Космічна наука і технологія. 1998. Т 4. № 5/6. С. 62—66.

УДК 621.391.372.019.3

Предложения по обеспечению безопасности информации в единой спутниковой системе передачи информации

И. Д. Горбенко[1], Ю. В. Стасев[2], А. В. Потий[2], А. М. Ткачев[2]

[1]Харьківський державний технічний університет радіоелектроніки

[2]Харківський військовий університет

Надійшла до редакції 17.03.98

Пропонується концепція побудови системи забезпечення безпеки інформації, що створюється єдиною супутниковою системою передачі інформації України. Розглядається загальний ідеологічний подхід до побудови системи захисту інформації в такій системі.

ВВЕДЕНИЕ

В интересах управления государством в Украине создается единая спутниковая система передачи информации (ЕС СПИ), предназначенная для непрерывного и комплексного информационного обмена как внутри различных ведомств и министерств, так и между ними. В основу создания и развития ЕС СПИ положена многолетняя программа, предусматривающая последовательную и целенаправленную отработку технических решений и методов управления системой. По мере осознания целей и задач, стоящих перед ЕС СПИ, наметился системный подход к планированию, использованию и разработке технического облика системы. Опыт разработки и эксплуатации подобных систем за рубежом показывает, что создаваемая в Украине ЕС СПИ должна строиться на основе архитектуры открытых систем. Построение ЕС СПИ на принципах открытых систем позволяет объединить в единую информационную систему различные ведомственные системы и обеспечит простой доступ пользователей к корпоративной информации. Вместе с тем такое построение ЕС СПИ выдвигает на первый план проблему безопасности информации, вычислительных компонентов, аппаратных платформ, операционных систем, баз данных и прикладного программного обеспечения различных пользователей. Проблема безопасности информации в ЕС СПИ состоит не только в реализации совокупности мер, гарантирующих сохранность корпоративной информации от случайного или преднамеренного разрушения и несанкционированного использования, но и в согласовании работы средств защиты различных ведомств и звеньев системы. В настоящей статье авторы на основе опыта разработки и эксплуатации систем защиты информации в информационных системах рассматривают общий идеологический подход к построению системы защиты в ЕС СПИ Украины.

НАЗНАЧЕНИЕ И ЦЕЛЬ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЕС СПИ

Система защиты информации предназначена для непрерывной и комплексной защиты информации в процессе информационного обмена в сети ЕС СПИ Украины с требуемыми уровнями защиты, обеспечивающими реализацию политики безопасности

информации на всех этапах ее жизненного цикла с использованием передовых информационных технологий.

Ядром, определяющим принципы построения системы защиты информации ЕС СПИ, является политика безопасности - набор правил, определяющих процедуры и механизмы обеспечения безопасности всего множества объектов и субъектов безопасности ЕС СПИ.

В практическом приложении политика безопасности проявляется через совокупность документированных управленческих решений, направленных на обеспечение безопасности информации и ассоциированных с ней ресурсов. Политика безопасности реализуется в системе защиты информации, представляющей собой комплекс организационных мер, организационно-технических методов, мероприятий и средств, юридических и законодательных норм, физических ограничений, для предотвращения причинения вреда интересам собственника информации.

Основными целями создания системы защиты информации в ЕС СПИ являются:

1. Обеспечение конфиденциальности информации и сообщений, циркулирующих в ЕС СПИ, на основе применения симметричных и несимметричных сертифицированных (стандартных) алгоритмов шифрования.

2. Обеспечение целостности и подлинности информации и сообщений, циркулирующих в ЕС СПИ, на основе применения алгоритмов цифровой подписи.

3. Защита трафика ЕС СПИ на сетевом уровне с использованием стандартных протоколов.

4. Обеспечение надежной идентификации объектов и субъектов сети, а также защита от несанкционированных действий как санкционированных, так и несанкционированных пользователей.

5. Управление ключевыми структурами на сетевом и прикладном уровнях в автономном и общесистемном режимах.

6. Обеспечени юридической ответственности пользователей ЕС СПИ за сформированные, переданные и принятые сообщения и защита их от обмана на основе применения несимметричной цифровой подписи для модели взаимного недоверия.

7. Обеспечение помехозащищенности и аутентификации радиоканалов управления космическими аппаратами.

Выполнение перечисленных выше целей достигается при реализации в системе защиты информации следующих положений.

1. В соответствии с целями и задачами ЕС СПИ формулируется и приводится в жизнь политика безопасности.

2. С учетом модели угроз выбираются и реализуются основные услуги и механизмы безопасности информации в ЕС СПИ.

3. Защита информации производится на нескольких уровнях эталонной модели взаимодействия открытых систем.

4. Каждое ведомство (объект ЕС СПИ), осуществляющее информационный обмен как внутри, так и с другими ведомствами обязательно осуществляет защиту информации с реализацией механизмов цифровой подписи, аутентификации, контроля целостности, шифрования, управления доступом и маршрутизации, автоматического протоколирования и аудита.

5. Для решения задач генерации, распределения, передачи, приема, хранения, ввода, использования, уничтожения и восстановления ключевых структур для различных ведомств или групп ведомств, создаются центры управления безопасностью.

6. Защита от захвата и анализа пакетов (защита трафика) осуществляется на сетевом уровне посредством инкапсуляции пакетов с шифрованием информационной части пакета, заголовка и адресов с использованием высокоскоростных алгоритмов шифрования на сеансовых ключах.

7. Механизмы цифровой подписи, симметричного и несимметричного шифрования реализуется программно, программно-аппаратно или аппаратно.

8. Защита информации в отдельных компьютерах и серверах производится на основе прозрачного шифрования, управления доступом и разграничения полномочий.

СОСТАВ И СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ЕС СПИ может быть разбита на три подсистемы: наземная сеть передачи информации, спутниковая подсистема передачи информации, подсистема управления космическими аппаратами и наземными средствами передачи информации. Система защиты информации должна обеспечивать безопасность информации во всех элементах ЕС СПИ. Различная физическая природа наземной и спутниковой сетей предполагает использование различных подходов к обеспечению безопасности информации, а следовательно, приводит к необходимости разработки и реализации различных методов и средств защиты информации. Вместе с тем эти различные подходы должны быть интегрированы в ЕС СПИ с учетом единой политики безопасности.

Сложность построения системы обеспечения информации усугубляется еще и тем, что необходимо разрабатывать и совмещать друг с другом системы безопасности информации различных структурных звеньев ЕС СПИ. Здесь можно различить системы защиты информации ведомственных сетей, региональные системы обеспечения защиты информации и единую систему обеспечения безопасности информации. Ясно, что в этом случае нельзя говорить о полном аппаратном и программном совмещении и однородности этих систем. Отсюда вытекает важность и большая значимость выработки единой идеологии обеспечения безопасности информации в ЕС СПИ, необходимость разработки единых требований по безопасности информации, как организационных, так и технических, которые должны быть обязательными для всех субъектов (пользователей) ЕС СПИ.

Высокие характеристики безопасности могут быть достигнуты при комплексном подходе к разработке системы безопасности информации. А это значит, что политика и система безопасности должны разрабатываться параллельно с разработкой основных компонентов ЕС СПИ. В противном случае средства защиты информации не будут интегрированы в структуру всех компонентов единой сети. Процесс проектирования и создания системы защиты информации в ЕС СПИ должен быть многоэтапным: проведение анализа объекта защиты с выявлением характера защищаемой информации, выявление каналов утечки и угроз, разработка и внедрения методов и средств защиты информации, оценка эффективности принятых мер по защите информации. Сущность проблемы обеспечения безопасности информации предполагает постоянный контроль, анализ и оценку эффективности используемых организационных и технических средств ЗИ, проводятся работы по выявлению незащищенных или вновь возникших каналов утечки информации и угроз. На основе полученных результатов анализа осуществляется разработка дополнительных мер по обеспечению безопасности с целью ее усовершенствования.

Сложность и многообразие задач, решаемых ЕС СПИ предполагает многофункциональность системы защиты информации. Это позволит обеспечить гибкость системы и непрерывную комплексную защиту информации на всех этапах ее жизненного цикла с требуемым уровнем защиты.

Система защиты информации в ЕС СПИ может состоять из рабочих станций (РС) пользователей прикладного уровня, рабочих станций (серверов) сетевого уровня, центров управления безопасностью (главного (ГЦРК) и региональных центров управления ключами (ЦРК)), серверов администраторов локальных сетей и сетевых экранов (брандмауэров).

1. Рабочая станция пользователя ЕС СПИ на прикладном уровне должна обеспечивать:

цифровую подпись сообщения по алгоритму ГОСТ 3410-94, DSS и национальным алгоритмам;

симметричное шифрование и дешифрование сообщений по ГОСТ 28147-89, IDEA и национальным стандартам;

архивирование и рандомизацию сообщений;

направленное шифрование и дешифрование информации в системе с открытыми ключами;

подготовку криптограмм для эффективной передачи по сети ЕС СПИ;

автоматическое протоколирование всех операций, выполняемых на рабочих станциях, блокировку в случае несанкционированных действий с сигнализацией на вышестоящее звено;

генерацию личных и открытых ключей, передачу их в центр для сертификации, прием сертифицированных ключей их запись, хранение и использование.

2. Рабочая станция сетевого уровня должна обеспечивать:

инкапсуляцию или шифрование пакетов на сетевом уровне с использованием стандартных протоколов;

выработку личных и открытых ключей, передачу и прием открытых ключей после сертификации;

взаимодействие с «видимыми» рабочими станциями сетевого уровня, в том числе в режиме удаления или добавления;

взаимодействие с центрами управления безопасностью с использованием состоятельных протоколов.

3. Центр управления безопасностью должен обеспечивать:

генерацию (расчет) открытых ключевых параметров цифровой подписи по ГОСТ 3410-94, DSS и др.;

формирование секретных и открытых параметров ключа сертификации центра для ГОСТ 3410 -94, DSS и др.;

формирование, распределение и доставку открытых ключевых параметров, открытого ключа сертификации центра открытых и секретных ключей сертификации пользователей на соответствующие станции;

создание инсталляционного именного пакета станции генерации ключей для каждого пользователя;

сертификация открытых рабочих ключей всех рабочих станций и передачу их на рабочие станции.

4. Центры управления безопасностью на сетевом уровне должны обеспечивать:

формирование, распределение и доставку открытых и секретных ключевых параметров и ключей сертификации на рабочие станции сетевого уровня;

согласование механизмов защиты между различными ведомствами и регионами, выбор режимов работы;

управление ключевыми структурами с использование состоятельных протоколов;

изменение конфигурации сети, в том числе в режимах удаления или добавления рабочих станций.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В СПУТНИКОВЫХ РАДИОКАНАЛАХ

Основными задачами системы и аппаратуры защиты информации в спутниковых радиоканалах являются:

1) обеспечение подлинности и целостности передаваемой командно-программной информации;

2) обеспечение конфиденциальности данных и командно-программной информации;

3) обеспечение идентификации и аутентификации объектов и субъектов процесса управления в спутниковых радиоканалах;

4) защита от несанкционированного вхождения в связь, а также защита от несанкционированных действий пользователей спутниковых радиоканалов;

5) Обеспечение юридической ответственности пользователей за сформированные, переданные, принятые и исполненные команды;

6) управление специальными данными.

Проблема безопасности информации, передаваемой по спутниковым радиоканалам, требует решения проблем помехозащищенности и имитостойкости. В существующих системах на сегодняшний день эти проблемы решаются раздельно. Проблема помехозащищенности решается либо за счет увеличения энергетических ресурсов спутниковой радиолинии, либо за счет применения на физическом уровне сложных сигналов с частотной избыточностью. Требуемая имитостойкость обеспечивается посредством криптографического преобразования дискретной информации. Однако в такой концепции защиты информации не реализуются потенциальные возможности спутниковых систем связи и управления по обеспечению безопасности информации [1]. Комплексное решение проблемы помехозащищенности и имитостойкости достигаются за счет реализации в спутниковом радиоканале динамической смены форм сигналов, при которой соответствие «информационный символ — сигнал-переносчик» изменяется во времени по псевдослучайному закону [2].

Важной частью системы спутниковой связи и управления, реализующей режим динамической смены форм сигналов, является система синхронизации управляющих генераторов. Эта система должна обеспечить не только синхронность работы генераторов управляющих множеств наземной и бортовой аппаратуры, но и синхронность применения конфиденциальных ключей. Используемые конфиденциальные ключи, в зависимости от реализованного алгоритма функционирования генераторов управляющих множеств, могут быть как симметричными, так и несимметричными. Реализация режима динамической смены форм сигналов позволит решить на физическом уровне проблему защиты спутниковых систем связи и управления от несанкционированного доступа к каналу и обеспечит активную имито- и помехозащиту [2].

ЗАКЛЮЧЕНИЕ

Для технической реализации системы защиты информации в ЕС СПИ требуется реализовать следующие положения.

- Защите подлежат вся информация и ресурсы, представленные в ЕС СПИ.
- Защита информации производится не менее чем на двух уровнях - прикладном и сетевом.
- На прикладном уровне каждое ведомство или группа ведомств защиту информации осуществляют с разграничением по уровням секретности и ведомствам.
- Для защиты информации на прикладном уровне в той или иной мере применяются механизмы аутентификации, в том числе цифровой подписи, контроля целостности и подлинности, шифрования, управления доступом, автоматического протоколирования и аудита.
- Управление ключевыми структурами и безопасностью на прикладном уровне производится с ведомственных центров, которые взаимодействуют с главным и, возможно, региональными центрами управления безопасностью в ЕС СПИ.
- Защита трафика сети осуществляется на сетевом уровне посредством инкапсуляции пакетов с ис-

пользованием высокоскоростных алгоритмов шифрования с распределением и выработкой секретных пакетных ключей по каждому направлению в системе с открытым распространением ключей.

- На начальном этапе создания сети для реализации механизмов защиты используются процедуры и алгоритмы, разрешенные для применения в Украине, а на последующих этапах — и национальные, получившие соответствующие сертификаты.
- Процедуры и алгоритмы, в зависимости от финансовых возможностей Украины, могут быть реализованы программно, программноаппаратно или аппаратно.
- Защита информации, в том числе управление доступом в выделенных локальных сетях, производится специальным сервером-администратором.
- Защита локальных сетей от угроз извне производится с использованием специальных экранов (брандмауэров).
- Процедуры идентификации, аутентификации и обмена ключами реализуются с использованием состоятельных протоколов.
- В отдельных локальных сетях и ведомствах на прикладном уровне может осуществляться несколько процедур цифровой подписи, управления доступом и шифрования.
- Параметры процедур и алгоритмов защиты информации выбираются с учетом допустимых рисков и ограничений с использованием соответствующих показателей.
- На всех уровнях осуществляется обработка кодов возврата преобразований, которые фискально доступны соответствующим центрам управления безопасностью.

Изложенные предложения могут быть взяты за основу при разработке политики безопасности и системы защиты информации в ЕС СПИ.

1. Горбенко И. Д., Стасев Ю. В. Безопасность информации в космических системах связи и управления // Космічна наука і технологія.—1996.—**2**, № 5/6.—С. 64—68.
2. Стасев. Ю. В., Горбенко И. Д., Пастухов Н. В. Аутентификация в космических системах связи и управления с множественным доступом // Космічна наука і технологія.—1997.—**3**, № 1/2.—С. 83—86.

PROPOSITIONS FOR ENSURING THE INFORMATION SECURITY IN THE COMMON UKRAINIAN SATELLITE SYSTEM OF INFORMATION TRANSMISSION

I. D. Gorbenko, Yu. V. Stasev, A. V. Potii, and A. M. Tkachev

We propose a concept of constructing a system which would ensure the information security in the common satellite system of information fransmission being created in Ukraine. General ideas of the construction of the information protection system are considered.