УДК 629.785

ОРБИТАЛЬНЫЙ СЕРВЕР НА БАЗЕ СВЕРХМАЛОГО КОСМИЧЕСКОГО АППАРАТА

Д.В. Малыгин, генеральный директор
ООО «Лаборатория проектирования сверхмалых космических аппаратов «Астрономикон», Санкт-Петербург
E-mail: Malygin.DV@Astronomikon.ru

Когда-то сеть интернет создавалась для военных целей: связи между узлами управления огнём и военными базами [1]. Затем такие разработки стали использоваться в мирных целях, и постепенно наступил момент, когда большая часть населения планеты получила доступ к сети. Выкладывая информацию в интернет, она попадает в центры обработки данных (хранение информации, выкладываемой в сеть). Начиная от ваших личных фотографий, загруженных документов, записей разговоров по Скайпу, и заканчивая комментариями в блогах/социальных сетях. Таким образом дата-центр – хранилище контента (разработчики преследовали несколько целей: круглосуточную доступность, защиту, сохранение информации и целостности файлов) [1]. То есть суть дата-центров заключается в обеспечении конфиденциальности и полной неприкосновенность контента.

Этот вопрос стал особо актуален в банковской сфере, особенно при международных транзакциях: необходимо обеспечить защищённый доступ к данным в любой точке планеты. Более того с распространением криптовалют и подобных цифровых ресурсов, обладающих высокой ликвидностью, способы защиты и анонимности вышли на принципиально новый уровень [2].

Поясним: любые дата-центры (сервера) могут быть атакованы как через сеть виртуально, так и физически:

1. санкции, ограничения на транзакции – мир глобален, следовательно, при возникновении вопросов в какой-либо юрисдикции возможен вариант введения ограничений на финансовые потоки и тем самым наносится экономический ущерб конечному бенефициару таких ресурсов;
2. физические атаки на дата-центры – несанкционированный доступ с выемкой оборудования, либо форс-мажорные обстоятельства (воздействие факторов непреодолимой силы, которые нельзя предвидеть или избежать, включая объявленную или фактическую войну, гражданские волнения, эпидемии, блокаду, землетрясения, наводнения, пожары, техногенные катастрофы и другие стихийные бедствия);
3. выход из строя дата-центра из-за сбоя в системах энергопитания, локальные или веерные отключения доступа в сеть интернет;
4. проникновение через удалённый доступ, хакерские атаки и воздействие вредоносного программного обеспечения.

Также существует особо ценные данные, которые необходимо передать от одного абонента к другому. Если использовать сеть интернет, то есть вероятность отслеживания такого контента. Передача через курьеров тоже не решает вопрос безопасности: существует вероятность перехвата.

Резюмируя выше сказанное специалистами ООО «Лаборатория «Астрономикон» предлагается иным способом достичь поставленную цель по обеспечению безопасности: разработка автономного, исключающий физический доступ дата-центра. В данной статье рассмотрены концептуальные вопросы такого проекта – расположить хранилище данных на низкой околоземной орите (500-1000 км) в виде полезной нагрузки (ПН) сверхмалого космического аппарата (СМКА или наноспутника) [3].

В качестве стартовой единицы для сбора наноспутника выступает многоцелевая унифицированная платформа «Синергия» блочно-модульного типа, которая предназначена для обеспечения проведения научных, образовательных и технологических экспериментов в условиях космического пространства.

Служебный модуль обеспечивает совокупность служебных функций:

- управление работой бортовых систем, включая ПН;
- определение положения СМКА в пространстве на орбите относительно потребителя на Земле для обеспечения корректной связи и надёжного канала приёма-передачи;
- сбор телеметрической информации;
- двусторонняя связь с наземными пунктами;
- парирование внештатных ситуаций.

Модуль ПН (масса модуля ~ 2 кг, мощность электроснабжения ~ 3 Вт) предназначен для размещения массива твердотельных накопителей, коммутатора обеспечения корректной работы, включая электроснабжение и обеспечение теплового режима.

Таким образом исключается физический доступ к данным, достигается сохранность и анонимность доступа.

Библиографические ссылки

1. *Э. Таненбаум, Д. Уэзеролл «*Компьютерные сети» // 5-е изд., ISBN 978-5-4461-1248-7.
2. *Сборник научных трудов под редакцией Н. Э. Соколинской «*Современные проблемы и перспективы развития рынка криптовалюты в РФ» // ISBN 978-5-4365-2339-2
3. *Малыгин Д. В.* «Многоцелевая платформа «Синергия» блочно-модульного типа для сборки наноспутников». Известия высших учебных заведений. Приборостроение. 2018. Т. 61. № 8. С. 692-700.