотрено объединение портов узла безопасности в сетевой мост (bridge), который в свою очередь может быть включен в состав виртуального коммутатора. [4]

— шифрование информации. В VPN комплекса «Континент» используется криптографическая система, поддерживающая симметричное шифрование. Защищенное соединение между двумя узлами безопасности в сети осуществляется на ключах парной связи. Для шифрования данных используется алгоритм ГОСТ Р 34.12–2018 (Магма) в режиме гаммирования с обратной связью по шифртексту по ГОСТ Р 34.13–2018. Имитозащита данных осуществляется на базе ГОСТ Р 34.12–2018 (Магма) в режиме выработки имитовставки.

2. Сеть доступа НСК. Для обеспечения безопасности в сети доступа будут развернуты следующие элементы:

— в отказоустойчивом кластере узла безопасности необходимо настроить правила межсетевого экранирования;
— в отказоустойчивом кластере центра управления сетью необходимо развернуть центр сертификации, который включает в себя:
— службу корневых сертификатов, которая осуществляет выпуск, пере выпуск и экспорт корневых сертификатов;
— службу действующих сертификатов, которая подписывает запросы, осуществляет отзыв и экспорт выданных сертификатов;
— службу отозванных сертификатов, которая осуществляет просмотр, экспорт и публикацию CRL.

Управление корневыми, выданными и отозванными сертификатами, так же, как и настройка центра сертификации, выполняются только средствами удаленного управления. Принцип функционирования службы сертификатов и ключей безопасности в ЦССА и базовой земной станции представлена на рисунке 3.

3. Объектовая сеть НСК. Объектовая сеть ЦССА и базовой земной станции предназначена для обеспечения прохождения информации от всех элементов локальной вычислительной сети ЦССА и базовой земной станции.

Для обеспечения функционирования безопасности объектовых сетей необходимо:

— развернуть домен ИТКС с правами разграничения доступа;
— выдать сертификаты (TLS) с отказоустойчивого кластера центра управления сетью.

2. Анализ специального программного обеспечения для управления компонентами

2.1. Менеджер конфигурации для управления Континентом 4 (Код Безопасности)

Менеджер конфигурации представляет собой программное средство, устанавливаемое на автоматизированное рабочее место (далее — АРМ) для управления политиками безопасности комплекса «Континент».

Функциональные возможности:

— управление узлами безопасности;
— администрирование комплекса;
— учет конфигураций узлов;
— перезагрузку и выключение узлов безопасности;
— диагностика работы комплекса. [7]

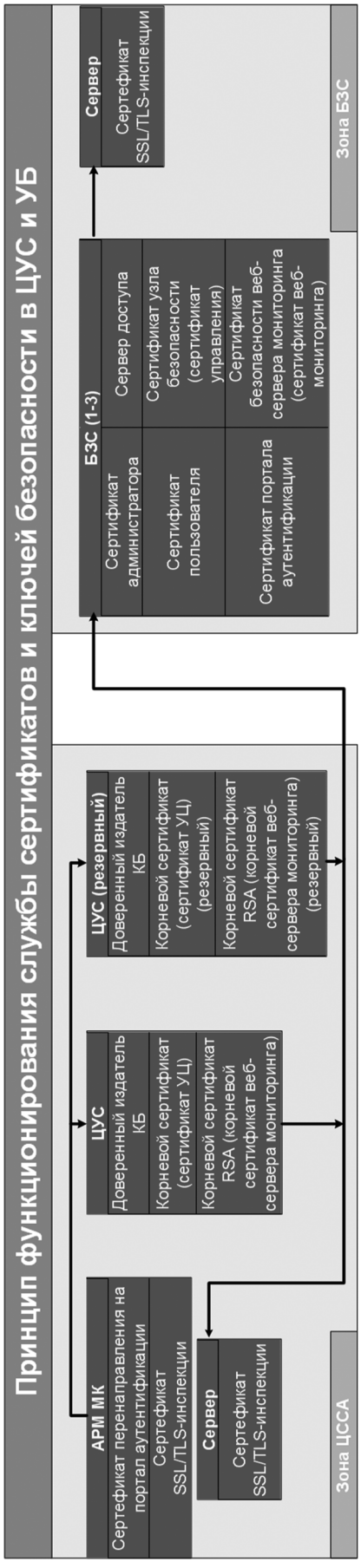


Рис. 3. Принцип функционирования службы сертификатов и ключей безопасности в ЦССА и базовой земной станции

2.2. ECCM для управления сетевым оборудованием (Eltex)

ECCM (Eltex Cloud Configuration Manager) — система, предназначенная для инвентаризации, управления и мониторинга сетевого оборудования Eltex. Автоматизирует задачи по конфигурированию и обновлению оборудования, осуществляет непрерывный мониторинг работы сети для быстрого реагирования и устранения возникающих неисправностей.

Функциональные возможности:
- выполнение операций на отдельных устройствах: перезагрузка, обновление ПО, редактирование конфигурации;
- подключение к устройству с помощью эмулятора терминала;
- группировка устройств и ограничение доступа пользователей;
- отслеживание состояния устройств в реальном времени;
- сбор, хранение и анализ инвентарных данных и метрик с устройств;
- прием, фильтрация и анализ Syslog-сообщений устройств. [8]

2.3. Континент TLS-сервер (Код Безопасности)

TLS-сервер предназначен для обеспечения доступа удаленных пользователей к защищаемым ресурсам в локальной сети с шифрованием трафика между рабочими местами пользователей и TLS-сервером.

Сервер решает следующие задачи:
- подключение удаленных пользователей и установление защищенного соединения после успешной двусторонней аутентификации с использованием несимметричной криптографии;
- защита передаваемых данных с использованием сертифицированных отечественных криптографических алгоритмов.

Функциональные возможности:
- настройка параметров журналирования;
- управление сертификатами безопасности;
- настройка оповещений;
- управление лицензиями.

2.4. Единый центр управления Dallas Lock

ЕЦУ Dallas Lock — это единый кросс-платформенный центр управления.

Функциональные возможности:
- централизованное управление решениями продуктовой линейки Dallas Lock;
- удаленная настройка, а также сбор журналов и отчетов с рабочих станций и серверов;
- контроль целостности настроек сетевого оборудования по протоколам SNMP и SSH и сбор событий по Syslog;
- интеграция со сторонними продуктами:
  а) Антивирус Kaspersky;
  б) SIEM-системы;
  в) Active Directory.

В результате анализа можно сделать вывод, что специальное программное обеспечения не обеспечивают управление компонентами различных производителей. Это ограничение может привести к снижению быстрого реагирования на инциденты и их нейтрализации. Важно учитывать этот фактор при выборе специальное программное обеспечения, особенно в контексте необходимости взаимодействия с многообразием аппаратных и программных решений.

Характер задач и условий управления программным обеспеченьем информационной безопасностью в наземной информационно-телекоммуникационной сети среднеорбитальной системе спутниковой связи «СКИФ» определяет проблему оптимизации управления. Принятия наиболее целесообразного и обоснованного решения в этих условиях — задача весьма сложная, что обусловлено рядом обстоятельств:
- неполнотой и недостоверностью сбора информации от СЗИ;
- сложностью и ограниченными возможностями СЗИ противодействия инцидентами информационной безопасностью в корпоративных и глобальных сетях связи;
- ограниченными по времени и ресурсам алгоритмов противодействия, возникающим угрозам информационной безопасностью, исходящих как из внешней сети так из локальных сетей объекта размещения.

3. Выбор оптимального специального программного обеспечения

В связи с этим, условиями оптимального управления процессом обеспечения информационной безопасностью будут являться:

1. Управляющие воздействия, вырабатывающиеся на основе информации о состоянии объектов управления и внешней среды. Чем большей информацией располагает управляющий объект, находящийся в ЦССА, тем более обоснованным и эффективным будет решение по нейтрализации угроз информационной безопасности.

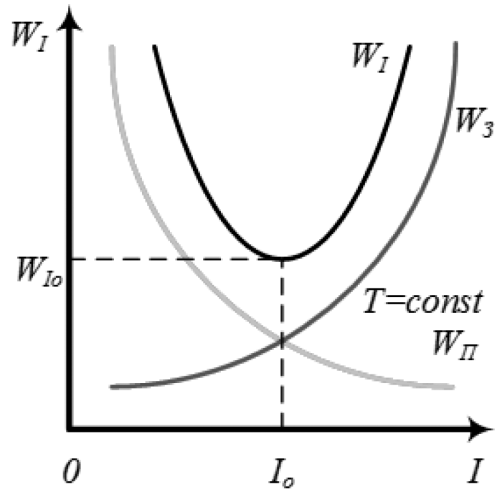
$$W_{lo} = \min (W_{П} (I) + W_{З} (I)) \text{ при } T = \text{const},$$

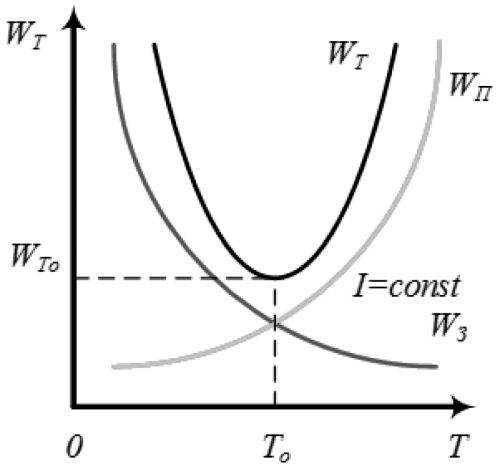
где W_o — оптимальность управления;
$W_П$ — плановая оптимальность управления;
$W_З$ — затраченная оптимальность управления;
T — время;
I — количество информации.

2. Наряду с информированностью управляющий объект большое значение имеет оперативность управления, т. е. оперативность сбора и обработки информации состояния и выработки управляющих воздействий. Поэтому вторым условием оптимальности управления является минимизация временных потерь на реализацию цикла управления.

$$W_{Io} = \min (W_П (I) + W_З (I)) \text{ при } T = \text{const},$$

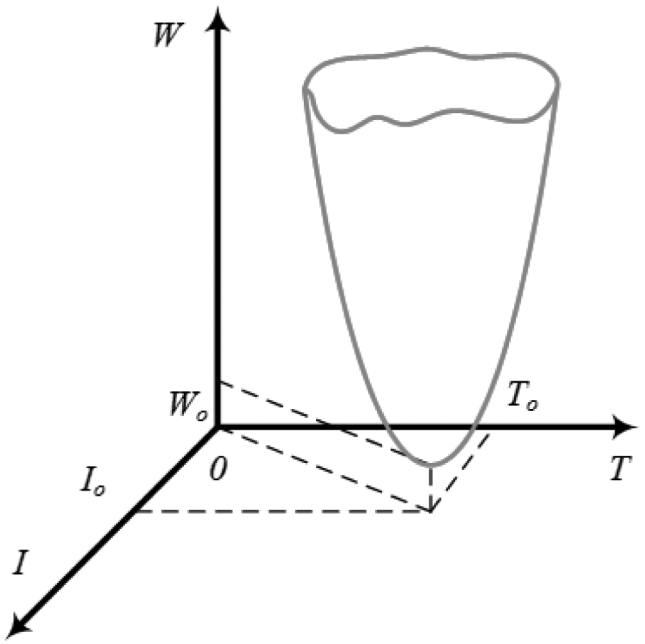
$$W_{To} = \min (W_П (T) + W_З (T)) \text{ при } I = \text{const}.$$





При управлении должны учитываться оба условия оптимального управления.

$$W_О = \min (W_{Io} + W_{To}).$$



Закон соответствия потребного и располагаемого времени при решении задач управления отражает одно из важнейших требований к управлению — его оперативность. Согласно данному закону, в процессе управления следует рассматривать два вида времени — располагаемое и потребное.

Располагаемое время — это то время, в который субъект должен уложиться при осуществлении какого-либо мероприятия, чтобы обеспечить его успех.

Потребное время — это время, которое необходимо затратить при осуществлении данного мероприятия. Благоприятный баланс времени обеспечивается лишь в том случае, если потребное время не превышает располагаемое. В том случае, когда потребное время оказывается больше располагаемого, образуется дефицит времени, который не позволяет выполнить то, что запланировано, с заданной эффективностью.

Закон зависимости эффективности решения задач управления от объема используемой информации выражает устойчивые связи и зависимости между качеством выполнения задач управления и объемом информации, используемой в интересах их решения.[6]

Для оптимизации процессом управления обеспечения информационной безопасностью в наземной информационно-телекоммуникационной сети среднеорбитальной системе спутниковой связи «СКИФ» предлагается использовать специальное программное обеспечения «Центр управления и мониторинга стойкой» 643.СПЕН.24051-01, которое позволит:

— оперативно выводить информацию о состоянии СЗИ и результатах её контроля;

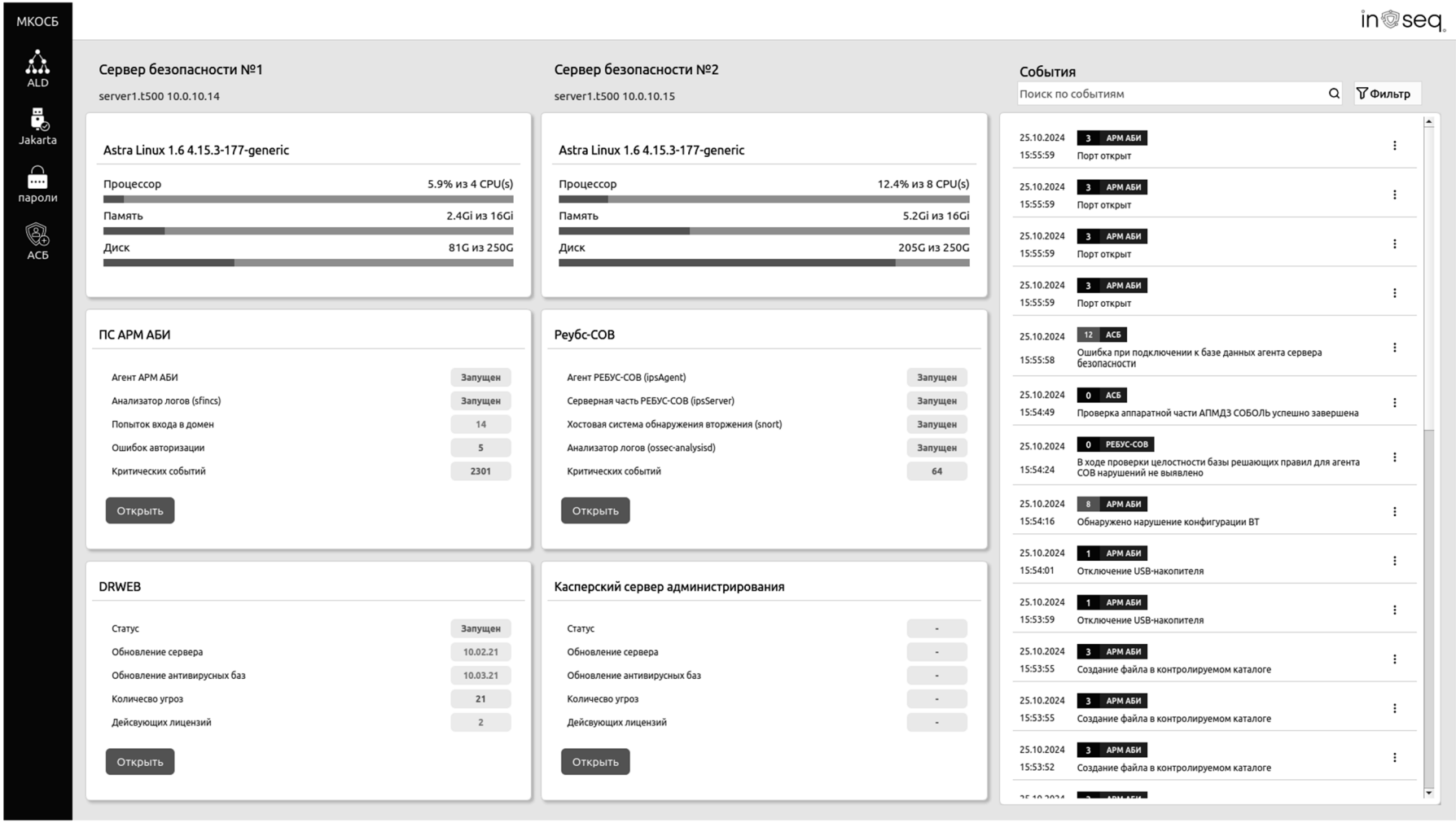


Рис. 4. Специальное программное обеспечения «Центр управления и мониторинга стойкой»

— гибко настраивать параметры выводимой информации и критерий оценки их значимости для обеспечения эффективности принятия решения по выбору алгоритма нейтрализации активных угроз;
— уменьшить время цикла управления по выявлению и устранению инцидента информационной безопасности ИТКС НСК.

Оптимизация рабочего пространства администратора безопасности информации СПО и применение специализированных методик поиска и нейтрализации инцидентов информационной безопасности позволяют сократить время обучения специалистов, а также нагрузку на них в процессе мониторинга ИТКС.

ЛИТЕРАТУРА

1. Проект «Сфера» переходит к практической реализации — Новости — Госкорпорация «Роскосмос» https://www.roscosmos.ru/33771/ (дата обращения: 15.11.2024).
2. Главное. Предприятие Роскосмоса изготовит ещё четыре спутника связи «Скиф» для проекта «Сфера» — Новости — Госкорпорация «Роскосмос» https://www.roscosmos.ru/40598/ (дата обращения: 15.11.2024).
3. Руководство по настройке ПО на базе операционной системы (программной оболочки) Dionis NX С 1.2–10 Hand UTM (2015).
4. Комплекс безопасности «Континент». Версия 4 Руководство администратора. Настройка VPN.
5. Проблемы информационной безопасности в интернете вещей Карев А.С., Бирих Э.В., Сахаров Д.В., Виткова Л.А. В сборнике: Интернет вещей и 5G. 2016. С. 66–70.
6. Технические аспекты управления с использованием сети интернет Алейников А.А., Билятдинов К.З., Красов А.В., Кривчун Е.А., Крысанов А.В. Монография / Санкт-Петербург, 2016.
7. Комплекс безопасности Континент Версия 4 Руководство администратора Управление комплексом.
8. Система управления сетевым оборудованием ECCM https://eltex-co.ru/catalog/eccm (дата обращения: 20.11.2024).