УДК 631.8

**Калмыков Игорь Анатольевич, Пашинцев Владимир Петрович,
Вельц Оксана Владимировна, Калмыков Максим Игоревич**

МЕТОДЫ ЗАЩИТЫ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ ДЛЯ СИСТЕМЫ УДАЛЕННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ ВЫСОКОТЕХНОЛОГИЧЕСКИМИ ОБЪЕКТАМИ

В статье рассмотрены методы защиты передаваемой информации между удаленным объектом и центром поддержки операций системы мониторинга, контроля и управления оборудованием критических технологий. Разработан алгоритм имитозащиты, позволяющей снизить вероятность навязывания ложной информации.

Ключевые слова: Протокол доказательства с нулевым разглашением, методы защиты данных, имитозащита, модулярная арифметика, псевдослучайная функция.

**Kalmykov Igor A., Pashintsev Vladimir P.
Velts Oksana V., Kalmykov Maksim I.**

METHODS FOR TRANSFERRED INFORMATION PROTECTION FOR REMOTE CONTROL SYSTEM AND HI-TECH FACILITY MANAGEMENT

There is a view on the methods for protection of the information transferred between a remote object and the centre for support system monitoring, control, and management of critical technologies. The item offers an imito-protection algorithm reducing the likelihood of imposing false data.

Keywords: zero-knowledge proof protocol; data protection method; modular arithmetics; pseudorandom function.

Дистанционное управление операциями на удаленных высокотехнологических объектах сокращает затраты и уменьшает сопутствующие риски. Для организации процесса контроля и управления в таких системах довольно часто используются системы космической связи. Однако при определенных условиях, существует вероятность нарушения нормальной работы системы космической связи злоумышленником. Дестабилизация работы системы мониторинга, контроля и управления может привести к нарушению функционирования оборудования, относящегося к критическим технологиям. Кроме того, это может спровоцировать экологическую катастрофу. Поэтому разработка подсистемы, обеспечивающей высокую степень имитозащиты для систем удаленного мониторинга и управления критическими технологиями, является актуальной задачей.

Применение интерактивных систем удаленного мониторинга, моделирования и контроля операционных процессов позволяет повысить эффективность работы оборудования, расположенного, как правило, в труднодоступных и малонаселенных областях, с одновременным улучшением безопасности проведения работ и уменьшения сопутствующих рисков. Это наглядно проявляется при освоении энергетических ресурсов и других полезных ископаемых прибрежного шельфа, морского и океанического дна Арктики.

Стратегические интересы России в Арктике обусловлены тем, что в недрах арктического шельфа хранятся огромные запасы нефти, газа, угля, золота, меди, никеля, олова, платины, марганца. Реальный ресурсный потенциал Арктики может быть и значительно выше прогнозов, так как изучение ее недр находится по существу на начальном этапе. При этом в ближайшем будущем арктические месторождения нефти и газа будут играть все большую роль в топливно-энергетическом балансе страны. От реализации нефтегазовых проектов в Арктике в будущем во многом будет зависеть международная энергетическая безопасность страны.

Так как добыча и транспортировки природных богатств производится в труднодоступных и малонаселенных областях Крайнего Севера, то компании создают системы удаленного мониторинга, контроля и управления операционными процессами [1–3]. При этом одним из наиболее важных элементов такой системы становится и связь с удаленными объектами. Эффективное использование последней, позволяет провести качественный интерактивный контроль и управление, которые станут базовой основой для обеспечения безопасности персонала, бесперебойной работы оборудования и повышения эффективности работы.

Для эффективного принятия решения по выбору управляющего воздействия высококвалифицированным специалистам, которые работают в центрах поддержки операций (ЦПО), необходимо обеспечить достоверный обмен данными о параметрах выполняемых работ, телеметрического сопровождения и измерений регистрируемых приборами, установленными на удаленном оборудовании. С этой целью на удаленном высокотехнологическом оборудовании размещают абонентские терминалы (АТ). Как правило, абонентские терминалы представляют собой программно-аппаратный комплекс, спроектированный на базе станции спутниковой связи для сбора и обработки навигационных и телеметрических данных на объекте мониторинга и дальнейшей передачи этих данных в ЦПО с возможностью обратного приема и обработки сообщений от клиентского ЦПО [2].

Большинство космических станций, которые используются в системах удаленного мониторинга, контроля и управления операционными процессами имеют геостационарную орбиту. Однако географическое положение многих месторождений за Полярным кругом и на арктическом шельфе делает невозможным использование геостационарных орбитальных установок. Поэтому для осуществления процедур контроля, мониторинга и управления создаются группировки космических аппаратов (КА) на низких околоземных орбитах. При этом количество аппаратов в группировке, как и число самих группировок, принадлежащих разным странам, будет неизменно расти [3].

В результате этого, в зону видимости абонентского терминала, спроектированного на базе станции спутниковой связи и представляющего собой программно-аппаратный комплекс для сбора и обработки навигационных и телеметрических данных на объекте мониторинга, может попасть сразу же несколько космических аппаратов, принадлежащих различным компаниям и государствам. В такой ситуации АТ должен однозначно «опознать» свой спутник и наладить с ним обмен данными.

Как известно, большинство спутниковых систем работают в режиме трансляции сигналов с кодовым разделением каналов. При таком типе разделения каналов сигналы от всех КА орбитальной группировки транслируются в одной полосе частот. В этом случае существует вероятность осуществления попыток злоумышленником нарушения нормальной работы системы космической связи. Такая дестабилизация работы системы мониторинга, контроля и управления может стать первопричиной нарушения функционирования высокотехнологического оборудования. При определенных условиях, это может привести к экологической катастрофе, последствия которой будут способствовать частичному или полному уничтожению экосистемы Крайнего Севера и Арктики.

Проведенные исследования показали, что множество дестабилизирующих действий на систему космической связи можно разделить на две группы. В основу первой группы будут входить методы радиоэлектронного подавления сигнала. Во вторую группу методов можно отнести те методы, которые базируются на и навязывании ложного базиса сигнала противнику [4].

Целью радиоэлектронного подавления сигнала КА на низких околоземных орбитах является блокирование передачи сигнала, в результате которого центр поддержки операций утрачивает возможность правильно принимать решение по выбору управляющего воздействия на удаленный объект.

В основу второй группы входят методы подмена базиса ложными сигналами. Основной целью подмены является искажение значений показателей, позволяющих оценить текущее состояние объекта управления, или навязывание некорректного управляющего воздействия, поступающего из центра поддержки операций. При этом подмена подразумевает создание копии базы сигналов и манипулирование его параметрами.

Очевидно, что в условиях Крайнего Севера, территория которого является труднодоступной и малозаселенной, методы, составляющие первую группу и дестабилизирующие работу космической системы связи, являются малоэффективными. При этом, несмотря на многообразие систем способных поставить различные виды радиопомех, данный подход к нарушению работы системы мониторинга, контроля и управления удаленным объектом в арктических условиях требует значительных аппаратных и финансовых затрат.

Следовательно, в условиях размещения оборудования в труднодоступных и малозаселенных районах, основным способом негативного воздействия на систему космической связи являются методы, образующие вторую группу. Таким образом, в работе будут рассмотрены методы противодействия попыткам навязывания ложного образа.

Проведенные исследования показали, что снизить последствия от навязывания ложных образов возможно за счет:

– применения криптографических методов защиты информации,

– повышения структурной скрытности системы.

Рассмотрим криптографические методы защиты информации, которые могут быть использованы в системе связи с удаленными объектами управления. Существующие методы поблочного шифрования, обеспечивая требуемый уровень защиты информации от НСД, характеризуются низкой скоростью зашифрования из-за многократно выполняемых раундов (итераций). Асимметричные системы шифрования также не позволяют обеспечить реальный масштаб времени обработки данных. Системы побитового шифрования потока данных обеспечивают высокую скорость зашифрования и расшифрования. Однако данная система криптографической защиты уязвимо к атакам на основе исходных и подобранных текстов из-за того, что при побитовом шифровании операция суммирования по модулю 2 является единственным способом построения обратимой функции шифрования.

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет разрабатывать криптографические процедуры защиты информации, обладающие всеми достоинствами систем нелинейного шифрования, обеспечивающие реальный масштаб времени закрытия информации и операций, связанных со сложением, умножением, возведением в степень элементов расширенных полей Галуа $GF(q^v)$, а также их различных комбинаций позволит существенно улучшить обеспечение конфиденциальности и целостности информации [5–8]. В этом случае символы шифрованного текста могут определяться в результате решения уравнения

$$\alpha(z) + y^{x_1}(z) \equiv \beta(z) \bmod \pi(z), \quad (1)$$

где x_1 – целое число, которое выбирается заранее и используется постоянно или меняется на каждом такте работы регистра сдвига;

$y(z)$ – полиномиальное представление псевдослучайной последовательности элементов поля Галуа;

$\alpha(z)$ – символы исходного сообщения, представленные в полиномиальном виде;

$\deg\alpha(z) < \deg\pi(z)$ – степень полинома $\alpha(z)$;

$\beta(z)$ – полиномиальное представление шифрованного сообщения; $\pi(z)$ – порождающий полином.

Дешифрование такого сообщения осуществляется путем решения уравнения

$$\beta(z) + (\pi(z) + y^{x_1}(z)) \bmod \pi(z) \equiv \alpha(z), \quad (2)$$

где «+» – суммирование по модулю два.

Также при зашифровании может быть использован алгоритм, определяемый выражением

$$\alpha(z) y^{x_1}(z) \equiv \beta(z) \bmod \pi(z). \quad (3)$$

В этом случае процедура дешифрования определяется следующим соотношением

$$\beta(z)(y^{x_1}(z))^{-1} \equiv \alpha(z) \bmod \pi(z) . \quad (4)$$

В работе [8] показан алгоритм нелинейного шифрования потока данных с операцией возведения в степень символов конечного поля. В этом случае для шифрования поступающих на вход символов исходного текста, представленного в полиномиальной форме $\alpha(z) = \{\alpha_j(z)\}$ вычисляются значения символов псевдослучайной последовательности конечного поля x = {xj} на различных тактах работы регистра сдвига j = 0,1,2,… и определяются символы шифрованного сообщения

$$\alpha(z)^x \equiv \beta(z) \bmod \pi(z) . \quad (5)$$

Однако следует отметить, что процедуры шифрования производятся подсистемой вторичной обработки сигналов. При этом, несмотря на хорошие результаты по противодействию дестабилизирующих действий злоумышленника, они не способны противостоять навязыванию ложного образа при первичной обработке сигнала.

Рассмотрим методы, позволяющие повысить структурную скрытность системы связи. Как правило, повышение структурной скрытности системы направлено на увеличение априорной неопределенности параметров передаваемых сигналов [9]. Для достижения поставленной цели производится манипулирование основными параметрами сигналов, к которым относятся частота несущего колебания, закон модулирования, стохастическое использование заранее подготовленных кодовых последовательностей.

Проведенные исследования показали, что реализация данного направления, позволяющего уменьшить последствия от ложного навязывания сигналов, требует значительных аппаратурных и финансовых затрат на свою реализацию.

Одним из перспективных направлений в решении отмеченной выше проблемы является разработка системы, позволяющей оперативно оценить статус спутника, находящегося в зоне видимости абонентского терминала. Рассмотрим алгоритм работы запросно-ответной системы опознавания, использующий протоколы с нулевым разглашением. Такие протоколы, базируясь на разработанной псевдослучайной функции повышенной эффективности, нашли широкое применение в системах электронных платежей, которые работают с электронной наличностью [9–12]. Использование разработанных протоколов с нулевым разглашением позволяет обеспечить решение такой проблемы, так как данные протоколы обладают хорошей криптографической стойкостью и обеспечивают высокую степень защиты информации от НСД.

Использование протоколов с нулевым разглашением в системах определения «свой-чужой» позволит повысить имитостойкость системы дистанционного контроля и управления удаленными объектами, обеспечивая повышение эффективности их функционирования и снижение рисков связанных с использованием критических технологий. С помощью этих протоколов запросчик, который располагается на стационарном объекте может в реальном масштабе времени определить статус КА, находящегося в зоне видимости. Для физической реализации данных протоколов в виде программно-аппаратного комплекса необходимо выполнение следующего алгоритма обмена данными.

Этап 1. В память вычислительного устройства ответчика, который располагается на борту КА, вводятся числа *U, S, T*. В этом случае число *U* выступает в качестве долгосрочного секретного ключа. Числа *S* и *T* являются базовой основой, с помощью которой производится вычисление сеансовых ключей *S(i)* и *T(i)*. Тогда имеем

$$S(i) = g^{\frac{1}{S+i+1}} \bmod q , \quad (6)$$

$$T(i) = g^{\frac{1}{T+i+1}} \bmod q , \quad (7)$$

где q – мультипликативная группа;
g – первообразный элемент этой группы;
i – номер проводимого сеанса.

Этап 2. Используя полученные данные U, S(i) и T(i) вычислительное устройство ответчика вычисляет истинный статус КА согласно

$$C(i) = g^{U} g^{S(i)} g^{T(i)} \bmod q \,. \tag{8}$$

Вычисленное значение истинного статуса записывается в блок памяти программно-аппаратного комплекса.

Этап 3. Затем в вычислительном комплексе, используя полученные данные U, S(i) и T(i), производится их зашумление

$$U^{*}(i) = U + \Delta U \bmod q \,, \tag{9}$$

$$S^{*}(i) = S(i) + \Delta S \bmod q \,, \tag{10}$$

$$T^{*}(i) = T(i) + \Delta T \bmod q \,, \tag{11}$$

где ΔU, ΔS, ΔT– величины зашумления значений U, S(i) и T(i) соответственно.

После этого вычислительное устройство ответчика вычисляет зашумленный статус космического аппарата согласно

$$C^{*}(i) = g^{U^{*}} g^{S^{*}(i)} g^{T^{*}(i)} \bmod q \,. \tag{12}$$

Вычисленное значение зашумленного статуса записывается в блок памяти программно-аппаратного комплекса.

Этап 4. При появлении КА в зоне видимости запросчик, находящийся на абонентском терминале, генерирует «запросное число» d и пересылает его космическому аппарату.

Этап 5. Получив «запросное число» d ответчик вычисляет ответы

$$r_1 = U^{*} - dU \bmod \phi(q) \,, \tag{13}$$

$$r_2 = S(i)^{*} - dS(i) \bmod \phi(q) \,, \tag{14}$$

$$r_3 = T(i)^{*} - dT(i) \bmod \phi(q) \,, \tag{15}$$

Этап 6. Окончив выполнение вычислений, ответчик передает запросчику сигнал, который содержит вычисленный истинный статус *C(i)*, вычисленный зашумленный статус *C*(i)*, ответы на поставленный вопрос r_1, r_2, r_3.

Этап 7. Запросчик, получив данный сигнал, вычисляет результат

$$Y(i) = C^{d}(i) g^{r_1} g^{r_2} g^{r_3} \bmod q \,. \tag{16}$$

Если вычисленное значение *Y(i)* совпадет со значением зашумленного статуса космического аппарата, т.е. $Y(i) = C^{*}(i)$, то принимается решение, что статус спутника «свой». Между абонентским терминалом, представляющим собой программно-аппаратный комплекс, спроектированный на базе станции спутниковой связи, и КА производится обмен данными, которые являются результатом обработки навигационных и телеметрических данных на объекте мониторинга, и управляющими воздействиями.

Если вычисленное значение *Y(i)* не совпадет со значением зашумленного статуса космического аппарата, т.е. $Y(i) \neq C^{*}(i)$, то принимается решение, что статус спутника «чужой» и обмен информацией не производится.

Рассмотрены основные методы противодействия дестабилизирующим действиям злоумышленника на космическую систему связи, используемую для проведения мониторинга, контроля и управления удаленных объектов. Показана возможность использования полиномиальной системы класса вычетов для обеспечения требуемого уровня защиты данных от НСД. Разработан алгоритм протокола с нулевым разглашением, позволяющий оперативно определить статуса космического аппарата, находящегося в зоне видимости абонентского терминала, установленного на удаленном объекте управления. С целью повышения эффективности алгоритма предлагается использовать разработанную псевдослучайную функцию. Применение нового протокола работы запросно-ответной системы опознавания позволяет защитить оборудование удаленного объект от деструктивных воздействий, повысить эффективность его работы и снизить вероятность выхода из строя.

Литература

1. Центр поддержки операций компании Шлюмберже. http://www.slb.ru/page.php?code=28.

2. http://www.esa.int/Our_Activities/Observing_the_Earth/CryoSat.

3. Пашинцев В. П., Чипига А. Ф., Галкина В. А., Смирнов А. А. Решение проблемы обеспечения энергетической скрытности в системах спутниковой связи при близком размещении приемника радиоперехвата // Наукоемкие технологии, 2012. Т. 13. № 7. С. 30–34.

4. Катков К. А. Адаптивный алгоритм определения вектора пространственно-временных координат // Известия ОрелГТУ. Информационные системы и технологии. 2011. № 1 (63). С. 5–14.

5. Калмыков И. А., Кихтенко О. А., Барильская А. В., Дагаева О. И. Криптографическая система на базе непозиционных полиномиальных алгебраических структур // Вестник Северо-Кавказского федерального университета, 2010. № 2. С. 51–57.

6. Калмыков И. А., Чипига А. Ф., Барильская А. В., Кихтенко О. А. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем // Известия Южного федерального университета. Технические науки. 2009. Т. 100. № 11. С. 210–220.

7. Калмыков И. А. Чипига А. А. Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации// Инфокоммуникационные технологии. Самара. 2007. Т. 5. № 2. С. 159–162.

8. Калмыков И. А., Стрекалов Ю. А., Щелкунова Ю. О., Кихтенко О. А., Барильская А. В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. 2010. Т. 8. № 2. С. 14–22.

9. Калмыков И. А., Дагаева О. И. Разработка псевдослучайной функции повышенной эффективности (статья) // Известия ЮФУ. Технические науки, Таганрог: ТРТУ , 2011. № 12. С. 160–169.

10. Калмыков И. А., Дагаева О. И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ. Технические науки. 2012. Вып. 12. С. 218–224.

11. Калмыков И. А., Дагаева О. И. Применение системы остаточных классов для формирования псевдослучайной функции повышенной эффективности // Известия Южного федерального университета. Технические науки, Таганрог: ТРТУ, 2013 г. № 12 (149), С. 228–234.

12. Калмыков И. А., Дагаева О. И., Науменко Д. О., Вельц О. В. Системный подход к применению псевдослучайных функций в системах защиты информации // Вестник Северо-Кавказского федерального университета. 2012. № 3 (32). С. 26–34.