УДК: 004.056.53
Оригинальная статья
Надежность, том 17, №3, 2017 DOI: 10.21683/1729-2646-2017-17-3-32-40

Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий

Сергей М. Климов, *4 ЦНИИ Минобороны России, Россия, Королёв_*
Сергей В. Поликарпов, *4 ЦНИИ Минобороны России, Россия, Королёв*
Андрей В. Федченко, *4 ЦНИИ Минобороны России, Россия, Королёв*

Резюме. Цель. *Целью статьи является разработка методики, позволяющей комплексно экспериментальным, расчетно-аналитическим и экспертным путем оценить уязвимость сетей спутниковой связи, реализуемость информационно-технических воздействий нарушителя на эти уязвимости и вероятность отказоустойчивости при выбранных вариантах средств защиты информации, доверенных информационных технологий и сенсоров отказоустойчивости. В статье показана актуальность и важность методики для повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий на технологические каналы управления и данные спутникового оборудования. Рассмотрены целенаправленные и массированные информационно-технические воздействия, приводящие к нарушению функционирования спутниковых модемов, управляющих станций и подключенных вычислительных сетей потребителей. Показаны особенности функционирования сетей спутниковой связи, связанные с глобальностью зоны обслуживания потребителей на поверхности Земли, доступностью широкополосных радиосигналов от космических аппаратов связи и ретрансляции для технического анализа и обработки в зоне обслуживания потребителей, потенциальной возможностью несанкционированного подключения к услугам связи. Определены основные перспективные направления развития методического и технологического обеспечения защищенности и отказоустойчивости сетей спутниковой связи.* **Методы.** *Разработана методика, основанная на трех компонентах: модели экспериментального выявления уязвимостей сетей спутниковой связи; имитационной, расчетно-аналитической модели обнаружения и идентификации угроз информационно-технических воздействий; алгоритме принятия решения по повышению отказоустойчивости сети спутниковой связи в условиях информационно-технических воздействий. Модель экспериментального выявления уязвимостей сетей спутниковой связи позволяет в ходе стендовых испытаний установить взаимосвязь между существующими уязвимостями аппаратно-программного обеспечения спутниковых модемов, управляющих станций, сетей потребителей услуг связи и потенциальными информационно-техническими воздействиями на них нарушителя. В рамках модели уязвимостей описаны паспорта уязвимых радиотехнических и информационных параметров сигналов сетей спутниковой связи, а также предложено аналитическое выражение для расчета вероятности выявления уязвимостей этих сетей. Представлена расчетно-аналитическая модель обнаружения и идентификации угроз информационно-технических воздействий в виде структуры перспективных средств обнаружения, предупреждения и ликвидации последствий информационно-технических воздействий на сеть спутниковой связи и математическое выражение для определения условной вероятности реализации угроз информационно-технических воздействий на сеть спутниковой связи. Рассмотрен алгоритм повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий, включающий подготовку параметров и проведение оценки отказоустойчивости сети спутниковой связи, регулирование параметров сети спутниковой связи и параметров средств защиты информации и сенсоров обеспечения отказоустойчивости, ситуационное регулирование вариантов отказоустойчивых сетей спутниковой связи.* **Выводы.** *Отмечается, что разработанная методика позволяет повысить отказоустойчивость сети спутниковой связи в условиях информационно-технических воздействий на основе совокупности взаимосвязанных процедур модели экспериментального выявления уязвимостей сети спутниковой связи на стендовом полигоне; имитационной, расчетно-аналитической моделей обнаружения и идентификации угроз информационно-технических воздействий; применения алгоритма принятия решения по повышению отказоустойчивости сети спутниковой связи.*

Ключевые слова: *сети спутниковой связи, уязвимости, информационно-технические воздействия, повышение отказоустойчивости, средства защиты информации, доверенные информационные технологии и сенсоры отказоустойчивости.*

Формат цитирования: *Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий // Надежность. 2017. № 3. С. 32-40. DOI: 10.21683/1729-2646-2017-17-3-32-40.*

Введение

В соответствии с Доктриной информационной безопасности Российской Федерации от 5 декабря 2016 года одним из важнейших направлений обеспечения информационной безопасности в области государственной и общественной безопасности является повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления.

К одним из сложнейших и развивающихся объектов современной критической информационной инфраструктуры, для которых необходимо обеспечить повышенные требования к защищенности и устойчивости от информационно-технических воздействий (ИТВ), относятся сети спутниковой связи (ССС). Например, активно развиваются информационно-телекоммуникационные системы на базе сервисов и услуг интерактивных сетей спутникового Интернета для передачи больших массивов данных на базе открытого стандарта DVB-RCS [1].

При разработке современных моделей и методов обеспечения устойчивости (живучести) информационных сетей в условиях разрушающих информационных воздействий [2] особенности взаимосвязанной оценки реальной защищенности и отказоустойчивости ССС могут быть учтены в форме предлагаемой методики повышения отказоустойчивости ССС в условиях ИТВ.

Целенаправленные и массированные ИТВ на протоколы передачи данных являются угрозой для нарушения защищенности и устойчивости функционирования ССС, что обусловливает необходимость разработки методик и средств обнаружения, предупреждения и ликвидации последствий этих информационных угроз на основе повышения отказоустойчивости этих сетей [3, 5].

В настоящее время наиболее опасны ИТВ, которые скрытно проникают, распространяются, вызывают сбои (отказы) и наносят ущерб информационным ресурсам ССС.

Особенностями функционирования ССС, прежде всего, на базе космических аппаратов (КА), находящихся на геостационарной орбите, являются:

- глобальность зоны обслуживания потребителей на поверхности Земли (например, КА «Ямал 401», обслуживающий территорию Российской Федерации в целом и сопредельные территории);

- доступность широкополосных радиосигналов от КА связи и ретрансляции для технического анализа и обработки в зоне обслуживания потребителей;

- потенциальная возможность несанкционированного подключения к услугам связи на расстоянии до 10 тысяч километров между абонентами, как с территории Российской Федерации, так и сопредельных государств;

- сетевая иерархическая инфраструктура ССС с территориально распределенными абонентами, взаимодействующими через разнородные КА связи и ретрансляции и наземные сети по стандартизированным протоколам передачи данных.

В статье используются следующие основные термины:

- уязвимости ССС – программные, архитектурные или логические недостатки в ССС, используя которые возможно получить несанкционированный доступ к защищаемой информации, нарушить ее целостность и доступность, а также вызвать нештатное функционирование ССС;

- информационно-техническое воздействие (компьютерная атака) – целенаправленное воздействие на автоматизированные, информационные и информационно-телекоммуникационные системы программно-техническими средствами, осуществляемое в целях нарушения функционирования и безопасности информации в ССС;

- методика повышения отказоустойчивости ССС – совокупность моделей и алгоритмов анализа, выявления уязвимых мест ССС, обнаружения угроз ИТВ, экспериментальной, расчетно-аналитической и экспертной оценки реальной отказоустойчивости ССС в условиях ИТВ.

Основные перспективные направления развития методического и технологического обеспечения защищенности и отказоустойчивости ССС включают в свой состав разработку:

- имитаторов угроз целенаправленных и массированных ИТВ для проверки ССС;

- методик, алгоритмов и средств обнаружения, предупреждения и ликвидации последствий ИТВ на ССС;

- стендовых полигонов испытаний ССС в условиях ИТВ;

- учебно-тренировочных средств на базе технологий виртуализации, облачных вычислений и сетевых компьютерных игр по противодействию ИТВ на ССС;

- проведение компьютерных учений по отработке действий операторов ССС в условиях чрезвычайных угроз целенаправленных и массированных ИТВ.

Постановка задачи

Предлагаемая в статье методика базируется на взаимосвязанной совокупности экспериментальных оценок реальной отказоустойчивости ССС в условиях имитации ИТВ нарушителя, расчетно-аналитических и экспертных оценок достигаемой отказоустойчивости ССС при выбранных вариантах, доверенных информационных технологий (ДИТ), средств защиты информации (СЗИ) и сенсоров отказоустойчивости (обнаружения, предупреждения и ликвидации последствий ИТВ).

Методика повышения отказоустойчивости ССС состоит из следующих моделей и алгоритма:

1. Модели экспериментального выявления уязвимостей ССС.

2. Имитационной, расчетно-аналитической моделей обнаружения и идентификации угроз ИТВ.

3. Алгоритма принятия решения по повышению отказоустойчивости ССС в условиях ИТВ.

На рисунке 1 приведена схема модели экспериментального выявления уязвимостей ССС. Она представ-

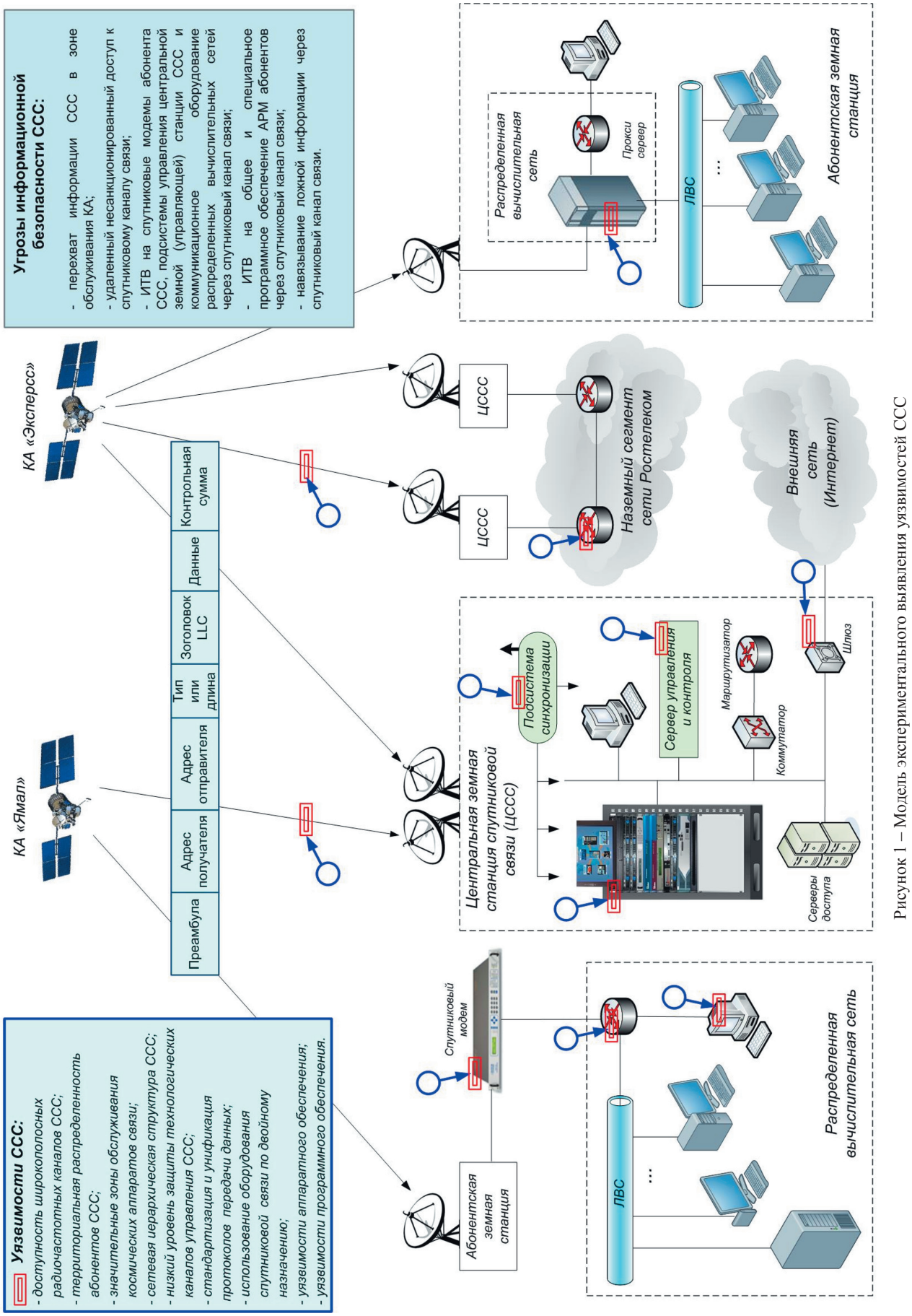

Рисунок 1 – Модель экспериментального выявления уязвимостей ССС

ляет собой типовую критическую информационную инфраструктуру ССС с характерными уязвимостями территориально распределенных объектов, которые взаимодействуют между собой через КА связи и ретрансляции, а также наземные магистральные сети. Уязвимостям ставятся в соответствие потенциальные ИТВ.

Главной уязвимостью являются стандартные и открытые протоколы передачи данных ССС, которые недостаточно защищены в технологических каналах управления и синхронизации. Высокая связность разнородных сегментов нескольких ССС создает возможность несанкционированного доступа к объектам воздействия, не являющихся элементом отдельной ССС.

Экспериментальное выявление уязвимостей ССС осуществляется путем практической проверки (тестирования) доступности протоколов управления и информационного обмена для технического анализа радиотехнических параметров и вскрытия информационных параметров широкополосных сигналов каналов передачи данных в ходе пассивного и активного сканирования.

На схеме двойной, красный прямоугольник обозначает уязвимость, а синяя стрелка с кругом – ИТВ. Рассматриваемая модель экспериментального выявления уязвимостей ССС, позволяет предварительно оценить доступность ССС с используемыми информационными технологиями и СЗИ для потенциальных ИТВ. Экспериментальные исследования проводятся на реальных каналах передачи данных ССС с использованием частотных ресурсов КА связи и ретрансляции, оборудования имитации спутниковых каналов связи между управляющей станцией и абонентами с учетом особенностей технологического цикла управления, а также с привлечением стендовой базы.

Таблица 1 – Пример паспорта уязвимых радиотехнических параметров сигналов ССС

Элементы описания уязвимых радиотехнических параметров	Описание уязвимых радиотехнических параметров ССС
Идентификатор сигнала	алфавитно-цифровая последовательность, идентифицирующая радиочастотный сигнал в базе данных
Наименование космического аппарата связи и ретрансляции	Ямал-401
Орбитальная позиция	90 в.д.
Значение частоты переноса	3050 МГц
Уровень сигнала	-34 дБм
Центральная частота	11245 МГц
Частотная полоса	20 МГц
Вид поляризации	горизонтальная (линейная)
Вид модуляции	QPSK
Тип многостанционного доступа	MF-TDMA
Тип помехоустойчивого кодера	5/6
Тип турбокодера	Рида-Соломона
Скремблирование	не используется
Мультиплексирование	Да

В рамках моделирования комплекс технических и программных средств стендовой базы позволяет проводить технический анализ радиотехнических и информационных параметров ССС, имитировать ИТВ, помеховую обстановку в соответствии с разработанными сценариями и исходными данными. Стенд для экспериментальной оценки защищенности ССС в условиях ИТВ должен содержать антенные системы различных диапазонов частот, приемо-передающие устройства, демодуляторы, программно-алгоритмическое обеспечение, реализующие технологию реальной работы ССС в условиях ИТВ.

В итоге модель обеспечивает формирование перечня выявленных уязвимостей ССС.

Паспорт уязвимых радиотехнических параметров сигналов ССС, доступных для технического анализа нарушителем, представлен в таблице 1.

Аналитическое выражение для расчета вероятности выявления уязвимостей ССС по результатам экспериментальных исследований с использованием [3–5] имеет вид:

$$P_{\text{уяз}}^{\text{ССС}}\left(t_{\text{ск}}\right) = P_{\text{НСД}}^{\text{ССС}}\left(t_{\text{ск}}\right) + \left(1 + P_{\text{НСД}}\left(t_{\text{ск}}\right)\right) \cdot P_{\text{ПСК}}\left(t_{\text{ск}}\right) + \\ + \left(1 - P_{\text{НСД}}\left(t_{\text{ск}}\right)\right) \cdot P_{\text{АСК}}\left(t_{\text{ск}}\right), \quad (1)$$

где $P_{\text{НДС}}(t_{\text{ск}})$ – вероятность наличия точек несанкционированного доступа в каналах передачи данных между абонентами ССС в направлениях «борт КА – Земля» (обратный уязвимый канал с доступными широкополосными сигналами) и «Земля – борт КА»;

$P_{\text{ПСК}}(t_{\text{ск}})$ – вероятность пассивного сканирования каналов передачи данных между абонентами ССС за время $t_{\text{ск}}$;

$P_{\text{АСК}}(t_{\text{ск}})$ – вероятность активного сканирования каналов передачи данных между абонентами ССС за время $t_{\text{ск}}$.

Паспорт уязвимых информационных параметров каналов передачи данных ССС представим с использованием ГОСТ Р 56546-2015 (таблица 2).

Имитационная, расчетно-аналитическая модели обнаружения и идентификации угроз ИТВ на ССС определяют перечень угроз информационной безопасности ССС, который соответствуют структуре протокола передачи данных между управляющей станцией и абонентским сегментом, а также элементам ССС. Имитационная модель угроз ИТВ позволяет вскрыть уязвимости протоколов, возможные способы реализации угроз ИТВ на них и последствия от нарушения безопасности информации ССС.

Наличие потенциальных уязвимостей и угроз реализации ИТВ на ССС обусловливает возможность несанкционированного подключения к сети и перехвата информации.

Таблица 2 – Пример паспорта уязвимых информационных параметров ССС

Элементы описания уязвимых информационных параметров ССС	Описание уязвимых информационных параметров ССС
1. Наименование уязвимости	Уязвимость протокола управления спутникового модема
2. Идентификатор уязвимости	УСМ-2017-00002
3. Краткое описание уязвимости	Уязвимость допускает перехват канала управления программным обеспечением спутникового модема
4. Класс уязвимости	Уязвимость программного обеспечения спутникового модема
5. Наименование уязвимого элемента и его версия	Программное обеспечение спутникового модема версии 7.34
6. Протокол передачи данных	Протокол управления telnet, прямой доступ к средствам управления спутникового модема
7. Особенности аппаратной и программной реализации	Аппаратно-программная платформа основана на технологиях клиент-сервер, протокол передачи данных TCP/IP версии v.4.0
8. Тип недостатка	Недостатки, связанные с аутентификацией администратора
9. Место возникновения (проявления) уязвимости	Уязвимость существует из-за отсутствия проверки легитимности источника команд управления спутниковым модемом
10. Идентификатор типа недостатка	Нет данных
11. Дата выявления уязвимости	1.03.2017
12. Автор, опубликовавший информацию о выявленной уязвимости	Подразделение информационной безопасности
13. Способ (правило) обнаружения уязвимости	Выполнение пошаговой инструкции
14. Критерии опасности уязвимости	Превышение установленного значения вероятности риска
15. Степень опасности уязвимости	Высокая
16. Возможные меры по устранению уязвимости	Доработка средств защиты информации и протоколов управления спутниковым модемом
17. Дополнительные сведения	В сети используется спутниковые модемы, допускающие удаленную перезагрузку программного обеспечения через ССС

Схема модели обнаружения и идентификации угроз ИТВ на ССС создается в форме структуры оперативного реагирования на ИТВ и повышения отказоустойчивости, состоит из трех контуров (рисунок 2):

- первый – ДИТ ССС;
- второй – управления защитой информации и повышением отказоустойчивости на основе информации от сенсоров средств обнаружения и идентификации ИТВ;
- третий – оповещения о нарушении информационной безопасности по типовой форме описания компьютерных инцидентов.

Элементы ДИТ ССС представляют собой защищенные аппаратно-программные платформы, включающие операционные системы (ОС), системы управления базами данных (СУБД), трансляторы с языков программирования высокого уровня и другое общее программное обеспечение. Аппаратная составляющая ДИТ ССС включает защищенные процессоры, модули памяти, интерфейсные шины, спутниковые модемы, управляющие станции, доверенное коммуникационное оборудование наземных распределенных сетей, которые в совокупности должны позволить сформировать неуязвимое спутниковое и коммуникационное оборудование в условиях ИТВ.

В модели обнаружения и идентификации угроз ИТВ, с одной стороны, к средствам защиты информации (СЗИ) относятся известные СЗИ, такие как автоматизированные модули доверенной загрузки (АМДЗ), межсетевые экраны (МЭ), ложные сетевые информационные объекты (ЛСИО), а с другой стороны – совокупность сенсоров, которые реализуют функции обнаружения, предупреждения и ликвидации последствий ИТВ. Для повышения отказоустойчивости ССС в условиях ИТВ совокупность сенсоров регистрируют и идентифицируют факты воздействий и формируют исходные данные для восстановления работоспособности ССС.

Элементы СЗИ ССС целесообразно реализовать на основе аппаратно-программных средств пункта мониторинга ИТВ и управления защитой информации.

В рамках повышения отказоустойчивости ССС анализируются потенциальные угрозы нарушения защищенности и отказоустойчивости ССС, потенциальные объекты поражения, ДИТ ССС, комплекс СЗИ и необходимый стендовый полигон испытаний ССС в условиях ИТВ.

Особенности повышения отказоустойчивости ССС в условиях ИТВ состоят в том, что требуемый ее уровень необходимо обеспечить в течение длительного периода эксплуатации при совершенствующихся угрозах нарушителей, в технологических трактах систем управления с различными протоколами передачи данных.

Порядок обнаружения и идентификации угроз ИТВ на ССС следующий:

1. Устанавливается сервер обнаружения ИТВ на центральной управляющей (земной) станции, размещаются сенсоры отказоустойчивости на подключенных абонентских управляющих станциях (терминалах) и осуществляется мониторинг защищенности ССС.

I	Доверенные информационные технологии
	Защищенные отечественные платформы на базе процессоров Эльбрус и Байкал
	Операционные системы ряда Astra Linux
	СУБД PostgreSQL
	Транслятор с языка программирования C++

II	Комплекс средств защиты информации и сенсоров отказоустойчивости
	Сервер обнаружения ИТВ
	Сенсоры отказоустойчивости ССС
	Межсетевые экраны
	Средства антивирусной защиты
	Аппаратно-программные средства доверенной загрузки

III	Оповещение о компьютерных инцидентах
	Ситуационный пункт мониторинга ССС

Средства обеспечения отказоустойчивости и ликвидации последствий ИТВ на ССС

Рисунок 2 – Схема модели обнаружения и идентификации угроз ИТВ

2. Производится первоначальное извещение о появлении незарегистрированного абонента в случае несанкционированного подключения нарушителя к ССС с активным использованием нештатного спутникового модема.

3. Осуществляется извещение о компьютерном инциденте при реализации ИТВ на абонентов и управляющую станцию ССС сенсорами отказоустойчивости на основе использования встроенных сигнатурных и эвристических методов.

4. Выполняется анализ целенаправленных и массированных ИТВ, идентификация их типа и обновление баз данных сигнатур ИТВ.

5. Принимаются решения о ликвидации последствий ИТВ путем блокирования спутникового модема нарушителя на основе контроля параметров прямого и обратного спутниковых каналов, информации от сенсоров отказоустойчивости.

Мониторинг защищенности ССС с целью обнаружения и идентификации ИТВ осуществляется следующими проверочными мероприятиями:

- контроль радиотехнических параметров;
- контроль каналов управления ССС;
- контроль параметров подключения и функционирования абонентов ССС;
- контроль информационных потоков в ССС;
- обнаружение открытых каналов управления и передачи данных;
- обнаружение ИТВ в прямом и обратном каналах ССС;
- локализация нарушителя (идентификация источника ИТВ и определение предполагаемого местоположения);
- блокирование нарушителя (отключение от ССС);
- технический анализ и выявление уязвимостей ССС;
- контроль параметров функционирования спутникового оборудования центральной и абонентских станций, коммуникационного оборудования, аппаратно-программного обеспечения, средств защиты информации и повышения отказоустойчивости.

Расчетно-аналитическая модель основана на математическом выражении для определения условной вероятности реализации угроз ИТВ на ССС (с использованием [3–5]):

$$P(S_{\text{Р}}/Y_{\text{ИТВ}})=\frac{P(S_{\text{Р}i})\cdot P(Y_{\text{ИТВ}i}/S_{\text{Р}j})}{P(S_{\text{Р}j})\cdot P(Y_{\text{ИТВ}i}/S_{\text{Р}j})+P(S_{\text{Н}k})\cdot P(Y_{\text{ИТВ}i}/S_{\text{Н}k})}, \quad (2)$$

где $P(S_{\text{Р}})$ – вероятность нахождения ССС в работоспособном состоянии в условиях ИТВ;

$P(Y_{\text{ИТВ}i}/S_{\text{Р}j})$ – условная вероятность реализации i-й угрозы ИТВ на j-й работоспособный элемент ССС;

$P(S_{\text{Н}k})$ – вероятность нахождения k-го элемента ССС в неработоспособном состоянии при реализации ИТВ;

$P(Y_{\text{ИТВ}i}/S_{\text{Н}k})$ – условная вероятность реализации i-й угрозы ИТВ на k-й элемент ССС, приводящей к нарушению его отказоустойчивости.

На рисунке 3 представлен алгоритм повышения отказоустойчивости ССС в условиях ИТВ.

Алгоритм обеспечения отказоустойчивости ССС основан на совокупности экспериментальных, расчетно-аналитических и экспертных оценках параметров ССС в условиях ИТВ для выбора вариантов отказоустойчивых ССС путем их ситуационного регулирования.

Сущность алгоритма обеспечения отказоустойчивости ССС в условиях ИТВ заключается в реализации пяти этапов:

1. Подготовка параметров (исходных данных) для оценки отказоустойчивости ССС в условиях ИТВ.
2. Проведение оценки реальной защищенности ИТВ.
3. Регулирование параметров ССС.
4. Регулирование параметров СЗИ и средств обеспечения отказоустойчивости.
5. Ситуационное регулирование вариантов отказоустойчивых ССС.

Алгоритм обеспечения отказоустойчивости ССС в условиях ИТВ, по сути, определяет схему поэтапного управления отказоустойчивостью сети, выбора наименее уязвимого и наиболее защищенного варианта ССС с возможностью ликвидации последствий ИТВ.

Технологический цикл управления (ТЦУ) ССС характеризуется реальным масштабом времени, динамически изменяющимися условиями ИТВ, использованием значительного числа ДИТ, что требует ситуационного регулирования параметров отказоустойчивости ССС адекватно складывающейся обстановке.

Предполагается, что в начальной стадии работы алгоритма существует неопределённость исходных данных об ИТВ, уязвимостях ССС, ДИТ, СЗИ и сенсорах отказоустойчивости, что обусловливает необходимость проведения экспериментальных и аналитических исследований по обеспечению отказоустойчивости ССС в условиях ИТВ.

Применение алгоритма предполагается как на этапах проектирования и разработки ССС в защищенном исполнении, так и регулирования параметров и средств обеспечения отказоустойчивости ССС в условиях эксплуатации.

Выполнение этапов алгоритма по управлению отказоустойчивостью ССС в условиях ИТВ позволяет осуществить:

- подготовку входных данных и учет факторов для оценки отказоустойчивости ССС в условиях ИТВ;
- имитационное моделирование реальных процессов функционирования ССС на стендовом полигоне;
- инструментальный контроль потенциальных возможностей нарушителя по проведению пассивного и активного сканирования уязвимостей ССС;
- регулирование параметров ССС, СЗИ, ДИТ и сенсоров отказоустойчивости по результатам расчетно-аналитических и экспертных оценок;
- ситуационное регулирование вариантов отказоустойчивых ССС при динамически изменяющихся ИТВ на основе устранения уязвимостей в аппаратно-программных средствах, выбора вариантов отказоустойчивых элементов ССС, СЗИ и сенсоров отказоустойчивости;

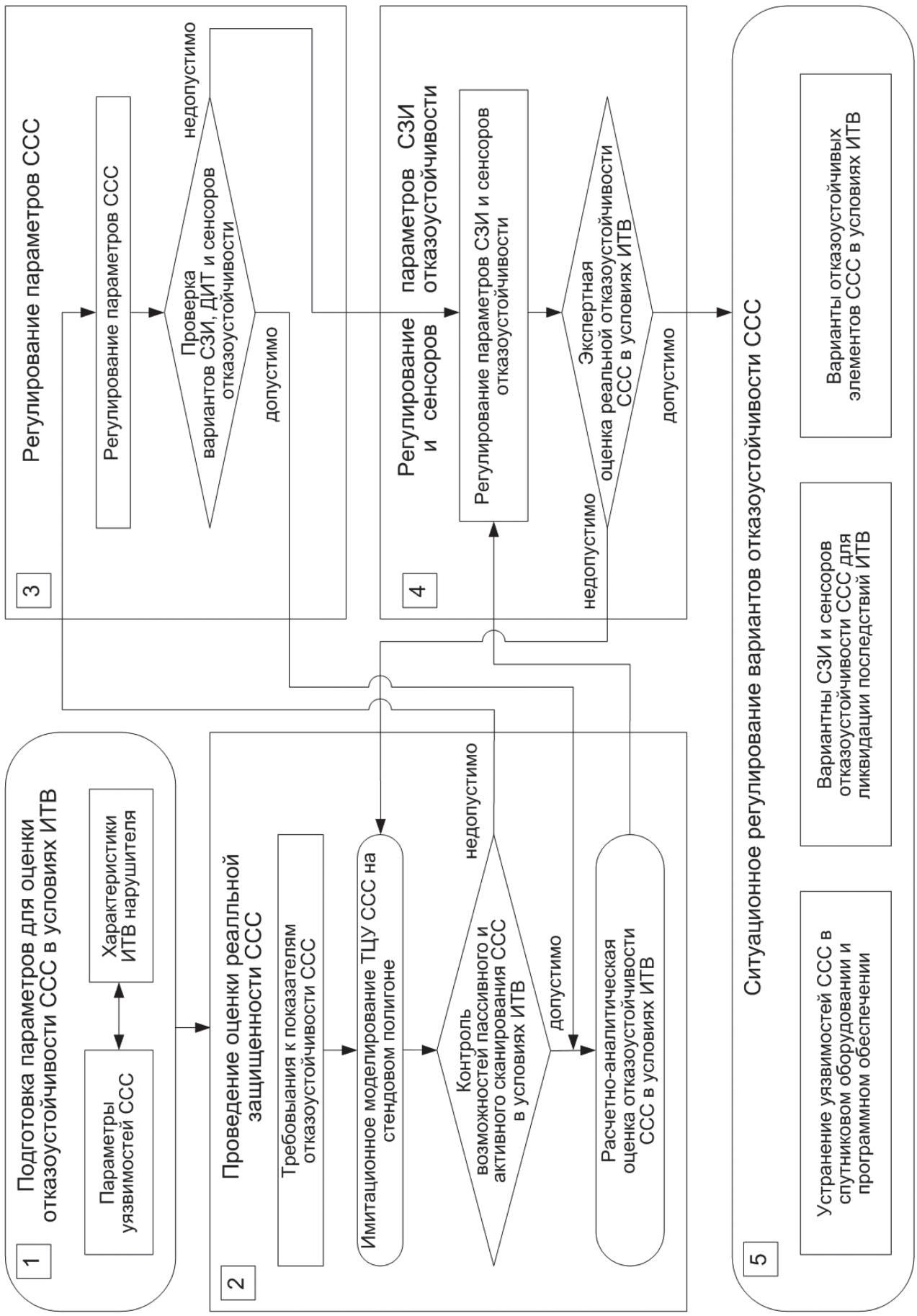

Рисунок 3 – Алгоритм обеспечения отказоустойчивости ССС в условиях ИТВ

- выбор моделей ССС, ИТВ, СЗИ, ДИТ, сенсоров отказоустойчивости для определения мер по повышению (обеспечению) функциональной устойчивости ССС;

- комплексную экспериментальную, расчетную и экспертную оценку отказоустойчивости ССС в условиях ИТВ;

- подготовку к ликвидации последствий ИТВ на ССС;

- эффективное управление отказоустойчивостью ССС в условиях неопределенности ИТВ и внесения различных замедлений в процесс выполнения ТЦУ по предоставлению услуг спутниковой связи и передачи данных;

- оценку выполнения предъявляемых требований к показателям отказоустойчивости ССС в условиях ИТВ и выдать практические рекомендации по ее обеспечению.

Множество различных параметров ССС, СЗИ, ДИТ, сенсоров отказоустойчивости и факторов ИТВ приводит к множеству возможных текущих состояний отказоустойчивости ССС. Количество вариантов регулирования (управляющих решений) по повышению отказоустойчивости ССС на практике ограничено. В этих условиях рассмотренный алгоритм на основе ситуационного регулирования вариантов отказоустойчивости ССС позволяет обеспечить выполнение требований к отказоустойчивости ССС.

Под ситуацией понимается совокупность уязвимостей и состояний ССС, СЗИ, ДИТ и сенсоров отказоустойчивости на определенный момент функционирования для определения необходимости вмешательства в процесс управления ССС.

При выполнении процедур контроля, проверки и экспертной оценки параметров отказоустойчивости ССС в условиях ИТВ, предполагается, что с использованием базы данных испытаний стендового полигона в ходе принятия решений на этапах выполнения алгоритма устанавливаются факты допустимого и недопустимого отклонения параметров текущего состояния ССС от требуемого значения.

Интервал регулирования состояния отказоустойчивости ССС выбирается исходя из значимости абонентов и узлов (управляющих станций) ССС и наиболее вероятной реализацией ИТВ.

Если состояние ССС в условиях ИТВ требует ситуационного регулирования, то ее описание классифицируется на основе паспортов радиотехнических и информационных параметров ССС, профиля нормального поведения и результатов расследования компьютерных инцидентов. Каждое текущее состояние ССС в условиях ИТВ можно отнести к определенному классу, которому соответствует некоторое множество регулируемых параметров ССС.

Ситуационное регулирование отказоустойчивости ССС характеризуется следующей последовательностью: описание состояния ССС в условиях ИТВ – подготовки регулируемых параметров ССС, СЗИ, ДИТ, сенсоров отказоустойчивости – реализация управляющих воздействий по противодействию ИТВ и восстановлению работоспособности (переходу на резервные сегменты) ССС.

Расчетное соотношение для вероятности отказоустойчивости ССС в условиях ИТВ с использованием [3–5] имеет вид:

$$P_{\text{отк}}(t)=\prod_{i=1}^{k}\left[1-\left(1-\prod_{j=1}^{r}P_{\text{БОТ}i}\left(S_{\text{Р}j}\right)\right)\right], \qquad (3)$$

где $P_{\text{БОТ}i}(S_{\text{Р}j})$ – вероятность безотказной работы j-го элемент ССС при i-й угрозе ИТВ;

k – общее количество элементов СЗИ (сенсоров), размещенных в ССС;

r – общее количество резервных элементов ССС.

Заключение

На базе системного анализа потенциальных уязвимостей и особенностей функционирования ССС в статье предложена методика повышения отказоустойчивости ССС в условиях возможных ИТВ. Методика основана на совокупности взаимосвязанных процедур модели экспериментального выявления уязвимостей ССС на стендовом полигоне, формирования имитационной, расчетно-аналитической моделей обнаружения и идентификации угроз ИТВ и применения алгоритма принятия решения по повышению отказоустойчивости ССС в условиях ИТВ.

Библиографический список

1. Воронин А.В, Иванов В.Н., Сотов А.М, Цифровое телевизионное вещание/ Под редакцией доктора технических наук, профессора А.М. Сомова – М.: Горячая линия – Телеком, 2017. – 240 с.: ил. – Серия «Цифровое телевизионное и радиовещание. Выпуск 1».

2. Величко В.В., Попков Г.В., Попков В.К. Модели и методы повышения живучести современных систем связи. – М.: Горячая линия – Телеком, 2016. – 270 с.: ил.

3. Климов С.М., Астрахов А.В., Сычев М.П. Экспериментальная оценка противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 116 с, 2013.

4. К. Капур, Л. Ламберсон. Надежность и проектирование систем. Под ред. И.А. Ушакова. Пер. с англ. – М.: «Мир», 1980. – 604 с., ил.

5. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза/ И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2016. – 544 с., ил. – («Журнал надежность»).

Сведения об авторах

Сергей М. Климов – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России. Россия, Королёв, тел. + 7 (985)928-13-55, e-mail: klimov.serg2012@yandex.ru.

Сергей В. Поликарпов – заместитель начальника отдела 4 ЦНИИ Минобороны России. Россия, Королёв, тел. +7 (916)332-60-66, e-mail: polikarpov.s.v@yandex.ru.

Андрей В. Федченко – начальник отдела 4 ЦНИИ Минобороны России. Россия, Королёв, тел. +7 (916)334-87-89, e-mail: fedchandr@yandex.ru

Поступила 15.05.2017