УДК 007

Е. С. Жукова, И. Н. Карцан

# ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ЦЕНТРЕ УПРАВЛЕНИЯ ПОЛЕТАМИ

*Рассмотрен комплекс мер обеспечения конфиденциальности информации, обрабатываемой информационной системой Центра управления полетами.*

*Ключевые слова: обеспечение информационной безопасности, криптографическая защита информации.*

Национальное агентство по аэронавтике и космическим исследованиям (NASA) не так давно подтвердило информацию о том, что доставленные на орбиту ноутбуки были заражены вирусом Gammima.AG. Данный случай проникновения вируса в служебные компьютеры космической станции далеко не единственный, а развитие космического туризма в будущем увеличит угрозу вирусных атак на компьютеры малых космических станций (МКС).

Вышедшие за пределы планеты компьютерные вирусы – это тревожный знак, показывающий необходимость ужесточения существующих мер по защите информации.

Основной задачей Центра управления полетами (ЦУП) является управление и координирование космических аппаратов. Под информационной системой ЦУП будем понимать рабочие места операторов ЦУП (наземный комплекс управления), системы и сети передачи данных и бортовой комплекс управления космических аппаратов. Обрабатываемая и передаваемая информация имеет высокую важность, а ее перехват или искажение могут принести не только разглашение информации ограниченного распространения, но и более разрушительные последствия. Одной из важных задач является обеспечение информационной безопасности системы ЦУП.

В современных условиях непрерывного повышения ценности информационных ресурсов, с одной стороны, и постоянного роста правонарушений в области информационных технологий – с другой, построение эффективной системы комплексного обеспечения информационной безопасности становится одним из ключевых факторов, обуславливающим жизнедеятельность информационной системы.

В соответствии с законодательством Российской Федерации информационную безопасность можно определить как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная безопасность имеет три основные составляющие: конфиденциальность, целостность и доступность.

Под конфиденциальностью понимается свойство информации, которое характеризуется способностью сохраняться в тайне от субъектов, у которых нет полномочий на право ознакомления с ней. Обеспечение конфиденциальности информации и защита ее от утечки, искажения или уничтожения особенно важны в информационных системах стратегических предприятий и организаций.

Показатель уровня защиты определяется основными видами потенциальных нарушений безопасности информации. В многофункциональной и глобальной информационной системе ЦУП меры защиты информации предупреждают следующие угрозы безопасности:

– нарушения, ведущие к утечке информации из подсистем и линий связи, искажению информации и дезорганизации системы;

– несанкционированные действия обслуживающего персонала системы, ведущие к искажению, уничтожению или утечке информации;

– несанкционированные действия абонентов, ведущие к утечке информации;

– нарушения безопасности и достоверности информации посредством несанкционированного доступа к программному обеспечению системы и базам данных, внедрения в них компьютерных вирусов;

– воздействие на систему и ее сети связи неблагоприятных факторов окружающей среды и стихийных бедствий, ведущих к нарушению функционирования системы и уничтожению информации.

Локализация и предотвращение указанных воздействий на систему могут быть реализованы только при системном подходе к организации и обеспечению защиты информации. Комплексный подход к обеспечению безопасности информационной системы предусматривает следующее:

– системный анализ потенциально возможных угроз безопасности информационной системы;

– комплексное использование методов и средств защиты и создание механизма защиты, гарантирующего надежное перекрытие возможных каналов утечки и несанкционированного доступа к информационной системе;

– разработку методов и средств защиты одновременно с созданием самой информационной системы, интеграцию средств защиты информации в информационную систему ЦУП;

– аттестацию и сертификацию средств защиты и каналов передачи, приема и обработки конфиденциальной информации.

Система защиты информации должна обеспечивать создание механизма защиты, адекватного потребностям защиты информации (критерий достаточности); удобство для пользователей; минимизацию привилегий в доступе к ресурсам системы и информации, предоставляемых пользователям; полноту контроля всех обращений к системе и информации; наказуемость нарушений (отказ в доступе к системе и др.); экономичность механизма защиты.

К настоящему времени разработан достаточно полный перечень способов и средств, позволяющих при их комплексном использовании создать достаточно надеж-

ный механизм защиты. Распределим меры по защите информации на основные группы:

– законодательные;

– организационные;

– технические;

– аппаратно-программные;

– криптографические.

*Законодательный уровень* является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается или наказывается обществом.

В процессе создания и эксплуатации Центр управления полетами строит свой механизм защиты, основываясь, в первую очередь, на законодательные акты, которые дают основные понятия, регламентируют правила использования и обработки информации, определяют основные требования как к мерам по защите информации, так и к средствам защиты, кроме того определяют меры ответственности за нарушение этих правил.

На законодательном уровне условно различают две группы мер:

– меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности;

– направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

Самое трудное и самое важное на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. На данный момент прогресс в информационной сфере намного обгоняет законодательные акты, что на практике ведет к существенному снижению уровня информационной безопасности.

Перечислим основные законы Российской Федерации в области информационной безопасности:

– Конституция Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Уголовный кодекс Российской Федерации;

– ФЗ «О государственной тайне»;

– ФЗ «О коммерческой тайне»;

– ФЗ «Об информации, информационных технологиях и о защите информации»;

– ФЗ «О лицензировании отдельных видов деятельности»;

– ФЗ «Об участии в международном информационном обмене»;

– ФЗ «Об электронной цифровой подписи»;

– ФЗ «О персональных данных».

Законодательная база дает основные понятия, а также определяет каналы утечки информации и требования к средствами защиты. Основываясь на данных требованиях, с помощью организационных мер по защите информации разрабатываются меры по обеспечению безопасности, а также порядок их введения и контроля.

*Организационные меры* защиты информации представляют собой совокупность мероприятий, решений и процедур, регламентирующих передачу и обработку информации на всех этапах технологического процесса создания и эксплуатации информационной системы Центра управления полетами. К ним относятся мероприятия, направленные на обеспечение защиты при разработке общего проекта информационной системы, ее монтаже, отладке, испытаниях и эксплуатации оборудования системы, организация охраны и ограниченного доступа в помещения, где обрабатывается конфиденциальная информация, организация технологии обработки информации, а также подбор и подготовка обслуживающего персонала.

В целом этот комплекс мероприятий позволяет полностью или частично перекрыть значительную часть каналов утечки информации и обеспечить объединение всех используемых средств в целостный механизм защиты.

К данной группе относятся также методы, обеспечивающие создание таких структур различных компонентов информационной системы, которые позволяют наиболее эффективно применять меры защиты: топология сети, режимы функционирования технических средств и т. д.

Для построения комплексной системы безопасности информационной системы Центра управления необходимо применение следующих организационных мероприятий:

1) определение уровня (категории) конфиденциальности защищаемой информации (зависит от категории космического аппарата: спутник связи, научно-исследовательский спутник, военный и т. д.);

2) выбор принципа методов (локальный, объектовый или смешанный) и средств защиты;

3) установление порядка обработки защищаемой информации;

4) учет пространственных факторов:

– введение контролируемых (охраняемых) зон;

– правильный выбор помещений и расположение объектов между собой и относительно границ контролируемой зоны;

5) учет временных факторов:

– ограничение времени обработки защищаемой информации;

– доведение обработки информации с высоким уровнем конфиденциальности до узкого круга лиц;

6) учет физических и технических факторов:

– определение возможности визуального (или с помощью технических средств) наблюдения отображаемой информации посторонними лицами;

– отключение контрольно-измерительной аппаратуры от информационного объекта и ее обесточивание;

– максимальное разнесение информационных кабелей между собой и относительно проводящих конструкций, их пересечение под прямым углом.

Для блокирования возможных каналов утечки информации через технические средства обеспечения производственной и трудовой деятельности с помощью специальных технических средств и создания системы защиты объекта по ним необходимо осуществить ряд мероприятий:

– проанализировать специфические особенности расположения зданий, помещений в зданиях, территорию вокруг них и подведенные коммуникации;

– выделить те помещения, внутри которых циркулирует конфиденциальная информация, и учесть используемые в них технические средства;

– осуществить следующие действия:

проверить используемую технику на соответствие величины побочных излучений допустимым уровням, экранировать помещения с техникой или эту технику в помещениях;

перемонтировать отдельные цепи, линии, кабели;

использовать специальные устройства и средства пассивной и активной защиты.

Следующим этапом при создании комплексной системы защиты информации должен быть подбор и внедрение *технических средств* защиты информации, т. е. таких средств, в которых основная защитная функция реализуется техническим устройством (комплексом или системой).

К техническим средствам относятся различные электронные и электронно-механические устройства, которые включаются в состав технических средств информационной системы Центра управления полетами и выполняют в комплексе с другими средствами функции защиты и контроля доступа к информации и системе в целом.

К техническим средствам также можно отнести средства экранирования отдельных устройств и помещений для исключения побочных электромагнитных излучений, а также специальные средства излучения шумовых сигналов, маскирующих информационные сигналы.

Некоторые каналы утечки информации возможно перекрыть как техническими (аппаратными), так и программными мерами защиты. Выбор средства защиты должен быть обусловлен принципом достаточности. Для информационной системы с более высоким классом защиты предпочтение следует отдать техническим средствам защиты. Несомненными достоинствами технических средств защиты информации являются следующие:

– достаточно высокая надежность;

– широкий круг задач;

– возможность создания комплексных систем защиты информации;

– гибкое реагирование на попытки несанкционированного воздействия;

– традиционность используемых методов осуществления защитных функций.

Основные недостатки технических средств защиты информации заключаются в высокой стоимости многих средств и необходимости регулярного проведения контроля за их работоспособностью.

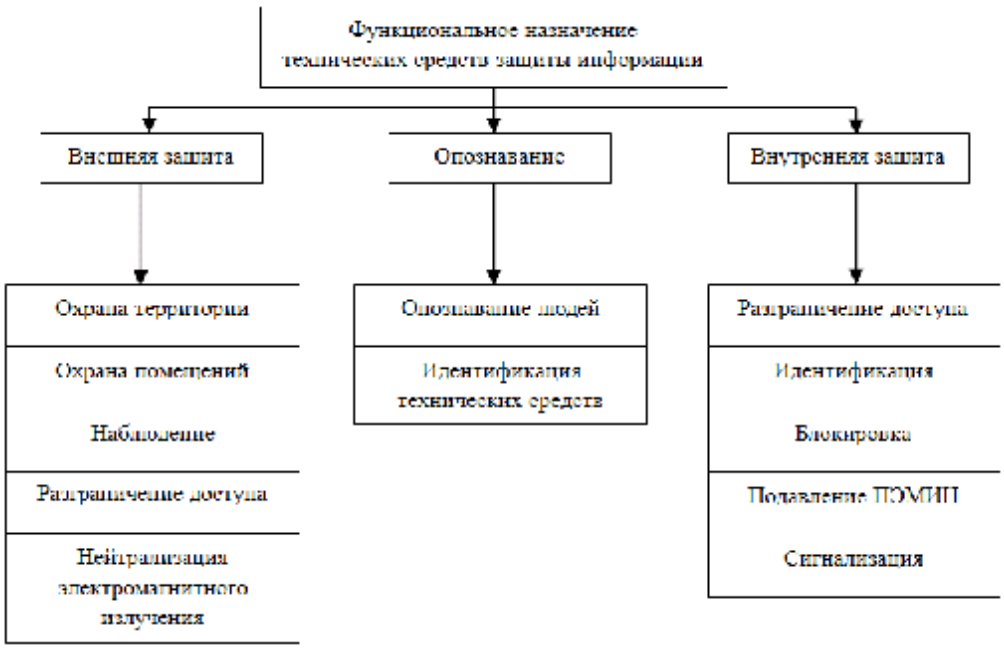
Выделяют три глобальные функции защиты, выполняемые техническими средствами: внешняя защита, опознавание и внутренняя защита. Дальнейшая детализация функциональной классификации технических средств защиты информации приводит к выделению одиннадцати групп (см. рисунок). Средства защиты, входящие в эти группы, могут быть различной сложности и различного исполнения.

Существует ряд уязвимостей информационной системы, устранить которые возможно только с использованием *программных средств защиты* информации. Несмотря на то что современные операционные системы (ОС) для персональных компьютеров, такие как Windows 2000, Windows XP и Windows NT, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Большинство систем не способно защитить данные, находящиеся за их пределами, и в этих случаях для их защиты используются программные средства защиты.

К программным средствам защиты информации относятся специальные программы, которые должны включаться в состав программного обеспечения информационной системы Центра управления полетами для обеспечения функций защиты.

В соответствии с выполняемыми функциями программы защиты разделяются на следующие группы:

– шифрование (криптографическая защита информации);




Классификация технических средств защиты информации по функциональному назначению

– резервное копирование данных;
– антивирусные программы;
– средства идентификации и аутентификации;
– контроль и управление доступом;
– протоколирование и аудит.

Защита информации от компьютерных вирусов (особенно важна в вычислительных сетях) обычно реализуется разнообразными методами и средствами, в том числе специальными антивирусными программами.

При выборе программного продукта для устранения той или иной уязвимости информационной системы, в первую очередь, необходимо учитывать требования, предъявленные к средствам защиты информации установленного класса.

*Криптографическую защиту* информации можно отнести как к программным, так и к аппаратным средствам защиты информации. Защита данных с помощью шифрования – одно из возможных решений проблемы безопасности, а в условиях передачи информации по радиочастотному каналу это решение становится основным средством обеспечения конфиденциальности информации. Зашифрованные данные становятся доступными только тем, кто знает, как их расшифровать, и поэтому похищение зашифрованных данных абсолютно бессмысленно для несанкционированных пользователей. Программная реализация более практична, допускает некоторую гибкость в использовании, а также отличается существенно меньшей стоимостью. Аппаратная реализация отличается высокой производительностью, простотой, защищенностью и т. д. Исходя из этого, в ряде зарубежных стран налажено промышленное производство аппаратуры для шифрования и имеется значительный опыт ее практического использования для сокрытия информации ограниченного распространения, особенно в информационно-вычислительных сетях, так как при передаче информации по линиям связи большой протяженности (в том числе радиолиниям) этот вид защиты является единственным способом надежной защиты передаваемых данных. Однако необходимо учесть, что зашифрованный текст будет передаваться на очень большие расстояния, и влияние помех будет велико. Исходя из специфики информационной системы Центра управления полетами, в данном случае будет использоваться помехоустойчивое кодирование, т. е. должна быть реализована возможность корректировки ошибок.

В настоящее время известно большое число методов криптографического закрытия информации. Классификация методов шифрования (криптоалгоритмов) может быть осуществлена по следующим признакам:

– по типу ключей – симметричные и асимметричные;

– по размеру блока информации – потоковые шифры, блочные шифры;

– по характеру воздействий, производимых над данными – метод замены (перестановки), метод подстановки, аналитические методы, аддитивные методы (гаммирование), комбинированные методы.

Кодирование может быть смысловое, символьное, комбинированное.

Независимо от способа реализации для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

– стойкость шифра должна противостоять криптоанализу или требовать создания и использования дорогих вычислительных систем;

– криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа;

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– шифр должен быть стойким даже в случае, если нарушителю известно достаточно много: зашифрованный текст, исходный текст;

– незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста;

– структурные элементы алгоритма шифрования должны быть неизменными;

– зашифрованный текст не должен существенно превосходить по объему исходную информацию;

– дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

– ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

– не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать равную криптостойкость;

– время шифрования не должно быть большим;

– стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

При использовании комплекса мер по защите информации, а также контроля их соблюдения и обновления, конфиденциальность информации, обрабатываемой в Центре управления полетами, будет полностью обеспечена. Однако не стоит забывать, что научно-технических прогресс не стоит на месте, и у злоумышленников в арсенале появляются новые возможности по взлому паролей, шифров, создаются новые вредоносные программы. Система безопасности информации должна постоянно проходить контроль соответствия требованиям безопасности и вводить новые рубежи защиты.

Принимая во внимание удаленность линий связи, специфику обработки информации, основной акцент в системе обеспечения конфиденциальности информации в информационной системе Центра управления полетами необходимо делать на криптографическую защиту. Шифрование информации позволит избежать последствий ее разглашения при несанкционированном доступе. Рекомендуется использовать аппаратные средства кодирования, которые обладают большей производительностью.

E. S. Zhukova, I. N. Kartsan

## MAINTENANCE OF THE INFORMATION CONFIDENTIALITY IN THE CENTRE OF FLIGHT CONTROL

*The series of measures to maintain the information confidentiality processed by information system in the Centre of flight control are considered.*

*Keywords: information safety maintenance, cryptographic protection of the information.*



УДК 629.78.064

П. И. Мельников, Р. В. Козлов, В. С. Кудряшов

# СИСТЕМА ЭЛЕКТРОПИТАНИЯ МАЛОГО КОСМИЧЕСКОГО АППАРАТА «СТУДЕНЧЕСКИЙ»

*Изложены результаты проектирования системы электропитания малого космического аппарата «Студенческий».*

*Ключевые слова: система электропитания, экстремальное регулирование мощности, мостовой инвертор, литий-ионная аккумуляторная батарея, концентраторы.*

Малый космический аппарат «Студенческий» (далее – СМКА) – космический аппарат микрокласса. Основное предназначение СМКА – решение прикладных задач и проведение экспериментальной отработки новых технологий, в том числе в части систем электропитания (СЭП).

Цель представленной работы – проектирование СЭП для СМКА (рис. 1).

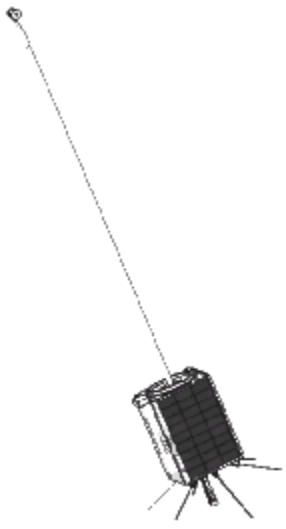


Рис. 1. Внешний вид космического аппарата «Студенческий»

СЭП состоит из следующих элементов:

– солнечной батареи;

– аккумуляторной батареи;

– блока автоматики и стабилизации напряжения.

При работе над СЭП принималась следующая философия проектирования:

1. На первых СМКА ввиду крайне сжатых сроков создания космического аппарата (КА) применялось решение, которое использовалось на малом космическом аппарате (МКА) «Юбилейный» – устанавливался комплект аппаратуры ДОКА-Б, поставляемый НИЛАКТ (г. Калуга). В состав этой аппаратуры входят металлогидридная аккумуляторная батарея (АБ) из 10 аккумуляторов емкостью 9,5 Ач и автоматика СЭП. Поэтому на первых МКА «Студенческий» разрабатывалась только солнечная батарея (БС).

2. На втором этапе проектировалась и разрабатывалась базовая СЭП СМКА на основе инновационных решений по АБ и электронной части СЭП. В составе базовой СЭП использовалась БС, разработанная для первого этапа.

3. Разрабатывалась программа летных экспериментов по СЭП КА, преследующая две цели:

– отработку новых технологий в интересах ОАО «ИСС»;

– отработку новых решений для базовой СЭП СМКА.

Использовались следующие исходные данные для проектирования:

– высота орбиты СМКА 1 200 км;

– период обращения 115 мин, максимальная длительность теневого участка орбиты 35 мин;

– срок активного существования (САС) 1 год;

– рассматривались два способа пассивной магнитогравитационной ориентации КА:

одноосная на Землю;

трехосная (одна ось на Землю, вторая – по нормали к орбите, третья – по направлению движения КА);

– напряжение питания аппаратуры $12^{+3}_{-2}$ В;

– форма КА (БС) – параллелепипед;

– дежурная нагрузка при одноосной ориентации 10,1 Вт, при трехосной ориентации – 12,1 Вт;