Сравнительный анализ и перспективы развития обеспечения ограничения доступа к навигационной информации в спутниковых навигационных системах «ГЛОНАСС» и GPS

Comparative analysis and prospects of access restriction to navigation information in «GLONASS» and GPS satellite navigation systems

Ключевые слова: спутниковые навигационные системы – satellite navigation systems; цифровая навигационная информация – digital navigation information; навигационная аппаратура потребителя – user navigation equipment; навигационные сигналы – navigation signals; навигационный кадр – navigation frame; достоверность и надежность информации – authenticity and reliability of information; ограничение доступа обеспечения безопасности – access restriction security assurance; избирательный доступ – selective access; криптографическое преобразование – cryptographic transformation; дифференциальные подсистемы – differential subsystems; специальное кодирование – special encoding.

В работе рассматривается актуальная тема обеспечения безопасности спутниковой навигационной информации в спутниковых навигационных системах «ГЛОНАСС» и GPS «Навстар». Автором отмечается положительная динамика состояния системы ограничения доступа и обеспечения безопасности навигационной информации в спутниковых навигационных системах (СНС).

The article addresses a topical subject of satellite navigation information security in «GLONASS» and SPS «Navstar» satellite navigation systems. The author shows positive dynamics of the access restriction system and security assuranceof navigation information in SIS.

ЛАЗАРЕВ / LAZAREV E.
Евгений Сергеевич
(tyulkin-mv@yandex.ru)
старший лейтенант, младший научный сотрудник 46-го Центрального научного исследовательского института МО РФ, Москва

Спутниковая радионавигация является одним из перспективных направлений прикладной космонавтики. Она гарантирует качественно новый уровень координатно-временного обеспечения наземных, морских, воздушных и космических потребителей. На сегодняшний день в мире существует две функционирующие современные спутниковые радионавигационные системы (СНС) – «ГЛОНАСС» (РФ) и GPS «Навстар» (США), обладающие самыми высокими показателями. Спутниковые радионавигационные системы «ГЛОНАСС» и GPS являются основным средством навигационно-временных определений, от результатов которых зависит не только успех каких-либо операции, но и безопасность людей. Поэтому пользователи данных систем должны доверять сигналам, принимаемым со спутников, и должны быть уверены в полной достоверности информации, содержащейся в них. В первую очередь, широкое внедрение спутниковой навигации выдвигает в число актуальных вопросов повышение точности, достоверности, надежности (ограничения доступа) навигационной информации в системах для различных потребителей. Ограничение доступа осуществляется для обеспечения защиты от несанкционированного доступа (НСД) к информации. В общем случае ограничение доступа предполагает разграничение полномочий пользователей (субъектов доступа), их идентификацию и аутентификацию с основной целью, защиту навигационной информации от НСД.

Для реализации режима ограничения доступа к сигналам навигационной информации СНС «ГЛОНАСС» и GPS и сигналов их функциональных дополнений (дифференциальных подсистем) используются специальные методы, режимы и средства, обеспечивающие защиту от НСД к данной информации. В связи с этим в американской навигационной системе GPS «Навстар» «Defense Global Positioning System Security Policy», являющейся наставлением по обеспечению безопасности навигационной аппа-

ратуры потребителя (НАП) от несанкционированного применения системы, используются методы:

– метод селективной доступности;

– метод предотвращения имитации защищенных сигналов и несанкционированного их использования;

– метод предотвращения использования корректирующих данных.

В соответствии с представленными методами обеспечения безопасности к навигационной информации спутники GPS работают в одном из трех основных режимов защиты данных:

1. Режим защиты методом селективной доступности – НАП стандартного режима навигационно-временных определений (НВО), обеспечивающий установленную ограниченную точность (двухчастотные приемники имеют преимущество перед одночастотными за счет устранения ионосферной ошибки). Навигационная аппаратура потребителя точного режима НВО для компенсации влияния данного метода должна быть снабжена ключами.

2. Режим защиты методом предотвращения имитации и несанкционированного использования (в настоящее время является повседневным режимом защиты) – АП точного режима НВО для обработки Y-сигнала должна быть соответствующим образом снабжена ключами, а при отсутствии таких ключей работает в стандартном режиме НВО (используется с 1993 года).

3. Режим защиты двумя методами одновременно (селективной доступности и предотвращения имитации и несанкционированного использования).

Кроме того, министерство обороны США использует для обеспечения ограничения доступа к навигационной информации спутники навигационной системы, оснащенные бортовыми стандартами частоты и различной навигационной аппаратурой и оборудованием, непрерывно передающие дальномерные сигналы, модулируемые навигационными сообщениями. Проверка аппаратуры спутников СНС GPS в режимах защиты методами селективной доступности и предотвращения имитации и несанкционированного использования проводится в ходе орбитальных испытаний новых искусственных спутников Земли (ИСЗ). Включение режима защиты методом предотвращения имитации и несанкционированного использования проводится одновременно с вводом спутника в эксплуатацию.

Временные шкалы бортовых стандартов частоты всех ИСЗ синхронизируются системой единого времени с помощью станций наземного командно-измерительного комплекса (КИК), сопровождающих спутники, принимающих и обрабатывающих их телеметрию, закладывающих в их бортовые запоминающие устройства данные, необходимые для формирования навигационных сигналов и сообщений. С борта каждого из спутников системы передаются три сигнала: открытый (C/A – Clear Acquisition) и два защищенных (P – Protected, подвергаются шифрованию и называются также P(Y) сигналами), в основе конструкции которых лежат уникальные для каждого ИСЗ дальномерные коды. Открытые сигналы предназначены для использования в любой аппаратуре потребителей, а защищенные сигналы – только в санкционированной АП, в том числе – в военной АП вооруженных сил США и их союзников.

Открытые сигналы модулируются по фазе (на 180°) со скоростью 250 бит/с навигационным сообщением и передаются с борта ИСЗ посредством фазовой манипуляции (на 180°) излучений круговой поляризации правого вращения с несущими частотами 1563,42–1587,42 МГц (сигнал L1 C/A). Эффективная изотропно излучаемая мощность (ЭИИМ) составляет 26,8–28 дБВт. В отличие от СНС «ГЛОНАСС», эфемеридная информация ИСЗ GPS передается в виде модифицированных кеплеровых элементов. Допустимый временной интервал использования составляет 4 часа.

Защищенные сигналы манипулируются по фазе (на 180°) со скоростью 250 бит/с навигационным сообщением и передаются с борта ИСЗ посредством фазовой манипуляции (на ±90°) двух излучений круговой поляризации правого вращения с несущими частотами 1563,42–1587,42 (сигнал L1 P/Y) и 1215,6–1239,6 МГц (сигнал L2 P/Y). Так как сигнал на частоте L2 используется в основном для определения поправок, связанных с задержками распространения сигналов в ионосфере, по сравнению с открытым сигналом, его мощность снижена. Эффективная изотропно излучаемая мощность сигнала L1 P/Y составляет 23,8–25 дБВт, а сигнала L2 P/Y – 19,7–22,3 дБВт. Предусмотрено, что на частоте L2 вместо P/Y-сигнала может также передаваться C/A-сигнал. Также было принято решение об удовлетворении требования авиационного агентства США об использовании новой третьей частоты L5 с несущей частотой 1176,45 МГц, которая будет находиться в полосе авиационных служб. Таким образом, с борта спутников возможна передача следующих сигналов: L1 C/A, L1 P/Y и L2 P/Y (используется на постоянной основе с 1991 года), L1 C/A, L1 P и L2 P (использовалась периодически до 1991 года), L1 C/A, L1 P и L2 C/A (не использовалась), L5 C/A (не использовалась).

В навигационной аппаратуре потребителей (НАП) проводятся:

– прием навигационного сообщения, выбор не менее 4 ИСЗ из 5–12;

– прием и обработка дальномерных сигналов;
– обработка измеряемых навигационных параметров и эфемеридно-временных данных для определения пространственных координат, составляющих скорости движения подвижных носителей НАП и точного системного времени.

Мощности принимаемых НАП открытых и защищенных сигналов на частоте L1 и защищенных сигналов на частоте L2 составляют -160 и -166 дБВт, соответственно. Существующие С/А-коды на частоте L1 и P/Y-коды на частотах L1 и L2 должны быть сохранены до тех пор, пока не будет развернуто созвездие модернизированных КА, передающих новые сигналы для гражданских и военных пользователей, и пока не будет выпущено достаточное количество аппаратуры пользователей, работающих по модернизированным сигналам, на что может потребоваться от 10 до 15 лет. Согласно текущим планам, предусматриваются продолжение предоставления гражданским пользователям С/А-кодов на частоте L1 и постепенная передача С/А-кодов на частоте L2 по мере запуска новых КА для восполнения созвездия (Block IIR-M и IIF). В частности, предполагается ввести два новых открытых сигнала на частоте L2 – L2 CM-Code и L2 CL-Code. Тактовая частота кодов составит 511,5 кбит/с, длительность – 20 мс и 1,5 с, соответственно. Длина кода L2 CM составит 10 230 символов, а длина кода L2 CL – 762 250 символов. Периоды всех кодов, передаваемых на частоте L2, будут жестко синхронизированы с Р-кодом. Оба дальномерных кода – L2 CM-Code и L2 CL-Code, будут формироваться с использованием линейного генератора псевдослучайных последовательностей (ПСП) на основе 27-разрядного регистра сдвига. Каждому КА системы будет предписано работать с использованием своего фрагмента данного кода (для обеспечения технологии коллективного доступа с кодовым разделением каналов – CDMA). Для повышения надежности передачи эфемеридной информации предполагается использовать дополнительное блочное кодирование с использованием сверхточных кодов.

Планы в части передачи кодов на частоте L5 предусматривают использование в этом диапазоне более высокой частоты следования символов кода и большую длину периода кодовой последовательности, чем у используемых в настоящее время С/А-кодов. Частота следования элементов дальномерного кода на L5 предполагается равной 10,23 МГц, а его длина – 10 230 символов. Предполагается, что на частоте L5 не будут передаваться эфемеридные данные. В перспективе для специальных и военных потребителей планируют ввести новый набор специальных кодов (М-кодов), способных обеспечить захват сигналов без предварительного доступа к С/А-кодам, что существенно повысит надежность навигационных определений для военных потребителей. Одним из направлений внесения изменений в основную систему может стать повышение мощности гражданского сигнала.

Модернизированный КА GPS должен обеспечивать гражданских пользователей сигналом С/А-кода на частоте L2. В качестве второго основного сигнала, требования к мощности данного сигнала должны быть сопоставимы с требованиями к сигналу С/А-кода на частоте L1 (-160 дБВт). Мощность P/Y-кода на частоте L2 также требует четырехкратного увеличения (на 6 дБ) для всех модернизированных КА. Новый сигнал L5 в полосе частот для авиационных радионавигационных служб потребует уровня мощности, на 6 дБ превышающего уровень мощности сигнала С/А-кода на L1, чтобы компенсировать более высокие уровни помех и шумов в этой полосе. С точки зрения безопасности, стоимости и возможных характеристик, в настоящее время предлагается повышение уровня всех гражданских сигналов на 3–6 дБ. Сигналы для военных пользователей на частотах L1 и L2 для повышения характеристик обнаружения навигационных сигналов в условиях радиоэлектронного противодействия будут излучаться с уровнем мощности, на 6–10 дБ превышающим современный уровень. Вместе с тем, правительства США и европейских стран считают, что в независимых спутниковых системах, таких как GPS и Galileo, для гражданских пользователей должны использоваться одни и те же частоты и структуры сигналов, чтобы сигналы независимых систем были совместимы с точки зрения частотного плана. Система GPS используется потребителями в двух основных режимах – в стандартном и точном, а также в одном дополнительном дифференциальном режиме НВО.

СТАНДАРТНЫЙ РЕЖИМ НВО

В стандартном режиме автономная НАП позволяет определять пространственные координаты потребителя с точностью не ниже 5–25 м (на плоскости значение точности определения вертикальной составляющей не ниже 7–38 м) при выключенном режиме селективной доступности. Скорость и время определяются с точностями 0,15–0,3 м/с и 170–350 нс, соответственно. Основным фактором, влияющим на ошибку определения координат, является задержка распространения сигналов в ионосфере, значение которой зависит от времени суток, периода года и солнечной активности.

ТОЧНЫЙ РЕЖИМ НВО

Потребители точного режима НВО делятся на две категории – на санкционированные (министерство обороны, другие федеральные министерства,

администрации и агентства правительства США) и прочие (вооруженные силы и правительства стран-союзниц и дружественных стран, причем финансирование потребителей в федеральных правительствах должно осуществляться через министерства обороны). Санкционированные потребители точного режима НВО имеются в Австралии, Бельгии, Великобритании, Венгрии, Германии, Греции, Дании, Израиле, Исландии, Испании, Италии, Канаде, Кувейте, Люксембурге, Малайзии, Нидерландах, Новой Зеландии, Норвегии, Польше, Португалии, Республике Корея, Саудовской Аравии, Сингапуре, Тайване, Турции, Финляндии, Франции, Чехии, Швейцарии, Швеции и Японии.

В точном режиме автономная НАП позволяет определять пространственные координаты потребителя с точностью не ниже 3–15 м (на плоскости значение точности определения вертикальной составляющей не ниже 7–38 м). Скорость и время определяются с точностью 0,1 м/с и 100 нс, соответственно. Потребители, использующие систему для решения оперативных и обеспечивающих задач, должны оснащаться НАП точного режима НВО. Многие военные и гражданские потребители системы нуждаются в предоставлении высокой точности НВО, например – при проведении поисково-спасательных операций, навигации судов в портах и обеспечении точного захода воздушных судов на посадку. Поэтому во всем мире принимаются меры по повышению точности НВО путем передачи потребителям дополнительных корректирующих данных.

ДИФФЕРЕНЦИАЛЬНЫЙ РЕЖИМ НВО

Данный режим основан на исключении различного рода систематических погрешностей при совместной обработке результатов НВО в НАП, аппаратуре опорной станции и передаче в НАП корректирующих данных. Применение дифференциального режима позволяет гражданским потребителям с АП стандартного режима НВО выйти на уровень точности, предоставляемый защищенными навигационными сигналами в АП точного режима НВО. Дифференциальная АП, обеспечивающая прием несущей частоты L2 и отстоящая от опорной станции на 20–200 км, позволяет определять координаты с точностью не ниже 1–5 м, скорость и время – с точностью 0,1–0,2 м/с и 30–60 нс, соответственно. Применение дифференциального режима в точном режиме НВО способствует повышению устойчивости бортовой военной и специальной АП, так как позволяет эффективно компенсировать погрешности, возникающие при нештатной работе системы (например – при уходе бортовых шкал времени отдельных ИСЗ, отказе бортового стандарта частоты с переходом на кварцевый генератор или нарушении работы наземного комплекса системы). Аналогичным образом предусматривается решение проблемы ограничения доступа в отечественной СНС «ГЛОНАСС».

Многолетний опыт использования СНС «ГЛОНАСС» показал, что она стала стержневым элементом в обеспечении национальной безопасности и ускоренного социально-экономического развития РФ. Во многом это связано с выполнением ФЦП «Глобальная навигационная система» от 20.08.2001 года. В соответствии с Указом Президента РФ от 17 мая 2007 года № 638 Правительству РФ поручено утвердить в 2011 году новую федеральную целевую программу – «Поддержание, развитие и использование системы "ГЛОНАСС" на 2012–2020 годы». Основными целями новой федеральной целевой программы являются массовое внедрение перспективных отечественных навигационных технологий, улучшение ее характеристик, расширение функциональных возможностей, условий и сфер использования. Для достижения целей федеральной целевой программы необходимо обеспечить соответствие темпов развития технологий системы «ГЛОНАСС» росту требований специальных и гражданских потребителей, связанных с повышением точности, доступности, оперативности и надежности навигационной информации.

Спутниковая навигационная система «ГЛОНАСС» представляет собой орбитальную группировку КА, бортовая аппаратура которых содержит средства ограничения доступа к навигационным сигналам высокой точности (ВТ), выполняющие функции специального кодирования информации. Навигационные радиосигналы с частотным разделением, передаваемые каждым НКА системы «ГЛОНАСС», излучаются в диапазонах L1 и L2. С выводом НКА «Глонасс-К» в системе «ГЛОНАСС» планируется передавать навигационные радиосигналы одновременно уже в трех частотных поддиапазонах с использованием частотно-кодового разделения, таких как:

– f (L1) = 1563x1,023 МГц = 1598,95 МГц;
– f (L2) = 1220x1,023 МГц = 1248,06 МГц;
– f (L3) = 1174x1,023 МГц = 1201,01 МГц.

В интересах экономии частотного ресурса КА, находящиеся в противоположных точках орбитальной плоскости (антиподные КА), могут передавать навигационные радиосигналы на одинаковых частотах (литерах). Состав существующих и вновь вводимых навигационных сигналов системы «ГЛОНАСС» определен в утвержденной в 2008 году «Концепции развития навигационных сигналов глобальной навигационной системы "ГЛОНАСС"».

Существующая орбитальная группировка системы «ГЛОНАСС» состоит из КА «ГЛОНАСС» и «ГЛОНАСС-М», которые излучают четыре навигационных сигнала:

– сигнал L1OF с открытым доступом и частотным разделением в диапазоне L1;

– сигнал L2OF с открытым доступом и частотным разделением в диапазоне L2;

– сигнал L1SF с санкционированным доступом и частотным разделением в диапазоне L1;

– сигнал L2SF с санкционированным доступом и частотным разделением в диапазоне L2.

При этом предусматривается этапность перспектив развития и реализации новых сигналов системы «ГЛОНАСС».

Этап 1 (2008—2009 годы)

Космические аппараты системы «ГЛОНАСС» излучают навигационные сигналы L1OF, L2OF, L1SF и L2SF с открытым и санкционированным доступом в частотных диапазонах L1 и L2. Осуществляется разработка перспективных сигналов, состава передаваемой в них цифровой информации, в том числе – методов управления доступом к навигационным сигналам с учетом всех требований МО РФ.

Этап 2 (2010—2015 годы)

Дополнительно вводятся новые навигационные сигналы L3OF и L3SF с открытым и санкционированным доступом с частотным разделением каналов в диапазоне L3, а также новые навигационные сигналы L1ROC и L5ROC с открытым доступом с кодовым разделением каналов в диапазонах L1 и L5, при этом сигналы L3OF и L3SF реализуются в 2010 году.

Этап 3 (после 2015 года)

Дополнительно вводятся навигационные сигналы L1SC, L2SC и L3SC с санкционированным доступом для специальных потребителей с кодовым разделением каналов в частотных диапазонах L1, L2 и L3 системы «ГЛОНАСС» и сигнал L2OC с открытым доступом. В частотных поддиапазонах L1, L2 и L3 КА «ГЛОНАСС» будут передавать навигационные радиосигналы двух типов – стандартный сигнал СТ и сигнал, отвечающий требованиям потребителей МО РФ (сигнал ВТ).

Мощность излучаемого СТ радиосигнала в диапазоне L3 составит не менее 20–30 Вт, при этом мощность радиосигнала, принимаемого потребителем от НКА «ГЛОНАСС-К» в поддиапазоне L3, должна быть не менее -161 дБВт. Модулирующая цифровая последовательность, используемая при формировании сигнала стандартной точности для манипуляции несущей частоты поддиапазона L3, образуется сложением по модулю 2 трех двоичных сигналов:

– навигационного сообщения, передаваемого со скоростью 125 бит/с;

– вспомогательного меандрового колебания, передаваемого со скоростью 250 бит/с;

– псевдослучайного дальномерного кода, передаваемого со скоростью 4,095 Мбит/с.

Дальномерный код представляет собой псевдослучайную последовательность (ПСП) максимальной длины, снимаемую с выхода регистра сдвига, с периодом повторения 1 мс и скоростью передачи символов 4,095 Мбит/с. Степень образующего полинома, соответствующего регистру сдвига, формирующему ПСП, равна 12.

Из анализа современных и прогнозируемых требований к навигационным услугам для специальных потребителей и потребителей социально-экономической сферы и с учетом тенденций развития СНС и их международной интеграции рассматривается возможность реализации в системе «ГЛОНАСС» следующих новых навигационных сигналов, реализуемых на перспективных КА, начиная с модификаций КА «ГЛОНАСС-К»:

– L3OF с открытым доступом и частотным разделением в диапазоне L3;

– L3SF с санкционированным доступом и частотным разделением в диапазоне L3;

– L1ROC с открытым доступом и кодовым разделением в диапазоне L1;

– L1SC с санкционированным доступом и кодовым разделением в диапазоне L1;

– L2OC с открытым доступом и кодовым разделением в диапазоне L2;

– L5ROC с открытым доступом и кодовым разделением в диапазоне L5;

– L2SC с санкционированным доступом и кодовым разделением в диапазоне L2;

– L3SC с санкционированным доступом и кодовым разделением в диапазоне L3.

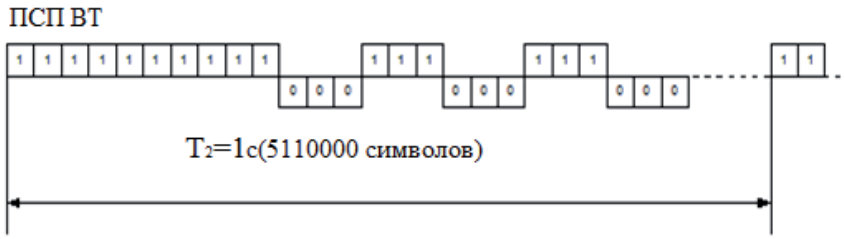
Управление доступом к сигналам СНС «ГЛОНАСС» включает в себя реализацию следующих режимов:

– режима затруднения несанкционированного доступа (НСД) к существующим сигналам высокой точности в диапазонах L1 и L2;

– режима исключения НСД к новым ВТ сигналам с кодовым разделением, излучаемым в диапазонах L1, L2;

– режимов исключения НСД и селективного доступа для гражданского навигационного сигнала, излучаемого в диапазоне L3;

– режима селективного доступа для гражданских сигналов с частотным и кодовым разделением, излучаемым в диапазонах L1, L2.



Фрагмент последовательности ПСП ВТ

Министерством обороны РФ принята Концепция создания Единой дифференциальной системы (ЕДС) и системы контроля целостности СНС. Согласно ее замыслу, составной частью ЕДС должны стать дифференциальная подсистема видов ВС РФ, как совокупность технических средств с соответствующей инфраструктурой, обеспечивающих формирование и передачу корректирующей информации для повышения точности и надежности навигационных определений потребителей.

В настоящее время в СНС «ГЛОНАСС» для затруднения несанкционированного доступа к навигационной информации сигналов ВТ, измеряемых в диапазонах L1 и L2, и вновь вводимому ВТ сигналу, излучаемому в диапазоне L3, целесообразно использование режима «Доступ – 1, 2, 3».

Режим «Доступ – 1, 2, 3» основан на смене фаз начального состояния генераторов (НСГ) дальномерных (ПСП) и отличающихся друг от друга периодичностью смены фаз начального состояния:

– в конце десятой секунды в начале каждых суток;

– в конце десятой секунды в начале каждого часа;

– в конце десятой секунды в начале каждого интервала 5 минут.

Автоматизированная смена НСГ осуществляется с помощью алгоритмического датчика ПСП. Датчик ПСП выполнен в виде цифрового автомата, содержащего 25 последовательно соединенных триггеров с переключаемыми обратными линейными связями. Синхронно со сменой НСГ на НКА производится автоматизированная смена НСГ в каналах приемника у санкционированных потребителей навигационных радиосигналов. Признак применяемого режима передается потребителю в кадрах цифровой информации, передаваемых с КА сигналов ВТ. На рисунке приведен фрагмент последовательности ПСП сигнала ВТ, 25 символов ПСП ВТ в случае, когда код начального состояния регистра сдвига в генераторе ПСП ВТ содержит 25 единиц. Начальным символом периода ПСП ВТ в этом случае является первый символ в группе из 25 символов, повторяющейся через 1 с и имеющей вид 1111111111000111000111000.

Кроме того, в настоящее время, в морской и мобильной дифференциальных подсистемах (ДПС) СНС «ГЛОНАСС» внедряется режим избирательного доступа к корректирующей информации. Указанный режим реализован с помощью аппаратуры избирательного доступа, которая является универсальной как для контрольно-корректирующей станции, так и для навигационной аппаратуры потребителя. Особенность данного режима заключается в том, что кодированию подвергается не весь кадр, а только подлежащая защите информация (кроме первых двух строк и проверочных элементов). В эфир передается корректирующая информация в полном соответствии с протоколом RTCM (наиболее отработанный формат корректирующей информации морской ДПС). Указанная аппаратура позволяет реализовать режим избирательного доступа и гарантированной защиты от несанкционированного использования навигационной информации, не внося изменения в существующие средства ДПС.Преобразование информации только части навигационного кадра, например – содержащей эфемеридные и частотно-временные данные, является предпочтительным. Такой метод преобразования позволяет сохранить структуру навигационного кадра (протокола передачи информации), который передается в эфир и воспринимается несанкционированным потребителем как доступная для него информация, т.е. дает возможность варьировать значениями разрядов в строках кадра, которые подвергаются преобразованию, и тем самым выбирать точностные характеристики задачи навигационных определений, решаемой несанкционированным потребителем. Для полноценного решения данной задачи, т.е. для исключения НСД, целесообразно применять методы криптографического преобразования информации с гарантированной стойкостью, основанные на сертифицированных алгоритмах криптографического преобразования.

При реализации криптографических методов защиты учитывается следующее:

– система защиты основывается на зашифровывании цифровой информации сигналов ВТ и сигнала L3 и на использовании ответных средств расшифровывания в НАП;

– возможность смены ключей криптографической системы, управление которой должно осуществляться с использованием сигналов СНС;

– алгоритм криптографического преобразования цифровой информации обеспечивает процесс зашифровывания и расшифровывания информации в реальном масштабе времени, т.е. реализовывается поточный метод криптографического преобразования.

Криптографическим преобразованием информации является безызбыточное кодирование данных, которое используется для маскировки информации, такое преобразование информации служит эффективным средством против перехвата несанкционированным потребителем информации, передаваемой по линиям связи, и внесения им не обнаруживаемых средствами сети связи искажений в передаваемое сообщение. Преобразование, выполняемое над исходными данными (ИД) по определенному алгоритму, управляется с помощью ключа преобразования (КП). Алгоритмом преобразования является любой алгоритм, который выполняет посимвольное алгоритмическое преобразование некоторых данных в соответствии с КП. Чтобы получить ИД, нарушитель должен знать алгоритм преобразования, который является общедоступным, и КП, который не должен быть ему доступен. В общей форме в криптографической системе ИД и КП являются входами в некоторое криптографическое преобразующее устройство, которое может быть реализовано аппаратно, программно или аппаратно-программно.

Реализация режима селективного доступа для сигналов СТ, излучаемых в диапазонах L1 и L2, возможна на усовершенствованном сигнальном методе селективного доступа, предполагающем криптографическое закрытие части навигационной информации, обеспечивающее дозированное ухудшение точности навигационного обеспечения несанкционированных потребителей. Для санкционированных потребителей ухудшения точности навигационного обеспечения происходить не должно.

На основании проведенного сравнительного анализа существующих методов, режимов и систем обеспечения ограничения доступа от несанкционированных действий к цифровой навигационной информации СНС в РФ и за рубежом можно сделать следующие выводы:

1. Исключение несанкционированного использования и последствий имитации цифровой навигационной информации в СНС «ГЛОНАСС» и GPS обеспечивается путем:

– разработки методов и алгоритмов, обеспечивающих гарантированную криптографическую защиту цифровой информации канала ВТ от ее несанкционированного использования;

– использования смены кода начального состояния, регистра триггеров, генератора ПСП;

– внедрения и использования методов режима избирательного доступа;

– использования дифференциальных подсистем;

– применения специального кодирования;

– использования криптографического преобразования только части навигационного кадра (например, содержащей эфемеридные и частотно-временные данные);

– применения криптографического оборудования, которое существенно ограничивает несанкционированный доступ.

2. Анализ показал, что космические агентства и военные ведомства России и США совершенствуют и внедряют методы и системы обеспечения ограничения доступа к навигационной информации в СНС «ГЛОНАСС» и GPS, что в свою очередь, обеспечивает гарантированное, качественное и безопасное использование санкционированными потребителями всех возможностей глобальных спутниковых навигационных систем.

Литература

1. Промежуточный НТО о СЧ НИР «Исследования по обоснованию облика и основных ТТХ перспективных многофункциональных унифицированных помехозащищенных навигационных приборов и их функциональных дополнений различного целевого назначения и базирования» (шифр «Авальман»), этап 7 «Разработка тактико-технических требований к системе ограничения доступа к информации радионавигационных систем, передаваемой по специальным каналам, предназначенным для использования в ВС РФ. Разработка предложений по созданию системы ограничения доступа к информации радионавигационных систем, передаваемой по специальным каналам, предназначенным для использования в ВС РФ», ООО «"НПФ "Гейзер"», 2008 г.

2. НТО о СЧ НИР «Разработка предложений по созданию системы ограничения доступа к информации радионавигационных систем, передаваемой по специальным каналам, предназначенным для использования в ВС РФ» (шифр «Авальман»), ГУ «РАРАН», 2008 г.

3. Военная доктрина Российской Федерации (утверждена 21 апреля 2000 г.). – М.: Ось-89, 2004.

4. Эскизный проект модернизированной глобальной навигационной спутниковой системы «ГЛОНАСС» на основе КА «ГЛОНАСС-К». – Кн. 2. – Ч. 4. – НПО «ПМ», 2003.

5. *Ксендзук А.В., Басараб М.А., Волосюк В.К. и др.* Цифровая обработка сигналов. – М.: Физматлит, 2008.

6. «О государственной тайне». – № 131-ФЗ от 06.10.1997 г.

7. Изделие 14Ф113. Исходные данные для реализации в системе «ГЛОНАСС» защиты от несанкционированного доступа к навигационным сигналам ВТ. – Вторая и третья редакции. 2001, 2006 г.

8. ГОСТ № 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

9. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: Кудиц-Образ, 2001.

10. Государственный стандарт РФ «Морская дифференциальная подсистема глобальных навигационных спутниковых систем "ГЛОНАСС" / GPS. Формат передачи корректирующей информации».

11. Руководство по защите информации от несанкционированного доступа в ВС РФ, введенное в 2005 г. приказом МО РФ № 011.

12. «Новости навигации». – 2009. – № 4.

13. Мат-лы IV Международного форума по спутниковой навигации. – 1 июня 2010 г., Москва, ЦВК «Экспоцентр».